Semantics for a Higher Order Functional Programming Language for Quantum Computation

Benoît Valiron

To cite this version:


HAL Id: tel-00483944
https://tel.archives-ouvertes.fr/tel-00483944
Submitted on 17 May 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Benoît Valiron

Thesis Submitted to the Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

© Benoît Valiron, Ottawa, Canada, 2008

1The Ph.D. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics
Pour mon père.
Abstract

The objective of this thesis is to develop a semantics for higher-order quantum information.

Following the work done in the author’s M.Sc. thesis, we study a lambda calculus for quantum computation with classical control. The language features two important properties. The first one, arising from the so-called no-cloning theorem of quantum computation, is the need for a distinction between duplicable and non-duplicable elements. For keeping track of duplicability at higher-order, we use a type system inspired by the resource-sensitive linear logic. The second important aspect is the probability inherent to measurement, the only operation for retrieving classical data from quantum data. This forces us into choosing a reduction strategy for being able to define an operational semantics.

We address the question of a denotational semantics in two respects. First, we restrict the study to the strictly linear aspect of the language. Doing so, we suppress the need for distinguishing between duplicable and non-duplicable elements and we can focus on the description of quantum features at higher-order. Using the category of completely positive maps as a framework, we build a fully abstract denotational model of the strictly linear fragment of the language.

The study of the full language is more demanding. For dealing with the probabilistic aspect of the language, we use a method inspired by Moggi and build a computational model with a distinction between values and computations. For the distinction between duplicability and non-duplicability in the calculus, we adapt Bierman’s linear category, where the duplication is considered as a comonad with specific properties. The resulting model is what we call a linear category for duplication. Finally, we only focus on the fragment of the language that contains the aforementioned elements, and remove the classical Boolean and quantum Boolean features to get a generic computational linear lambda-calculus. In this idealized setting, we show that such a language have a full and complete interpretation in a linear category for duplication.
Acknowledgements

Numerous people allowed me to write this thesis. In particular, I would like to thank:

• Peter, who supported me for yet another degree;
• Caroline, who came all the way to Halifax;
• my parents, for being supportive all that time;
• Rob, for feeding me with coffee;
• the administrative staff of both Dalhousie and Ottawa University, for being so helpful;
• and finally Gilles, for printing more than 1000 pages of this opus of content.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>iii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>iv</td>
</tr>
<tr>
<td>List of Figures</td>
<td>ix</td>
</tr>
<tr>
<td>List of Tables</td>
<td>x</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2 Notions of Category Theory</td>
<td>6</td>
</tr>
<tr>
<td>2.1 Categories and Functors</td>
<td>6</td>
</tr>
<tr>
<td>2.2 Natural Transformations</td>
<td>7</td>
</tr>
<tr>
<td>2.3 Adjoint Functors</td>
<td>8</td>
</tr>
<tr>
<td>2.4 Products and Coproducts</td>
<td>9</td>
</tr>
<tr>
<td>2.5 Monads</td>
<td>10</td>
</tr>
<tr>
<td>2.6 Comonads</td>
<td>11</td>
</tr>
<tr>
<td>2.7 Symmetric Monoidal Categories and Comonoids</td>
<td>13</td>
</tr>
<tr>
<td>2.7.1 Monoidal Categories</td>
<td>13</td>
</tr>
<tr>
<td>2.7.2 Commutative Comonoids</td>
<td>13</td>
</tr>
<tr>
<td>2.8 Monoidal Comonads and Coalgebras</td>
<td>14</td>
</tr>
<tr>
<td>3 Quantum Computation</td>
<td>17</td>
</tr>
<tr>
<td>3.1 Mathematical Formalism</td>
<td>17</td>
</tr>
<tr>
<td>3.1.1 Generalities on Finite Dimensional Hilbert Spaces</td>
<td>17</td>
</tr>
<tr>
<td>3.1.2 Tensor Products of Hilbert Spaces</td>
<td>19</td>
</tr>
<tr>
<td>3.1.3 Completely Positive Maps</td>
<td>19</td>
</tr>
<tr>
<td>3.1.4 Superoperators</td>
<td>20</td>
</tr>
<tr>
<td>3.1.5 The 2-Dimensional Hilbert Space</td>
<td>21</td>
</tr>
<tr>
<td>3.2 Quantum Foundations</td>
<td>23</td>
</tr>
<tr>
<td>3.2.1 Quantum Bits</td>
<td>23</td>
</tr>
<tr>
<td>3.2.2 Operations</td>
<td>23</td>
</tr>
<tr>
<td>3.2.3 Mixed States</td>
<td>25</td>
</tr>
<tr>
<td>3.3 Quantum Effects</td>
<td>26</td>
</tr>
<tr>
<td>3.3.1 No Cloning</td>
<td>26</td>
</tr>
<tr>
<td>3.3.2 Entanglement</td>
<td>26</td>
</tr>
<tr>
<td>3.3.3 Bell’s Inequalities</td>
<td>27</td>
</tr>
<tr>
<td>3.4 Some Algorithms and Uses of Quantum Effects</td>
<td>28</td>
</tr>
<tr>
<td>3.4.1 Teleportation</td>
<td>28</td>
</tr>
</tbody>
</table>
### 4. A Tour in Existing Models of Quantum Computation

4.1. The Various Paradigms

4.1.1. Unitary Gates as Computation

4.1.2. Concurrent Quantum Computation

4.1.3. Measurement-Based Quantum Computation

4.1.4. The ORAM Model

4.2. Formalism of Hilbert Spaces

4.2.1. Dagger Compact-Closed Categories

4.2.2. Classical Objects

4.3. A Flow-Chart Language

4.3.1. The language

4.3.2. The Category of Superoperators

4.3.3. Interpretation of the Flow-Chart Language

4.4. Extension to Higher-Order

### 5. Lambda Calculus and Semantics of Higher-Order Computation

5.1. Lambda Calculus

5.1.1. The Language

5.1.2. Free and Bound Variables

5.1.3. Alpha-Equivalence

5.1.4. Operational Meaning of Lambda Calculus

5.1.5. Typed Lambda Calculus

5.2. Proofs as Computations

5.2.1. Intuitionistic Logic

5.2.2. Curry-Howard Isomorphism

5.3. Categorical Logic

5.4. Lambda Calculus and Side Effects

5.4.1. Pure Versus Impure Calculus

5.4.2. Reduction Strategies

5.4.3. Towards a Semantics

5.4.4. Computational Model for Call-By-Value

5.5. Intuitionistic Linear Logic

5.6. Linear Calculi and their Interpretations

5.6.1. Earlier Models

5.6.2. Bierman’s Linear Category

### 6. A Lambda Calculus for Quantum Computation

6.1. The Language

6.2. Operational Semantics

6.2.1. Abstract Machine

6.2.2. Evaluation Strategy

6.2.3. Probabilistic Reduction Systems

6.2.4. Reduction System

6.3. Type System

6.3.1. Types

6.3.2. Typing Rules

6.4. Properties of the Type System
CONTENTS

6.4.1 Safety Properties .................................................. 62
6.4.2 Type Inference Algorithm ....................................... 63
6.5 Examples of Algorithms ........................................... 64
   6.5.1 The Deutsch Algorithm ....................................... 64
   6.5.2 The Teleportation Procedure ................................ 64
   6.5.3 Type Derivation of the Teleportation Protocol ........... 65
   6.5.4 Reduction of the Teleportation Term ....................... 67
   6.5.5 Reduction of the Superdense Coding Term ................ 68
6.6 Towards a Denotational Semantics ................................. 69

7 The Linear Fragment .................................................. 70
   7.1 A Linear Lambda Calculus for Quantum Computation ....... 70
   7.2 Operational Semantics ........................................... 75
      7.2.1 Small Step Semantics ..................................... 75
      7.2.2 Safety Properties ......................................... 77
      7.2.3 Normalization .............................................. 79
      7.2.4 Quantum Context and Reduction ......................... 81
      7.2.5 Reduction to Values ...................................... 82
   7.3 Denotational Semantics .......................................... 83
      7.3.1 Modeling the Linear Quantum Lambda Calculus ........ 83
      7.3.2 Fullness of the First-Order Fragment ................... 89
      7.3.3 Fullness up to Scalar Multiple .......................... 91
   7.4 Equivalence Classes of Terms ................................... 94
      7.4.1 Axiomatic Equivalence .................................... 94
      7.4.2 Operational Context ...................................... 95
      7.4.3 Operational Equivalence ................................ 95
      7.4.4 Denotational Equivalence ................................ 96
   7.5 Soundness and Full Abstraction ................................ 96
      7.5.1 Proof of the Soundness Theorem ......................... 97
      7.5.2 Full Abstraction: Preliminary Lemmas ................. 97
      7.5.3 Proof of the Full Abstraction Theorem ................ 98

8 Structure of the Linear-Non-Linear Fragment ....................... 99
   8.1 Computations and Values ....................................... 99
   8.2 Duplicability Versus Non-Duplicability ....................... 100
      8.2.1 Computations as Proofs .................................. 100
   8.3 Structure of the Exponential .................................. 100
      8.3.1 Idempotency .............................................. 100
      8.3.2 Coherence Property for Idempotent Comonads .......... 101
      8.3.3 Duplicable Pairs and Pairs of Duplicable Elements ... 107
   8.4 Linear Category for Duplication ............................... 107

9 A Computational Lambda Calculus for Duplication ................. 109
   9.1 An Indexed Lambda Calculus .................................. 109
      9.1.1 Type System ............................................... 109
      9.1.2 Terms .................................................... 110
      9.1.3 Typing Judgements ....................................... 111
      9.1.4 Type Casting and Substitution Lemma ................. 116
   9.2 Equational Logic of Typed Terms ................................ 123
   9.3 The Category \( \mathbb{C} \) ........................................... 128
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3.1</td>
<td>Monoidal Structure</td>
<td>129</td>
</tr>
<tr>
<td>9.3.2</td>
<td>Monadic Structure</td>
<td>139</td>
</tr>
<tr>
<td>9.3.3</td>
<td>Comonadic Structure</td>
<td>145</td>
</tr>
<tr>
<td>9.3.4</td>
<td>The Category $\mathcal{C}_\lambda$ is a Linear Category for Duplication</td>
<td>147</td>
</tr>
<tr>
<td>10     Proof of Theorem 9.2.7</td>
<td>148</td>
<td></td>
</tr>
<tr>
<td>10.1</td>
<td>A Handy Tool: Neutral Terms</td>
<td>148</td>
</tr>
<tr>
<td>10.2</td>
<td>Term Rewriting System Number One</td>
<td>152</td>
</tr>
<tr>
<td>10.3</td>
<td>Term Rewriting System Number Two</td>
<td>158</td>
</tr>
<tr>
<td>10.3.1</td>
<td>The Rewriting System</td>
<td>158</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Height of Terms</td>
<td>160</td>
</tr>
<tr>
<td>10.3.3</td>
<td>Degree of Terms</td>
<td>161</td>
</tr>
<tr>
<td>10.3.4</td>
<td>Last Notion of Measure: Number of a Term</td>
<td>163</td>
</tr>
<tr>
<td>10.3.5</td>
<td>Putting Everything Together</td>
<td>164</td>
</tr>
<tr>
<td>10.4</td>
<td>Proof of Theorem 9.2.7</td>
<td>172</td>
</tr>
<tr>
<td>11     Categorical Semantics</td>
<td>174</td>
<td></td>
</tr>
<tr>
<td>11.1</td>
<td>Denotational Semantics</td>
<td>174</td>
</tr>
<tr>
<td>11.1.1</td>
<td>Interpretation of the Type System</td>
<td>174</td>
</tr>
<tr>
<td>11.1.2</td>
<td>Interpretation of the Language</td>
<td>174</td>
</tr>
<tr>
<td>11.2</td>
<td>Soundness of the Denotation</td>
<td>182</td>
</tr>
<tr>
<td>11.3</td>
<td>Completeness</td>
<td>198</td>
</tr>
<tr>
<td>11.4</td>
<td>Towards a Denotational Model</td>
<td>200</td>
</tr>
</tbody>
</table>

Bibliography | 201  |

Index | 207  |
List of Figures

3.1 The Bloch sphere .......................................................... 22
3.2 Quantum teleportation protocol ........................................ 28
3.3 Dense coding protocol ...................................................... 30
4.1 The ORAM model ............................................................. 35
### List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Rules for constructing quantum flow-charts</td>
<td>38</td>
</tr>
<tr>
<td>5.1</td>
<td>Intuitionistic logic: natural deduction rules</td>
<td>46</td>
</tr>
<tr>
<td>5.2</td>
<td>Interpretation of the simply typed lambda calculus</td>
<td>48</td>
</tr>
<tr>
<td>6.1</td>
<td>Reductions rules of the quantum lambda calculus</td>
<td>60</td>
</tr>
<tr>
<td>6.2</td>
<td>Typing rules</td>
<td>62</td>
</tr>
<tr>
<td>7.1</td>
<td>Typing rules for the linear quantum lambda calculus</td>
<td>71</td>
</tr>
<tr>
<td>7.2</td>
<td>Reduction rules for the linear quantum lambda calculus</td>
<td>76</td>
</tr>
<tr>
<td>7.3</td>
<td>Denotational semantics for typing judgements</td>
<td>84</td>
</tr>
<tr>
<td>7.4</td>
<td>Axiomatic equivalence</td>
<td>94</td>
</tr>
<tr>
<td>9.1</td>
<td>Typing rules for the linear-non-linear quantum lambda calculus</td>
<td>111</td>
</tr>
<tr>
<td>9.2</td>
<td>Axiomatic equivalence axioms: beta-eta-rules</td>
<td>124</td>
</tr>
<tr>
<td>9.3</td>
<td>Axiomatic equivalence axioms: computation rules</td>
<td>124</td>
</tr>
<tr>
<td>9.4</td>
<td>Axiomatic equivalence: derived rules</td>
<td>125</td>
</tr>
<tr>
<td>9.5</td>
<td>Definitions of maps and operations on maps in $\mathcal{C}$</td>
<td>147</td>
</tr>
<tr>
<td>11.1</td>
<td>Interpretation of core values</td>
<td>177</td>
</tr>
<tr>
<td>11.2</td>
<td>Interpretation of extended values</td>
<td>178</td>
</tr>
<tr>
<td>11.3</td>
<td>Interpretation of computations</td>
<td>179</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Quantum computation is a paradigm of computation where information is potentially non-local, can be non-duplicable, and for which one of the core features is inherently probabilistic. However, using quantum computation, numerous hard problems, such as factoring, can be performed efficiently. Higher-order computation brings new light on these algorithms, but raises several challenging problems such as dealing with non-duplicable functions, or marrying duplicability and probabilistic behavior. By taking the problem both at the concrete level of completely positive maps and at the abstract level of categorical structures, this thesis addresses the issue of the semantics of higher-order quantum computation.

Background

Quantum computation. While classical computation uses data encoded on objects governed by the laws of classical physics, quantum computation uses data encoded on the state of particles governed by the laws of quantum physics. The basic unit of data in quantum computation is a quantum bit, which can be modeled by a normalized vector in a 2-dimensional Hilbert space $\mathcal{H}$. Choosing an orthonormal basis $\{|0\rangle, |1\rangle\}$, one can consider $|0\rangle$ and $|1\rangle$ as vectors of information, leading to potential superposition of information. The state of a system of two or more quantum bits is a normalized vector in $\mathcal{H} \otimes \mathcal{H} \otimes \ldots \otimes \mathcal{H}$. The permissible operations on quantum bits are determined by the laws of quantum physics. The only possible operations are initializations, unitary operations and measurements (and combinations thereof). Here, measurement is an operation that sends a quantum bit in state $\alpha|0\rangle + \beta|1\rangle$ to $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$, while simultaneously returning a Boolean 0 or 1, respectively.

Shor [1994] has shown that quantum computers can factor an integer in a time that is polynomial in its number of digits. It is not known whether any classical algorithm can solve the problem in polynomial time. The factoring problem has numerous implications in cryptography. This discovery has focused attention on quantum computing. Quantum computing is also able to bring change in other domains, such as database manipulation, with algorithms to query elements in databases, and such as numerical methods, with the ability to perform Fourier transform efficiently [Nielsen and Chuang 2002].

From the point of view of quantum programming languages, there are several features of quantum computation that deserve special attention. First, unlike classical data, quantum data cannot in general be duplicated: there is no map $(\alpha|0\rangle + \beta|1\rangle) \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$. This is known as the “no-cloning theorem” [Wootters and Zurek 1982]. Second, quantum data can be entangled: Consider the two-quantum bit state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Although one can speak of “quantum
Semantics of programming languages. When dealing with a programming language, an important question is how to describe the behavior of programs, and to characterize the set of possible behaviors. A semantics [Pierce 2002] for a programming language serves as a description of properties that valid programs satisfy. This permits to get insights into the capabilities of the language and the logic underlying it. This can help for example in understanding the power and the limitations of the computational paradigm considered, or more pragmatically to build automated tools to check for the validity of a piece of code, along a set of specifications.

An operational semantics is a description of how valid programs behave by sequences of computational steps. Depending on the programming language considered, this can take the form of a rewriting system of the code itself (in the case, for example, of the simply-typed lambda calculus), or it can be more involved and require the description of an abstract machine (as, for example, in the case of the Turing machine).

An axiomatic semantics is a description of local syntactic equivalences of code. The goal is to provide an equational logic of programs, in order to exhibit general syntactic properties of the language. It is helpful to describe a system of normal forms in which every program can be rewritten. An important property of an axiomatic semantics is soundness. We say that an axiomatic semantics is sound if two axiomatically equivalent programs are operationally equivalent.

A denotational semantics is built by drawing a parallel between the programs in the language and a mathematically structured set. The properties of the language are understood as mathematical and logical properties, giving a handle to answer questions about the language. A very strong property for a denotational semantics is full abstraction: the semantics is fully abstract when any two programs have the same denotation precisely when they are operationally equivalent in every context. When the interpretation is also onto, the denotation is fully complete.

Sometimes, at first it is only possible to describe the axiomatic structure of the language. In this situation, by studying the relations between pieces of code it can be possible to describe the categorical structure underlying the logic and infer a categorical semantics.

Higher-order computation and lambda calculus. An essential paradigm in computation is higher-order computation. A higher-order function is a function that inputs or outputs a “black box”, which is itself a function. The canonical formalism for expressing higher-order functions is the lambda calculus developed by [Church 1936 and Kleene 1935a,b] to characterize computable functions. This endeavour was shown [Turing 1936] to have the same computational power as Turing machines.

The lambda calculus not only permits the design of all computable functions, but it also allows one to draw a correspondence between proofs in logic and programs. This correspondence, known as the Curry-Howard isomorphism [Girard et al. 1990], is the one of the main tools used for passing from an axiomatic semantics to a categorical semantics [Lambek and Scott 1989]. It is thus a powerful handle to grasp the structure behind potentially intricate computational schemes.

Pure and impure lambda calculus. In its most general formulation, the lambda calculus is called pure, or purely functional. This means that programs are completely determined by their output result on each possible input. It is fairly restrictive and unfortunately rules out many interesting side effects, such as non-determinism, probabilistic outcomes, or input-outputs. To give a semantics to languages with side-effects, [Moggi 1989, 1991] defines a lambda calculus, the computational lambda calculus, where two classes of terms are considered: the values and the computations. Using
an axiomatic equivalence and some categorical tools, he describes a general model of computations with side effects.

**Semantics of Quantum Programming Languages**

Besides a few existing algorithms, quantum computation is a relatively fresh area of research with no single best way of thinking about the processes in play. Understanding the semantics of quantum programming languages is therefore a useful tool in understanding the capabilities of quantum computation and for deciding on the most appropriate form to use as a computational scheme. Being in the intersection of physics, computer science and mathematics, several paradigms to process quantum computation exist, and a wide ranges of approaches are studied (Gay, 2006).

Some studies focus primarily on the unitary evolution of the quantum states, and view measurement as a meta-operation outside of the formalism. Benioff (1980) and Deutsch (1985) built a quantum Turing machine, where the tape, the head and the states are encoded as quantum information. Van Tonder (2003, 2004) described a lambda calculus encoded on strings of quantum bits. Altenkirch and Grattage (2005a, b) studied a first order functional language with a notion of quantum test compiling into a quantum circuit.

Other approaches consider measurements as the driving force in the computation. This is the one-way model of Raussendorf and Briegel (2001), further extended with an axiomatic and a denotational semantics in (Danos et al., 2007).

It is also possible to see measurements as an active part in the computation and to allow interleaved unitary operations and measurements. One example is the QRAM model of Knill (1996) and Bettelli et al. (2003). Here, a quantum computer consists of a classical computer with a quantum device attached to it. In this configuration, called “classical control” (Selinger, 2004a), the operation of the machine is controlled by a classical program which emits a sequence of instructions to the quantum device for performing measurements and unitary operations. Several programming languages have been proposed to deal with such a model, see for example the works of Sanders and Zuliani (2000), Bettelli et al. (2003), Selinger (2004b).

The denotational aspect of quantum computation has been studied in various ways. A first trend of research, started by Abramsky and Coecke (2004), focuses on the basic structures required for performing quantum computation, using a categorical framework. This work gave birth to a range of publications, such as Coecke (2004), Coecke and Pavlovic (2007), Selinger (2005) and Coecke and Paquette (2006). Other approaches focus on the description of quantum computation in term of superoperators. Selinger (2004b) defines a flow-chart language and provides a fully complete semantics for the language in term of superoperators. Selinger (2004d) is an attempt to generalize this semantics at higher-order, by looking for a suitable category of normed vector spaces. However, none of the studied descriptions capture the required structure. Another related work is the one of Girard (2004), describing a model of linear logic in terms of normed vector spaces. However, although being a *-autonomous category, it does not yield the correct answer at base types, as pointed out by Selinger (2004e).

**A Lambda Calculus for Quantum Computation**

Selinger and Valiron (2006a, 2005) and Valiron (2004a, b) developed a higher-order language for quantum computation. The language is a typed lambda calculus together with classical and quantum data, featuring creations of quantum bits, measurements and unitary operations. For example, in such a language one can build a function that inputs a Boolean and returns a function from quantum bits to quantum bits based on the input bit.
The first important feature built into the language is the distinction between duplicable and non-duplicable elements. This arises from the no-cloning property of quantum computation. So if \( x: \text{qbit} \) is a variable representing a quantum bit, and \( y: \text{bit} \) is a variable representing a classical bit, then it is legal to write \( f(y, y) \), but not \( g(x, x) \). In order to keep track of duplicability at higher-order types we use a type system based on linear logic [Girard, 1987]. We use the duplicability operator “!” to mark classical types.

The second feature of quantum computation included in the language is the probabilistic nature of the measurement. This was taken care of by defining an abstract machine together with an operational semantics in the form of a call-by-value reduction strategy.

The most significant results of [Valiron, 2004a] were the proof that the type system prevents a typed program from ending up in an error state, and the description a type inference algorithm for deciding whether a given program is typeable or not.

### Semantics for Higher-Order Quantum Computation

We now turn to the question of a semantics for the quantum lambda calculus of [Valiron, 2004a].

As explained before, we use the duplicability operator “!” to mark classical types. In the categorical semantics, this operator gives rise to a comonad as in the work of Seely [1989] and Benton et al. [1992]. Another account of mixing copyable and non-copyable data is Coecke and Pavlovic [2007], where the copyability is internal to objects. However, it is not clear whether this approach scales well to higher order.

To model the probabilistic effect of the measurement operator in our call-by-value setting, our semantics requires a computational monad in the sense of Moggi [1991]. The coexistence of the computational monad and the duplicability comonad in the same category is what makes our semantics interesting and novel. It differs from the work of Benton and Wadler [1996], who considered a monad and a comonad one two different categories, arising from a single adjunction.

The computational aspects of linear logic have been extensively explored by many authors, including Abramsky [1993], Benton et al. [1992, 1993], Bierman [1993], and Wadler [1992]. However, these works contain explicit lambda terms to witness the structural rules of linear logic, for example, \( x : !A \triangleright \text{derelict}(x) : A \). By contrast, in our language, structural rules are implicit at the term level, so that \( !A \) is regarded as a subtype of \( A \) and one writes \( x : !A \triangleright x : A \). As it was shown in Selinger and Valiron [2006a], linearity information can automatically be inferred by the type checker. This allows the programmer to program as in a regular non-linear language.

This use of subtyping is the main technical complication in our proof of well-definedness of the semantics. This is because one has to show that the denotation is independent of the choice of a potentially large number of possible derivations of a given typing judgement. We are forced to introduce a Church-style typing system, and to prove that the semantics finally does not depend on the additional type annotations.

Another technical choice we made in our language concerns the relation between the exponential “!” and the pairing operation. Linear logic only requires \( !A \otimes !B \triangleright !(A \otimes B) \) and not the opposite implication. However, in our programming language setting, we find it natural to identify a classical pair of values with a pair of classical values, and therefore we will have an isomorphism \( !A \otimes !B \cong !(A \otimes B) \).

### Plan of the Thesis

The content of the thesis is summarized as follows.

In Chapter 2, we state the notions of category theory used in the thesis. In Chapter 3, we give a brief overview of quantum computation, and we describe in Chapter 4 the works in the
literature concerned with the semantics of quantum programming languages. In particular, we detail in Section 4.3 the flow-chart language of Selinger (2004b) and its semantics in term of superoperators, used in Chapter 4.

The last chapter on general background is Chapter 5 giving a brief introduction on lambda calculus and its categorical interpretation. We review the simply-typed lambda calculus, its computational extension for dealing with side-effects, and the computational interpretation of intuitionistic linear logic. Chapter 6 summarizes of the results contained in Valiron (2004a). The quantum lambda calculus that will be referred to all along the remainder of the thesis is defined here, together with its type system and its operational semantics.

The next chapters are the main contribution of this thesis. Chapter 7 contains a precise study of the linear fragment of the quantum lambda calculus. This fragment is typed, its operational semantics is described in the same way as in Chapter 6 and a denotational semantics in term of completely positive maps is provided. Using the fact that the semantics is full at first order, the semantics is proved to be fully abstract.

Chapter 8 raises the issue of the structure of the full language. Using Moggi’s computational model and Bierman’s linear categories, a categorical structure candidate for being a model of the language, called linear category for duplication is provided.

Chapter 9 describes a version of the quantum lambda calculus stripped from the classical and the quantum Boolean structure. The language is reduced to its core features, namely the distinction between linearity and non-linearity, the higher-order, the pairing and the computational aspect. An axiomatic semantics is described, yielding a syntactic category that is proved to be a linear category for duplication. The result requires Theorem 9.2.7, whose proof requires some technical machinery. Chapter 10 explains this machinery: We introduce two rewriting systems. They converge to a special class of terms, called the neutral terms, for which the theorem is trivial. The main difficulty is to prove a weak-normalization result for these rewriting systems. We use techniques from Girard et al. (1990, Ch. 4) by defining a well-founded measure of convergence, decreasing with each reduction of the rewriting system.

Chapter 11 develops the interpretation of the computational lambda calculus for duplication into a general linear category for duplication, and the proof that the interpretation is sound and complete.
Chapter 2

Notions of Category Theory

In this chapter we give a brief exposition of the definitions and results of category theory used in the remainder of the thesis. For a complete introduction to category theory, \textit{Mac Lane 1998} is a solid reference. An approach to category theory oriented towards semantic aspects of computation can be found in \textit{Lambek and Scott 1989}.

2.1 Categories and Functors

The content of this section follows \textit{Lambek and Scott 1989}.

**Definition 2.1.1.** A category \( C \) consists of the following three elements.

- A class of \textit{objects}, denoted by \(|C|\).
- A class of \textit{morphisms}. To each morphism \( f \) is associated a domain \( A \) and a codomain \( B \), where \( A, B \) are objects. We say \( f \) is a morphism (or an \textit{arrow}, or a \textit{map}) from \( A \) to \( B \) and we write \( f : A \to B \). For any given \( A \) and \( B \), we define the homset of \( A \) to \( B \) as the class of morphisms from \( A \) to \( B \), and we denote it \( \text{hom}_C(A, B) \), \( \text{hom}_C(A, B) \), or \( \text{hom}(A, B) \) if there is no ambiguity.
- For each \( A \) there is a special morphism \( \text{id}_A : A \to A \), called the \textit{identity}.
- A binary operator \( \circ \) called \textit{composition} such that if \( f : A \to B \) and \( g : B \to C \) are morphisms, then \( g \circ f : A \to C \) is a morphism. We will also write \( g \circ f \) as \( f ; g \).

The composition satisfies two properties: if \( f : A \to B \), \( g : B \to C \) and \( h : C \to D \) are morphisms, then

\[
(f; g); h = f; (g; h) \quad \text{and} \quad f; \text{id}_B = f = \text{id}_A; f.
\]

We say that the category is \textit{locally small} if for all objects \( A, B \) the class \( \text{hom}(A, B) \) is a set. We say it is \textit{small} if moreover the class of objects is a set.

**Definition 2.1.2.** We say that a morphism \( f : A \to B \) in a category \( C \) is an \textit{isomorphism} if there exists a morphism \( f^{-1} : B \to A \) such that \( f; g = \text{id}_A \) and \( g; f = \text{id}_B \).

**Example 2.1.3.** The trivial category \( 1 \). Its class of objects is the singleton \( \{\ast\} \) and its unique arrow is the identity on \( \ast \). Composition is defined trivially.

**Example 2.1.4.** The category \( \text{Set} \) of sets. Its objects are arbitrary sets and its morphisms arbitrary mappings between sets.
Example 2.1.5. Given a category $C$, the opposite category $C^{\text{op}}$ consisting of the objects of $C$ and the arrows of $C$ in “opposite” direction: $f$ is an arrow from $B$ to $A$ in $C^{\text{op}}$ if and only if $f : A \to B$ is an arrow of $C$. We write $f^{\text{op}}$ for the arrow in $C^{\text{op}}$ corresponding to $f$ in $C$.

Example 2.1.6. Given two categories $C$ and $D$ one defines a category $C \times D$ with the following data.

- Objects are pairs $(A, B)$ where $A \in |C|$ and $B \in |D|$.
- An arrow $(A, B) \to (C, D)$ is a pair of arrows $(f : A \to C, g : B \to D)$, where $f \in C$ and $g \in D$.
- The identity arrow $id_{A,B}$ is the pair $(id_A, id_B)$.
- The composition of two maps $(f, f') : (A, A') \to (B, B')$ and $(g, g') : (B, B') \to (C, C')$ is the map $(f; g, f' ; g') : (A, A') \to (C, C')$.

Definition 2.2.1. Given two categories $C$ and $D$, a functor $F$ from $C$ to $D$ is a map from $|C|$ to $|D|$ and from $\text{hom}_C(A, B)$ to $\text{hom}_D(FA, FB)$ for all $A, B$ in $C$ preserving identities and composition:

$$F(id_A) = id_{FA} \quad \text{and} \quad F(f \circ g) = Ff \circ Fg.$$  

A functor $F : C \to D$ is full if for all objects $A$ and $B$ of $C$ the map

$$F_{A,B} : \text{hom}_C(A, B) \to \text{hom}_D(FA, FB)$$  

is surjective. The functor $F$ is faithful if the maps $F_{A,B}$ are injective, and fully faithful if they are bijective. A full embedding is a fully faithful functor that is also injective on objects.

Example 2.1.8. The diagonal functor on $C$ is the functor $\Delta_C : C \to C \times C$ sending $A$ to $(A, A)$ and $f$ to $(f, f)$. It is faithful but not in general full.

Example 2.1.9. The terminal functor on $C$ is the functor $\bigcirc_C : C \to \mathbf{1}$ sending every object on $\star$ and every morphism on $id_\star$. It is full but not in general faithful.

Example 2.1.10. Consider three categories $C$, $D$ and $E$.

1. Given a functor $F : C \to D$ and a functor $G : D \to E$, the map $GF : C \to E$ defined as the composition of $F$ and $G$ is also a functor.

2. The map $id_C : C \to C$ sending an object $A$ to itself and a map $f : A \to B$ to itself is the identity functor.

Definition 2.1.11. One defines the category $\mathbf{Cat}$ of small categories as the category where objects are small categories and morphisms are functors of small categories. The identity morphism on $C$ is the identity functor $id_C$ and the composition of arrows is the composition of functors.

### 2.2 Natural Transformations

The content of this section follows [Mac Lane 1998].

Definition 2.2.1. Given two functors $F, G : C \to D$, a natural transformation $n$ from $F$ to $G$, denoted as $n : F \to G$, is a collection of maps $n_A : FA \to GA$ in $D$ for each object $A$ of $C$ such that for all morphism $f : A \to B$ in $C$ the following diagram commutes:

$$
\begin{align*}
FA & \xrightarrow{n_A} GA \\
\downarrow_{Ff} & \quad \downarrow_{Gf} \\
FB & \xrightarrow{n_B} GB.
\end{align*}
$$
We say that a diagram commutes when for every two vertices $X,Y$ in the diagram, all the paths from $X$ to $Y$ (following arrows) yield equal morphisms. In this particular case, this means $n_A; Gf = Ff; n_B$. The diagrammatic notation for a natural transformation $n : F \Rightarrow G$ is

$$
\begin{array}{ccc}
F & \Rightarrow & G \\
\downarrow n & & \\
C & \Rightarrow & D
\end{array}
$$

(2.2.1)

We say that a natural transformation $n$ is a natural isomorphism if for all objects $A$ the map $n_A$ is an isomorphism.

**Definition 2.2.2.** Given three functors $F,G,H : \mathcal{C} \to \mathcal{D}$ and two natural transformations $m : F \Rightarrow G$ and $n : G \Rightarrow H$, one defines the composition $m; n : F \Rightarrow H$ as the collection of maps $m_A; n_A : FA \to HA$. One defines the identity on $F$ as the collection of arrows $id_{FA} : FA \to FA$.

**Definition 2.2.3.** Consider two categories $\mathcal{C}$ and $\mathcal{D}$. One defines the functor category $\text{Func}(\mathcal{C}, \mathcal{D})$, or $\mathcal{D}^{\mathcal{C}}$, as the category whose objects are functors $\mathcal{C} \to \mathcal{D}$ and arrows natural transformations $F \Rightarrow G$, where $F,G : \mathcal{C} \to \mathcal{D}$ are functors.

**Definition 2.2.4.** Consider four categories, four functors and one natural transformation in the following situation:

$$
\begin{array}{ccc}
A & \xrightarrow{F} & B \\
\downarrow n & \downarrow & \downarrow m \\
\Downarrow & & \\
\Downarrow & & \\
C & \xrightarrow{K} & D
\end{array}
$$

(2.2.2)

One defines the two natural transformations $nF : GF \Rightarrow HF$, $Kn : KG \Rightarrow KH$ as $(nF)_A = n_{FA}$ and $(Kn)_A = K(n_A)$.

**Lemma 2.2.5.** Consider the situation

$$
\begin{array}{ccc}
A & \xrightarrow{F} & B \\
\Downarrow & \Downarrow & \Downarrow \\
\Downarrow & \Downarrow & \\
\Downarrow & \Downarrow & \\
C & \xrightarrow{K} & D
\end{array}
$$

Then $K(nF) = (Kn)F$, $K(n;m) = (Kn; Km)$ and $(n;m)L = (nL; mL)$. □

**Definition 2.2.6 [Mac Lane, 1998, p. 93].** Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. We say that $\mathcal{C}$ and $\mathcal{D}$ are equivalent if there exists a pair of functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ together with natural isomorphisms $id_{\mathcal{C}} \cong G \circ F$ and $id_{\mathcal{D}} \cong F \circ G$. We say that $F$ and $G$ are equivalences of category.

### 2.3 Adjoint Functors

The following definitions and lemmas are taken directly from [Lambek and Scott, 1989, pp. 13–15]

**Definition 2.3.1.** An adjunction between categories $\mathcal{C}$ and $\mathcal{D}$ is given by a quadruple $(F,U,\eta,\epsilon)$, where $F : \mathcal{C} \to \mathcal{D}$ and $U : \mathcal{D} \to \mathcal{C}$ are functors and $\eta : id_{\mathcal{C}} \Rightarrow UF$ and $\epsilon : FU \Rightarrow id_{\mathcal{D}}$ are natural transformations such that $(\eta U) ; (U \epsilon) = id_U$ and $(F \eta) ; (\epsilon F) = id_F$. One says that $U$ is right adjoint to $F$, or that $F$ is left adjoint to $U$, and one calls $\eta$ the unit and $\epsilon$ the counit of the adjunction.
2.4. Products and Coproducts

Lemma 2.3.2. An adjunction \((F, U, \eta, \epsilon)\) between locally small categories \(C\) and \(D\) gives rise to and is determined by a natural isomorphism \(\tau\)

\[ \tau_{A,B} : D(FA, B) \cong C(A, UB). \]

between the two functors \(D(F-, -)\) and \(C(-, U-)\) of type \(C^{op} \times D \to \text{Set}\).

Lemma 2.3.3 (Uniqueness). Adjoint functors determine each other uniquely up to natural isomorphism.

Lemma 2.3.4 (Composition). Given the two following adjunctions:

\[ (F : C \to D, \ U : D \to C, \ \eta : id_C \Rightarrow UF, \ \epsilon : FU \Rightarrow id_D), \]
\[ (F' : D \to E, \ U' : E \to D, \ \eta' : id_D \Rightarrow U'F', \ \epsilon' : F'U' \Rightarrow id_E), \]

the quadruple

\[ (F'F : C \to E, \ \ UU' : E \to C, \ \eta U\eta' F : id_C \Rightarrow UU'F'F, \ \epsilon' F UU' \Rightarrow \epsilon F F') \]

is an adjunction between \(C\) and \(E\).

Definition 2.3.5. We say that the adjunction \((F'F, UU')\) of Lemma \(2.3.2\) is the composition of \((F, U)\) and \((F', U')\).

Remark 2.3.6. The new structure is an adjunction because the two equations of Definition \(2.3.1\) namely

\[ ((\eta U\eta' F)(UU')); ((UU')(F'\epsilon U'; \epsilon')) = id_{UU'}, \quad (2.3.1) \]
\[ ((F'F)(\eta U\eta' F)); ((F'\epsilon U'; \epsilon')(F'F)) = id_{F'F}, \quad (2.3.2) \]

are satisfied.

2.4 Products and Coproducts

Definition 2.4.1 [Mac Lane 1998]. An object \(T\) in a category \(C\) is called a terminal object if for each object \(A\) there exists a unique map \(\bigcirc_A : A \to T\).

Definition 2.4.2. An object \(\perp\) in a category \(C\) is called an initial object if for each object \(A\) there exists a unique map \(\Box_A : \perp \to A\).

Lemma 2.4.3 [Lambek and Scott 1989]. The category \(C\) has a terminal (respectively initial) object if and only if the functor \(\bigcirc_C : C \to 1\) has a right (respectively left) adjoint.

Definition 2.4.4 [Lambek and Scott 1989]. Given a category \(C\) and two objects \(A\) and \(B\), the product of \(A\) and \(B\) is, if it exists, the data consisting of an object \(A \times B\) and two maps \(\pi^1_{A,B} : A \times B \to A\) and \(\pi^2_{A,B} : A \times B \to B\), such that for all maps \(f : C \to A\) and \(g : C \to B\) there exists a unique map \((f, g) : C \to A \times B\) with the following equations holding for all \(h : C \to A \times B\):

\[ \langle f, g \rangle; \pi^1_{A,B} = f \quad (2.4.1) \]
\[ \langle f, g \rangle; \pi^2_{A,B} = g \quad (2.4.2) \]
\[ \langle h; \pi^1_{A,B}, h; \pi^2_{A,B} \rangle = h \quad (2.4.3) \]

We say that the category \(C\) has binary products if there is a product for all \(A\) and \(B\).
Definition 2.4.5 [Mac Lane 1998]. Given a category $\mathcal{C}$ and two objects $A$ and $B$ in $\mathcal{C}$, the coproduct of $A$ and $B$ is, if it exists, the data consisting of an object $A + B$ and two maps $i^!_{A,B} : A \rightarrow A + B$ and $i^\flat : B \rightarrow A + B$ such that for all maps $f : A \rightarrow C$ and $g : B \rightarrow C$ there exists a unique map $[f, g] : A + B \rightarrow C$ with the following equations holding for all $h : A + B \rightarrow C$:

\begin{align*}
  i^!_{A,B} [f, g] &= f \\
i^\flat [f, g] &= g \\
 [i^!_{A,B}; h, i^\flat_{A,B}; h] &= h
\end{align*}

We say that the category $\mathcal{C}$ has binary coproducts if there is a coproduct for all $A$ and $B$.

Lemma 2.4.6. Binary products (respectively binary coproducts) in a category $\mathcal{C}$ induce a functor $\times$ (respectively $+$): $\mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$.

Lemma 2.4.7 [Lambek and Scott 1989]. The category $\mathcal{C}$ has binary products (respectively binary coproducts) if and only if the functor $\Delta_C : \mathcal{C} \rightarrow \mathcal{C} \times \mathcal{C}$ has a right (respectively left) adjoint.

Definition 2.4.8 [Lambek and Scott 1989]. We say that a category $\mathcal{C}$ is cartesian if it has a terminal object $T$ and binary products $\times$. The category is cartesian closed if for all $A$ the functor $A \times (-)$ has a right adjoint $A \Rightarrow (-)$.

2.5 Monads

Definition 2.5.1 [Mac Lane 1998]. A monad over a category $\mathcal{C}$ is a triple $(T, \eta, \mu)$ where $T : \mathcal{C} \rightarrow \mathcal{C}$ is a functor, $\eta : \text{id} \Rightarrow T$ and $\mu : T^2 \Rightarrow T$ are natural transformations and the following diagrams commute:

\begin{align*}
  &\begin{array}{c}
    T^3 A \\
    \downarrow \mu_T A \\
    T^2 A \\
    \downarrow \mu_A \\
    TA
  \end{array} \\
  &\begin{array}{c}
    T^3 A \\
    \downarrow \mu_T A \\
    T^2 A \\
    \downarrow \mu_A \\
    TA
  \end{array}
\end{align*}

The natural transformation $\mu$ is called the multiplication of the monad and $\eta$ the unit of the monad.

Definition 2.5.2 [Manes 1976]. A Kleisli triple over a category $\mathcal{C}$ is a triple $(T, \eta, -^*)$ where $T : |\mathcal{C}| \rightarrow |\mathcal{C}|$, $\eta_A : A \rightarrow TA$ for all $A$ and $f^* : TA \rightarrow TB$ for all $f : A \rightarrow TB$, and the following equations hold:

\begin{align*}
  \eta^*_A &= \text{id}_{TA}, \\
  \eta_A ; f^* &= f \text{ for } f : A \rightarrow TB, \\
  f^* ; g^* &= (f ; g^*)^* \text{ for } f : A \rightarrow TB \text{ and } g : B \rightarrow TC.
\end{align*}

Lemma 2.5.3 [Manes 1976]. There is a one-to-one correspondence between Kleisli triples and monads.

Proof. Given a Kleisli triple $(T, \eta, -^*)$, we construct a monad $(T, \eta, \mu)$ by extending $T$ to arrows: $T(f) = (f ; \eta_B)^*$ for $f : A \rightarrow B$, and by defining $\mu_A = \text{id}_{TA}^*$. Conversely, given a monad $(T, \eta, \mu)$, $-^*$ is defined by $f^* = (Tf) ; \mu_B$ for $f : A \rightarrow TB$. \qed

Definition 2.5.4 [Manes 1976]. Given a Kleisli triple $(T, \eta, -^*)$ over $\mathcal{C}$, the Kleisli category $\mathcal{C}_T$ is defined as follows:

- the objects of $\mathcal{C}_T$ are the objects of $\mathcal{C}$,
2.6. Comonads

- the set \( C_T(A, B) \) of morphisms from \( A \) to \( B \) in \( C_T \) is \( C(A, TB) \),
- the identity on \( A \) is \( \eta_A : A \to TA \),
- The composition of \( f \in C_T(A, B) \) and \( g \in C_T(B, C) \) in \( C_T \) is \( f \circ g : A \to TC \).

**Lemma 2.5.5.** Consider a monad \((T, \mu, \eta)\) over a category \( C \). There is an adjunction

\[
\begin{tikzcd}
C \ar[rr,bend left] \ar[rr,bend right] & & C_T \\
\downarrow \ar[rr] & & \downarrow
\end{tikzcd}
\]

arising from the monad, where \( F(A) = A, U(A) = T(A) \), and \( F \) and \( U \) perform the following operations on morphisms:

\[
F : (A \xrightarrow{f} B) \mapsto (A \xrightarrow{f} B \xrightarrow{\eta_B} TB),
U : (A \xrightarrow{g} TB) \mapsto (TA \xrightarrow{g} TB).
\]

The unit \( \eta \) of the adjunction is the unit of the monad, and the counit \( \epsilon \) is the map \( TA \xrightarrow{id_T} TA \) in the category \( C \).

**Lemma 2.5.6.** Conversely, given an adjunction \((F, U, \eta, \epsilon)\), there is a canonical monad arising from it, by setting \( T = UF \). The unit of the monad is the unit of the adjunction, and the multiplication \( \mu \) of the monad is \( U\epsilon F : UFUF \to UF \).

2.6 Comonads

A dual notion to monad is the notion of comonad. We are going to use it extensively in the rest of the thesis.

**Definition 2.6.1** [Mac Lane, 1998]. A comonad in a category \( C \) is a tuple \((L, \epsilon, \delta)\) where \( L : C \to C \) is a functor and \( \epsilon : L \to I \) and \( \delta : L \to L^2 \) are natural transformations which render commutative the diagrams

\[
\begin{align*}
\begin{array}{ccc}
L^2 A & \xrightarrow{\delta} & L^3 A, \\
\downarrow{\delta_A} & & \downarrow{L\delta_A} \\
L^2 A & \xrightarrow{\delta_L A} & L^3 A,
\end{array}
\end{align*}
\]

By analogy with monads, we define the map \((-)_{\ast}\)

\[
f : LA \to B \\
f_{\ast} : LA \xrightarrow{\delta_B} L^2 A \xrightarrow{L} LB
\]

**Definition 2.6.2.** Given a comonad \((L, \epsilon, \delta)\) over a category \( C \), the co-Kleisli category \( C_L \) is defined as follows:

- the objects of \( C_L \) are the objects of \( C \),
- the set \( C_L(A, B) \) of morphisms from \( A \) to \( B \) in \( C_L \) is \( C(LA, B) \),
2.6. Comonads

- the identity on $A$ is $\epsilon_A : LA \to A$,
- The composition of $f \in C_L(A, B)$ and $g \in C_L(B, C)$ in $C_L$ is $f \circ g : LA \to C$.

**Definition 2.6.3.** Given a comonad $(L, \delta, \epsilon)$ on a category $C$, an $L$-coalgebra is a pair $(A, h_A : A \to LA)$ where $A$ is an object and $h_A$ is an arrow of $C$, such that both

\[ h_A \downarrow \quad \delta_A \downarrow \quad \epsilon_A \quad \downarrow \quad h_A \downarrow \quad \epsilon_A \]

commute. A morphism $f : (A, h_A) \to (B, h_B)$ of $L$-coalgebras is an arrow $f : A \to B$ of $C$ which renders commutative the diagram

\[ \begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow h_A & & \downarrow h_B \\
LA & \xrightarrow{Lf} & LB.
\end{array} \]

The category $C^L$ of $L$-coalgebras of $C$ is the category whose objects are $L$-coalgebras and whose maps are morphisms of $L$-coalgebras. It is called the co-Eilenberg-Moore category of the comonad $L$.

**Lemma 2.6.4.** Given a comonad $(L, \delta, \epsilon)$ on a category $C$, for each object $A$ in $C$ the pair $(LA, \delta_A : LA \to L^2A)$ forms a coalgebra. Given any map $f : A \to B$, the map $Lf : (LA, \delta_A) \to (LB, \delta_B)$ is a coalgebra map. \[ \square \]

**Lemma 2.6.5.** Given a category $C$ and a comonad $(L, \delta, \epsilon)$ on it, the coalgebra $(LA, \delta_A)$ has the following universal property: If $(X, h_X)$ is any $L$-coalgebra, and if $f : X \to A$ is any map in $C$, there exists a unique coalgebra map $f^\sharp : (X, h_X) \to (LA, \delta_A)$ such that

\[ \begin{array}{ccc}
LA & \xrightarrow{\epsilon_A} & A \\
\downarrow f^\sharp & & \downarrow f \\
X & \xrightarrow{f} & A.
\end{array} \]

Moreover, $f^\sharp = h_X \circ Lf$. \[ \square \]

**Corollary 2.6.6.** Given a category $C$ and a comonad $(L, \delta, \epsilon)$, there is a one-to-one correspondence between coalgebra morphisms $g : (LA, \delta_A) \to (LB, \delta_B)$ and maps of $C$ of the form $f : LA \to B$. \[ \square \]

**Definition 2.6.7.** The coalgebra $(LA, \delta_A)$ in Lemma 2.6.4 is called a (co)free coalgebra.

**Corollary 2.6.8.** There is a full embedding of $C_L$ into $C^L$ sending the object $A$ of $C_L$ to $(LA, \delta_A)$ and sending the morphism $f : LA \to B$ into $f \circ : LA \to LB$. \[ \square \]

**Lemma 2.6.9.** Given an adjunction $(F, U, \eta, \epsilon)$ there is a canonical comonad arising from it, by setting $T = FU$, the counit of the comonad is the counit of the adjunction, and the comultiplication $\delta$ of the comonad is $F\eta U : FUFU \to FU$. \[ \square \]
2.7 Symmetric Monoidal Categories and Comonoids

2.7.1 Monoidal Categories

Definition 2.7.1 (Mac Lane, 1998). A monoidal category $\mathcal{C}$ is a tuple $(\mathcal{C}, \otimes, \top, \alpha, \lambda, \rho)$ where $\mathcal{C}$ is a category, $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is a functor, $\top$ is an object of $\mathcal{C}$ and $\alpha, \lambda, \rho$ are three natural isomorphisms

$$\alpha_{A,B,C} : A \otimes (B \otimes C) \to (A \otimes B) \otimes C,$$

$$\lambda_A : \top \otimes A \to A,$$

$$\rho_A : A \otimes \top \to A$$

such that the diagrams

$$\begin{array}{c}
A \otimes (B \otimes (C \otimes D)) \\
\downarrow^{\text{id} \otimes \alpha} \\
A \otimes ((B \otimes C) \otimes D) \\
\downarrow_{\alpha \otimes \text{id}} \\
(A \otimes (B \otimes C)) \otimes D
\end{array}$$

and

$$\begin{array}{c}
A \otimes (\top \otimes C) \\
\downarrow^{\text{id} \otimes \lambda} \\
A \otimes C
\end{array}$$

commute. We call the category strict monoidal when $\alpha_{A,B,C}, \lambda_A$ and $\rho_A$ are identity morphisms.

Definition 2.7.2 (Mac Lane, 1998). A monoidal category is said to be symmetric when it is equipped with a natural isomorphism $\sigma_{A,B} : A \otimes B \to B \otimes A$ such that the diagrams

$$\begin{array}{c}
A \otimes B \\
\downarrow^{\sigma_{A,B}} \\
B \otimes A
\end{array}$$

and

$$\begin{array}{c}
A \otimes (B \otimes C) \\
\downarrow^{\text{id} \otimes \sigma} \\
A \otimes (C \otimes B)
\end{array}$$

commute.

2.7.2 Commutative Comonoids

Definition 2.7.3. In a symmetric monoidal category $\mathcal{C}$, a commutative comonoid object is an object $A$ of $\mathcal{C}$ equipped with two arrows $\hat{\Delta}_A : A \to \top$ and $\Delta_A : A \to A \otimes A$ such that the following diagrams commute

$$\begin{array}{c}
A \otimes (A \otimes A) \\
\downarrow_{\alpha} \\
(A \otimes A) \otimes A
\end{array}$$
A morphism \( f : (A, \Delta_A, \Delta_A) \to (B, \Delta_B, \Delta_B) \) of commutative comonoids is an arrow \( f : A \to B \) in \( C \) such that

\[
\begin{array}{ccc}
\Delta_A & \xrightarrow{f} & \Delta_B \\
\downarrow \rho_A & & \downarrow \rho_B \\
A & \xrightarrow{f} & B
\end{array}
\]

\[
\begin{array}{ccc}
\Delta_A & \xrightarrow{A} & \Delta_B \\
\downarrow \lambda_A & & \downarrow \lambda_B \\
A & \xrightarrow{A} & B
\end{array}
\]

\[
\begin{array}{ccc}
\Delta_A \otimes A & \xrightarrow{\sigma_{A-A}} & A \otimes A \\
\downarrow \Delta_A & & \downarrow \Delta_A \\
A & \xrightarrow{\Delta_A} & A
\end{array}
\]

\[
\begin{array}{ccc}
A & \xrightarrow{\triangle} & A \\
\downarrow \rho_A & & \downarrow \rho_A \\
A & \xrightarrow{\rho_A} & A
\end{array}
\]

Definition 2.7.4 [Selinger 2001]. We call a diagonal structure on a symmetric monoidal category \( (C, \otimes, T) \) a family \( \{(A, \Delta_A, \Delta_A)\}_{A \in |C|} \) of commutative comonoids that respects the symmetric monoidal structure of \( C \), that is, such that the following diagrams commute:

\[
\begin{array}{ccc}
A \otimes B & \xrightarrow{\Delta_A \otimes B} & (A \otimes A) \otimes (B \otimes B) \\
\downarrow \lambda_T & & \downarrow \lambda_T \\
T \otimes T & \xrightarrow{\lambda_T} & T
\end{array}
\]

\[
\begin{array}{ccc}
A \otimes B & \xrightarrow{\Delta_A \otimes B} & (A \otimes B) \otimes (A \otimes B) \\
\downarrow \lambda_T & & \downarrow \lambda_T \\
A \otimes B & \xrightarrow{\Delta_A \otimes B} & (A \otimes B) \otimes (A \otimes B)
\end{array}
\]

where \( sw \) is defined as the natural transformation constructed from \( \alpha \)'s and \( \sigma \)'s swapping the two middle objects, that is \( \alpha : (\alpha^{-1} \otimes id) ; (id \otimes \sigma) \otimes id) ; (\alpha \otimes id) ; \alpha^{-1} \).

Theorem 2.7.5 [Selinger 2001]. Let \( (C, \otimes, T, \alpha, \lambda, \rho, \sigma) \) be a symmetric monoidal category. It is a cartesian category if and only if there exist two natural transformations \( \Delta_A : A \to A \otimes A \) and \( \Delta_A : A \to T \) such that \( \{(A, \Delta_A, \Delta_A)\}_{A \in |C|} \) forms a diagonal structure. In this case the cartesian structure is given by

\[
\begin{align*}
\circ_A : A \xrightarrow{\triangle_A} T, & \quad (f, g) : C \xrightarrow{\Delta_C} C \otimes C \xrightarrow{f \otimes g} A \otimes B, \\
\pi^1_{A,B} : A \otimes B \xrightarrow{\Delta_A \otimes B} A \otimes T \xrightarrow{\rho_A} A, & \quad \pi^2_{A,B} : A \otimes B \xrightarrow{\Delta_A \otimes B} T \otimes B \xrightarrow{\lambda_B} B,
\end{align*}
\]

where \( f : C \to A \) and \( g : C \to B \). Given a cartesian structure, we construct the diagonal structure with \( \Delta_A = (id_A, id_A) \) and \( \Delta_A = \circ_A \).

\[\square\]

2.8 Monoidal Comonads and Coalgebras

This section is taken from [Eilenberg and Kelley 1965].

Definition 2.8.1. A (lax) monoidal functor \( F \) between two monoidal categories \( (C, \otimes, T) \) and \( (D, \otimes', T') \) consists of a functor \( F : C \to D \) together with two natural transformations

\[
\begin{align*}
d_{A,B}^F : FA \otimes' FB & \to F(A \otimes B), \\
d_{T}^F : T' & \to FT,
\end{align*}
\]
called coherence maps, with the following coherence equations:

\[
\begin{align*}
(FA \otimes' FB) \otimes' FC & \xrightarrow{\alpha'} FA \otimes' (FB \otimes' FC) \\
\llcorner_{A,B}^{\otimes'FC} & \llcorner_{A,B}^{\otimes'FC} \\
F(A \otimes B) \otimes' FC & \xrightarrow{\eta'} FA \otimes' F(B \otimes C) \\
\llcorner_{A,B,C}^{\otimes'FC} & \llcorner_{A,B,C}^{\otimes'FC} \\
F((A \otimes B) \otimes C) & \xrightarrow{F\alpha} F(A \otimes (B \otimes C)),
\end{align*}
\]

If the categories are symmetric, the functor is said to be lax symmetric monoidal if the following diagram also commutes:

\[
\begin{align*}
FA \otimes' \blacksquare & \xrightarrow{\rho} F\otimes' FA \\
\llcorner_{A,B}^{\otimes'\blacksquare} & \llcorner_{A,B}^{\otimes'\blacksquare} \\
F(A \otimes \blacksquare) & \xrightarrow{\eta} FA \otimes F(\blacksquare) \\
\llcorner_{A,B}^{\otimes'\blacksquare} & \llcorner_{A,B}^{\otimes'\blacksquare} \\
F((\blacksquare \otimes \bullet) \otimes \bullet) & \xrightarrow{\phi} F(\bullet \otimes (\blacksquare \otimes \bullet)).
\end{align*}
\]

We call the functor strong monoidal if the natural transformations \(\llcorner_{A,B}^{\otimes'FC}\) and \(\llcorner_{A,B}^{\otimes'\blacksquare}\) are isomorphisms.

**Theorem 2.8.2** (Mac Lane, 1998, p. 257). Any monoidal category \(C\) is categorically equivalent, via a strong monoidal functor \(F : C \rightarrow D\) and a strong monoidal functor \(G : D \rightarrow C\), to a strict monoidal category \(D\).

**Lemma 2.8.3.** Let \((C, \otimes, \tau_C), (D, \otimes_D, \tau_D)\) and \((E, \otimes_E, \tau_E)\) be symmetric monoidal categories.

1. The identity functor \(1_C : C \rightarrow C\) together with \(d^C_\otimes = id_{\tau_C} : \tau_C \rightarrow \tau_C\) and \(d^C_{A\otimes B} = id_{\tau_{A\otimes B}} : A \otimes_c B \rightarrow A \otimes_c B\) is a monoidal functor.

2. The functor \(\triangle_C\) from \(C\) to \(C\) sending \(A\) to \(\tau_C\) and \(f\) to \(id_{\tau_C}\) is monoidal, with
   \[
   d^C_{\triangle_C} = id_{\tau_C} : \tau_C \rightarrow \tau_C,
   \]
   \[
   d^C_{\triangle_{A,B}} = \lambda_{\tau_C} = \rho_{\tau_C} : \triangle_C A \otimes C B = \tau_C \otimes C \tau_C \rightarrow \tau_C = \triangle_C (A \otimes C B).
   \]

3. The diagonal functor \(\triangle_C\) from \(C\) to \(C\) sending \(A \otimes C A\) and \(f \otimes C f\) is monoidal with
   \[
   d^C_{\triangle_C} : T \xrightarrow{\lambda^{-1}_{\tau_C}} T \otimes T,
   \]
   \[
   d^C_{\triangle_{A,B}} : \triangle_C A \otimes \triangle_C B = (A \otimes A) \otimes (B \otimes B),
   \]
   \[
   (A \otimes C) \otimes (A \otimes B) = \triangle_C (A \otimes (C B)).
   \]

4. If \((F, d^F_{C}, d^F_{A,B}) : C \rightarrow D\) and \((G, d^G_{C}, d^G_{A,B}) : D \rightarrow E\) are any monoidal functor, so is \(G \circ F : C \rightarrow E\) together with
   \[
   d^{G \circ F}_{C} : \tau_E \xrightarrow{\tau_D} G \tau_D \xrightarrow{G \tau_C} GF \tau_C,
   \]
   \[
   d^{G \circ F}_{A,B} : GFA \otimes g FB \xrightarrow{d^G_{A,F} \circ d^F_{A,B}} G(FA \otimes_D FB) \xrightarrow{G \triangle_C} GF (A \otimes C B).
   \]

\[\square\]
Definition 2.8.4. In the setting of Definition 2.8.1, if \((F, d)\) and \((F', d')\) are two symmetric monoidal functors, we say that a natural transformation \(n : \mathcal{C} \to \mathcal{D}\) is monoidal if the following diagrams commute:

\[
\begin{align*}
F(A \otimes B) & \xrightarrow{n_{A \otimes B}} F'(A \otimes B), \\
F(A \otimes B) & \xrightarrow{n_{A \otimes B}} F'(A \otimes B),
\end{align*}
\]

Remark 2.8.5. The natural transformation \(n\) in Definition 2.8.4 could be called symmetric since the category is symmetric. However, since \(\sigma\) is not a structure but a property of monoidal functors, it does not yield any equation. In that sense the adjective “symmetric” does not apply to \(n\).

Definition 2.8.6. Let \((\mathcal{C}, \otimes, \top)\) be a (symmetric) monoidal category. A (symmetric) monoidal comonad on \(\mathcal{C}\) is a comonad \((L, \delta, \epsilon)\):

- equipped with two natural transformations \(d_{A,B} : LA \otimes LB \to L(A \otimes B)\) and \(d_\top : L\top \to \top\) making \((L, d)\) a lax (symmetric) monoidal functor,
- such that \(\delta\) and \(\epsilon\) are monoidal natural transformations, i.e. such that the following diagrams commute:

\[
\begin{align*}
LA \otimes LB & \xrightarrow{d_{A,B}} L(A \otimes B), \\
A \otimes B & \xrightarrow{\epsilon_A \otimes \epsilon_B} A \otimes B,
\end{align*}
\]

\[
\begin{align*}
L(A \otimes B) & \xrightarrow{\delta_{A,B}} L(A \otimes B), \\
A \otimes B & \xrightarrow{\epsilon_{AB \otimes A}} A \otimes B,
\end{align*}
\]

\[
\begin{align*}
L^2A \otimes L^2B & \xrightarrow{d_{LA,LB}} L(LA \otimes LB), \\
L^2(A \otimes B) & \xrightarrow{\delta_{AB \otimes A}} L^2(A \otimes B),
\end{align*}
\]

Theorem 2.8.7. Let \((\mathcal{C}, \otimes, \top)\) be a symmetric monoidal category with structure \(\alpha, \lambda, \rho\) and \(\sigma\). Let \((L, \delta, \epsilon, d)\) be a symmetric monoidal comonad on \(\mathcal{C}\). Then the co-Eilenberg-Moore category \(\mathcal{C}^L\) is also symmetric monoidal when equipped with

- the functor \(\otimes' : \mathcal{C}^L \times \mathcal{C}^L \to \mathcal{C}^L\), defined as \((A, h_A) \otimes' (B, h_B) = (A \otimes B, (h_A \otimes h_B); d_{A,B})\) on objects and \(f \otimes' g = f \otimes g\) on arrows.
- the unit object \(\top' = (\top, d_\top)\),
- the structure maps

\[
\begin{align*}
\alpha'_{(A,h_A), (B,h_B), (C,h_C)} & = \alpha_{A,B,C}, \\
\sigma'_{(A,h_A), (B,h_B)} & = \sigma_{A,B}, \\
\lambda'_{(A,h_A)} & = \lambda_A, \\
\rho'_{(A,h_A)} & = \rho_A.
\end{align*}
\]

Definition 2.8.8. In Theorem 2.8.7 we call \(\otimes'\) the induced tensor and \((\otimes', \top', \alpha, \lambda, \rho, \sigma)\) the induced symmetric monoidal structure. We identify \(\otimes'\) with \(\otimes\) and \(\top'\) with \(\top\).
Chapter 3

Quantum Computation

Whether the notion of data is thought of concretely or abstractly, it is usually supposed to behave classically: a piece of data is supposed to be clonable, erasable, readable as many time as needed, and is not supposed to change when left untouched.

Quantum computation is a paradigm where data can be encoded with a medium governed by the law of quantum physics. Although only rudimentary quantum computers have been built so far, the laws of quantum physics are mathematically well described. It is therefore possible to try to understand the capabilities of quantum computation, and quantum information turns out to behave substantially differently from usual (classical) information.

In this chapter we will describe the mathematics needed for quantum computation, and we will have a brief overview of the theory of quantum computation. A more complete study of the subject can be found in (Nielsen and Chuang, 2002) and in (Preskill, 1999).

3.1 Mathematical Formalism

This section will cover the common wisdom we need about Hilbert spaces and their operators. All considered vector spaces are assumed to be finite-dimensional. For a more complete mathematical analysis of the subject, see e.g. (Lang, 1993, Ch. V).

3.1.1 Generalities on Finite Dimensional Hilbert Spaces

Definition 3.1.1 [Lang, 1993, p. 95]. Let $E$ be a finite-dimensional vector space over the complex numbers $\mathbb{C}$. A sesquilinear form on $E$ is a map $\phi : E \times E \rightarrow \mathbb{C}$, which is linear in $y$: $\phi(x, \alpha y + \beta z) = \alpha \phi(x, y) + \beta \phi(x, z)$, and semi-linear in $x$: $\phi(\alpha x + \beta t, y) = \overline{\alpha} \phi(x, y) + \beta \phi(x, t)$, where $\overline{\alpha}$ is the complex conjugation of $\alpha$: $\overline{a + bi} = a - bi$, for $a, b \in \mathbb{R}$. We say the form is hermitian if moreover $\phi(x, y) = \overline{\phi(y, x)}$. It is positive definite if $\phi(x, x) \geq 0$ with equality if and only if $x = 0$. If a form is hermitian and positive definite, we will call it a scalar product. In this case we often denote it as $\langle.,.\rangle$.

Definition 3.1.2. Let $E$ be a complex vector space. A norm on $E$ is a map $\|\| : E \rightarrow \mathbb{R}$ such that

1. $\|v\| \geq 0$ for all $v$, with equality if and only if $v = 0$;
2. $\|\alpha v\| = |\alpha| \|v\|$;
3. $\|v + w\| \leq \|v\| + \|w\|$.
3.1. Mathematical Formalism

Lemma 3.1.3. Given a scalar product $\langle \cdot,\cdot \rangle$ on a complex vector space $\mathcal{E}$, the map $\|\cdot\| : \mathcal{E} \to \mathbb{C}$ mapping $v$ to $\sqrt{\langle v|v \rangle}$ is a norm.

Definition 3.1.4. Given a scalar product on a complex vector space $\mathcal{E}$. The norm in Lemma 3.1.3 is called the induced norm.

Definition 3.1.5. A vector space together with a norm is called a normed vector space.

Definition 3.1.6. Let $\mathcal{H}$ be a finite dimensional vector space over the field $\mathbb{C}$ of complex numbers. The space $\mathcal{H}$ is a Hilbert space if it comes equipped with a scalar product. When speaking about a given Hilbert space, we will always consider it to be normed by the induced norm.

Definition 3.1.7. An operator $A$ on a Hilbert space $\mathcal{H}$ is a linear map $A : \mathcal{H} \to \mathcal{H}$. A functional on $\mathcal{H}$ is a linear map $\lambda : \mathcal{H} \to \mathbb{C}$. The space of functionals on $\mathcal{H}$ is denoted by $\mathcal{H}^*$. 

Lemma 3.1.8. Let $\lambda$ be a functional on $\mathcal{H}$. Then there exists $x_0 \in \mathcal{H}$ such that for all $y \in \mathcal{H}$, $\lambda(y) = \langle x_0|y \rangle$.

Lemma 3.1.9. Let $\phi$ be a sesquilinear form on a Hilbert space $\mathcal{H}$. Then the map $\lambda_x : y \mapsto \phi(x,y)$ is a functional.

Let $A$ be an operator on $\mathcal{H}$. Define $\phi_A$ by $\phi_A(x,y) = \langle x|Ay \rangle$. Then $\phi_A$ is a sesquilinear form on $\mathcal{H}$. For each $x$, $\lambda_x(y) = \phi_A(x,y)$ is a functional. Therefore there exists some $x_0$ such that $\lambda_x(y) = \langle x_0|y \rangle$. Define $A^*$ as $A^*x = x_0$: we have $\langle x|Ay \rangle = \langle A^*x|y \rangle$.

Definition 3.1.10. One calls $A^*$ the adjoint of $A$. If $A = A^*$, we say $A$ is self-adjoint, or hermitian.

Lemma 3.1.11 (Lang, 1993, p. 106). The map $A \mapsto A^*$ satisfies the following properties:

- $(A + B)^* = A^* + B^*$,
- $(\alpha A)^* = \overline{\alpha} A^*$,
- $(AB)^* = B^* A^*$.

Lemma 3.1.12 (Lang, 1993, p. 107). If for all $x$, $\langle x|Ax \rangle = 0$ then $A = 0$.

Theorem 3.1.13 (Spectral Theorem, Lang, 2002). Let $A$ be a hermitian operator on a finite dimensional Hilbert space $\mathcal{H}$. Then $\mathcal{H}$ has an orthogonal basis consisting of eigenvectors of $A$.

Definition 3.1.14. We say that an operator $A$ on $\mathcal{H}$ is positive if it is hermitian and if all of its eigenvalues are positive. Equivalently, $A$ is positive if the form $\phi_A$ is positive definite. We say $A$ is a density matrix if moreover, the sum of the eigenvalues is less or equal to 1.

Lemma 3.1.15. Let $\mathcal{H}$ be a finite dimensional Hilbert space, and $A$ an invertible operator. Then the following conditions are equivalent:

1. $A^* = A^{-1}$;
2. $\|Ax\| = \|x\|$ for all $x \in \mathcal{H}$;
3. $\langle Ax|Ay \rangle = \langle x|y \rangle$ for all $x,y \in \mathcal{H}$;
4. $\|Ax\| = 1$ for every unit vector $x \in \mathcal{H}$.

Definition 3.1.16. An invertible operator satisfying the conditions of Lemma 3.1.15 is said to be unitary.
3.1.2 Tensor Products of Hilbert Spaces

**Definition 3.1.17** [Dummit and Foote, 1999]. Consider two finite Hilbert spaces \( V \) and \( W \) with respective bases \((e_1, \ldots, e_n)\) and \((f_1, \ldots, f_k)\). We define the tensor product of \( V \) and \( W \), denoted \( V \otimes W \), 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

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

We define the scalar product in \( V \otimes W \) as follows:

\[
\langle e_i \otimes f_j | e_k \otimes f_l \rangle = \langle e_i | e_k \rangle \langle f_j | f_l \rangle.
\]

**Lemma 3.1.18.** If \( U, V \) and \( W \) are finite-dimensional Hilbert spaces, there exists a one-to-one correspondence \( \Phi \) between linear maps \( U \otimes V \rightarrow W \) and linear maps \( U \rightarrow V \otimes W \).

**Proof.** Choose a basis \((e_i)\) for \( V \) and a basis \((f_j)\) for \( W \). Then if \( f : U \otimes V \rightarrow W \), we define \( g = \Phi(f) : U \rightarrow V \otimes W \) as the map

\[
g(u) = \sum_i e_i \otimes f(u \otimes e_i).
\]

If \( g : U \rightarrow V \otimes W \), and if

\[
g(u) = \sum_{i,j} \rho_{i,j} \cdot e_i \otimes f_j,
\]

we define \( f = \Phi^{-1}(g) : U \otimes V \rightarrow W \) as the map

\[
f(u \otimes e_i) = \sum_j \rho_{i,j} \cdot e_i \otimes f_j.
\]

**Convention 3.1.19.** If \( A \in \mathbb{C}^{n \times n} \) and \( B \in \mathbb{C}^{k \times k} \) are two square matrices of respective size \( n \times n \) and \( k \times k \) seen as operators respectively on \( \mathbb{C}^n \) and on \( \mathbb{C}^k \), the matrix \( A \otimes B \) is an operator on \( \mathbb{C}^{nk} \) and we represent it as the matrix of blocks

\[
A \otimes B = \begin{pmatrix}
    a_{1,1}B & \cdots & a_{1,n}B \\
    \vdots & \ddots & \vdots \\
    a_{n,1}B & \cdots & a_{n,n}B
\end{pmatrix}.
\]

3.1.3 Completely Positive Maps

In this section, we focus primarily on Hilbert spaces of the form \( \mathbb{C}^{n \times n} \), spaces of \( n \times n \)-matrices. We choose as basis for \( \mathbb{C}^{n \times n} \) the canonical basis \((E_{i,j})_{i,j \in \{1, \ldots, n\}}\), where \((E_{i,j})_{k,l} = 0\) for all \( k \) and \( l \) except when \( k = i \) and \( l = j \). We use the notations and definitions of [Selinger, 2004b].

**Definition 3.1.20.** A linear map \( F : \mathbb{C}^{n \times n} \rightarrow \mathbb{C}^{k \times k} \) is said to be a *positive map* if for all positive matrices \( A, F(A) \) is positive.

\(^1\)Note that we identified \( V \) with \( V^* \). Although the result is correct since we are in finite dimension, we lose the basis Independence of the correspondence.
Definition 3.1.21. A linear map $F : \mathbb{C}^{n \times n} \to \mathbb{C}^{k \times k}$ is said to be completely positive if for all $i$, if $id_i$ is the identity on $i \times i$-matrices, $id_i \otimes F$ is a positive map $\mathbb{C}^{ni \times ni} \to \mathbb{C}^{ki \times ki}$.

Definition 3.1.22. The characteristic matrix of a linear map $F : \mathbb{C}^{n \times n} \to \mathbb{C}^{k \times k}$ is defined as the $nk \times nk$-matrix of blocks

$$
\chi_F = \begin{pmatrix}
F(E_{1,1}) & \cdots & F(E_{1,n}) \\
\vdots & \ddots & \vdots \\
F(E_{n,1}) & \cdots & F(E_{n,n})
\end{pmatrix}.
$$

Lemma 3.1.23. Let $F : \mathbb{C}^{n \times n} \to \mathbb{C}^{k \times k}$ be a linear operator, and let $\chi_F$ be its characteristic matrix. Then $F(A) = UAU^*$ for some $U \in \mathbb{C}^{k \times n}$ if and only if there exists a vector $v \in \mathbb{C}^{nk}$ such that $vv^* = \chi_F$. \(\square\)

Theorem 3.1.24 (Choi 1975). Let $F : \mathbb{C}^{n \times n} \to \mathbb{C}^{k \times k}$ be a linear operator, and let $\chi_F$ be its characteristic matrix. Then the following are equivalent:

1. $F$ is completely positive
2. $\chi_F$ is positive
3. $F$ is of the form $F(A) = \sum U_i AU_i^*$ for some finite sequence of matrices $U_1, \ldots, U_l$ in $\mathbb{C}^{k \times n}$. \(\square\)

3.1.4 Superoperators

The following definitions and results are from [Selinger 2004b].

Definition 3.1.25 (Löwner order). We define a relation $\subseteq$ on $\mathbb{C}^{n \times n}$ as follows. Let $A, B$ be matrices in $\mathbb{C}^{n \times n}$. Then $A \subseteq B$ if and only if $B - A$ is positive.

Definition 3.1.26. A completely positive map $F : \mathbb{C}^{n \times n} \to \mathbb{C}^{k \times k}$ is called a superoperator if for all positive matrices $A \in \mathbb{C}^{n \times n}$, we have $\text{tr}(F(A)) \leq \text{tr}(A)$.

Theorem 3.1.27 (Kraus Representation Theorem). Let $F : \mathbb{C}^{n \times n} \to \mathbb{C}^{k \times k}$ be a completely positive operator. The following are equivalent:

1. $F$ is a superoperator;
2. $(id_n \otimes \text{tr}_k)(\chi_F) \subseteq I_n$, where $I_n$ is the identity matrix and $\text{tr}_k : \mathbb{C}^{k \times k} \to \mathbb{C}$ is the trace operation;
3. $F$ is of the form

$$
F(A) = \sum_i U_i AU_i^*
$$

for matrices $U_1, \ldots, U_n$ with $\sum_i U_i^* U_i \subseteq I_n$. \(\square\)

Definition 3.1.28. A matrix $U \in \mathbb{C}^{k \times n}$ is called contraction if $U$ is a sub-matrix of some unitary $U'$, that is, if there exist matrices $U_1, U_2, U_3$ such that

$$
U' = \begin{pmatrix}
U \\
U_1 \\
U_2 \\
U_3
\end{pmatrix}
$$

is unitary. A linear function $F : \mathbb{C}^{n \times n} \to \mathbb{C}^{k \times k}$ is called a contraction if it is of the form $F(A) = UAU^*$ for some contraction $U$. 
Lemma 3.1.29. Let $U \in \mathbb{C}^{n \times m}$ be a contraction. Then the matrix
\[
\begin{pmatrix}
U \\
0
\end{pmatrix} \in \mathbb{C}^{(n+1) \times m}
\]
is also a contraction.

Proof. With the notation of the definition, consider the unitary matrix
\[
\begin{pmatrix}
U & 0 & U_1 \\
0 & 1 & 0 \\
U_2 & 0 & U_3
\end{pmatrix}.
\]

Lemma 3.1.30. A matrix $U \in \mathbb{C}^{k \times n}$ is a contraction if and only if $UU^* \subseteq I_k$, and if and only if $U^*U \subseteq I_n$.

Definition 3.1.31. If $\text{tr}_n$ is the trace on matrices in $\mathbb{C}^{n \times n}$, we define the partial trace operator
\[
C^{k \times k} \rightarrow \mathbb{C}^{k}\times\mathbb{C}^{k}
\]
as
\[
\text{tr}_k^n = \text{tr}_n \otimes \text{id}_{\mathbb{C}^k}.
\]

Theorem 3.1.32 (Naimark Theorem). Every superoperator $F : \mathbb{C}^{n \times n} \rightarrow \mathbb{C}^{m \times m}$ can be factored as $F = E \circ G$, where $G$ is a contraction and $E$ is a partial trace operator.

3.1.5 The 2-Dimensional Hilbert Space

We will now study in more detail what we saw in the previous section, applied to the 2-dimensional Hilbert space. We identify it with $\mathbb{C}^2$ and we call the canonical basis $e_1 = (1 \ 0)$ and $e_2 = (0 \ 1)$. The results of this section can be found in [Preskill, 1999].

Lemma 3.1.33. The set of hermitian matrices on $\mathcal{H}$ is spanned as a real vector space by the following basis:
\[
I = \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}, \quad \sigma_x = \begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}, \quad \sigma_y = \begin{pmatrix}
0 & -i \\
i & 0
\end{pmatrix}, \quad \sigma_z = \begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix}.
\]

Definition 3.1.34. The matrices $\sigma_x, \sigma_y, \sigma_z$ are called the Pauli matrices.

Remark 3.1.35. The eigenvectors and eigenvalues of the Pauli matrices are as follows:
\[
\sigma_x(\frac{1}{2}) = \frac{1}{2}, \quad\quad \sigma_y(\frac{1}{2}) = \frac{1}{i}, \quad\quad \sigma_z(\frac{1}{2}) = \frac{i}{2},
\]
\[
\sigma_x(-\frac{1}{2}) = -\frac{1}{2}, \quad\quad \sigma_y(-\frac{1}{2}) = -\frac{i}{2}, \quad\quad \sigma_z(-\frac{1}{2}) = -\frac{i}{2}.
\]

Definition 3.1.36. Let $\mathcal{H}$ be a Hilbert space. A ray $[v]$ in $\mathcal{H}$ is an equivalence class of vectors in $\mathcal{H}$ that differ by multiplication by non-zero complex scalars: so $[v]$ contains all $\alpha v$, $\alpha \in \mathbb{C} \setminus \{0\}$.

Lemma 3.1.37. There is a group action from the group of linear operators of $\mathcal{H}$ on the set of rays of $\mathcal{H}$.

Lemma 3.1.38. If $v$ and $w$ are orthogonal, so are any two elements of their respective rays.

Lemma 3.1.39. The rays of $\mathbb{C}^2$ are in one-to-one correspondence with the points on the unit sphere of $\mathbb{R}^3$. In spherical coordinates, a point $(\theta, \varphi)$ with $\theta \in [0, \pi], \varphi \in [-\pi, \pi]$ is in correspondence with the ray of representative
\[
r(\theta, \varphi) = \begin{pmatrix}
\cos \frac{\theta}{2} \\
e^{i\varphi} \sin \frac{\theta}{2}
\end{pmatrix}.
\]

The correspondence is pictured in Figure 3.1.
3.1. Mathematical Formalism

One calls this unit sphere the Bloch sphere. In this representation, the Pauli matrices acts on the rays as follows:

- **σ<sub>x</sub>** sends \( r(\theta, \varphi) \) onto
  \[
  \left( e^{i\varphi} \sin \frac{\theta}{2}, e^{-i\varphi} \sin \frac{\theta}{2} \right) \mapsto \left( \cos \frac{\theta}{2}, \sin \frac{\theta}{2} \right).
  \]
  thus sends the point \((\theta, \varphi)\) of the unit sphere of \( \mathbb{R}^3 \) (in spherical coordinate) to \((\pi - \theta, -\varphi)\), that is, in cartesian coordinates,
  \[
  \begin{pmatrix}
  \sin \theta \cos \varphi \\
  \sin \theta \sin \varphi \\
  \cos \theta
  \end{pmatrix}
  \mapsto
  \begin{pmatrix}
  \sin \theta \cos \varphi \\
  -\sin \theta \sin \varphi \\
  -\cos \theta
  \end{pmatrix}
  \quad \text{or} \quad
  \begin{pmatrix}
  x \\
  y \\
  z
  \end{pmatrix}
  \mapsto
  \begin{pmatrix}
  x \\
  -y \\
  -z
  \end{pmatrix}.
  \]

The operator **σ<sub>x</sub>** acts on the sphere as an axial symmetry around \( Ox \). The two eigenvectors \( \left( \frac{1}{2} \right) \) and \( \left( \frac{-1}{2} \right) \) respectively correspond to the point \((1,0,0)\) and to the point \((-1,0,0)\) on the sphere.

- **σ<sub>y</sub>** sends \( r(\theta, \varphi) \) onto
  \[
  \left( e^{i\varphi} \sin \frac{\theta}{2}, e^{i(\pi - \varphi)} \sin \frac{\theta}{2} \right) \mapsto \left( \cos \frac{\theta}{2}, \sin \frac{\theta}{2} \right).
  \]
  i.e. maps \((\theta, \varphi)\) to \((\pi - \theta, \pi - \varphi)\), i.e. computes an axial symmetry around \( Oy \). The two eigenvectors \( \left( \frac{1}{2} \right) \) and \( \left( \frac{-1}{2} \right) \) respectively correspond to the point \((0,1,0)\) and to the point \((0,-1,0)\) on the sphere.

- Finally, **σ<sub>z</sub>** sends \( r(\theta, \varphi) \) onto
  \[
  \left( e^{i\varphi} \sin \frac{\theta}{2}, e^{i(\pi - \varphi)} \sin \frac{\theta}{2} \right) \mapsto \left( \cos \frac{\theta}{2}, \sin \frac{\theta}{2} \right).
  \]
  i.e. maps \((\theta, \varphi)\) to \((\theta, \pi - \varphi)\), i.e. computes an axial symmetry around \( Oz \). The two eigenvectors \( \left( \frac{1}{2} \right) \) and \( \left( \frac{-1}{2} \right) \) respectively correspond to the point \((0,0,1)\) and to the point \((0,0,1)\) on the sphere.

![Bloch sphere](image_url)

Figure 3.1: The Bloch sphere.
Lemma 3.1.40. Two rays in $\mathbb{C}^2$ are orthogonal if and only if their representations on the Bloch sphere are antipodal.

\[ \square \]

3.2 Quantum Foundations

Quantum computation is somehow the art of making the theory of finite Hilbert spaces into a theory of computation: In quantum computation, information is encoded on states of quantum particles, states whose mathematical representation are rays in some Hilbert space.

Convention 3.2.1. In the following, we use the Dirac convention for writing vectors:
- vectors are written as kets: $|\phi\rangle$;
- functionals are written as bras: $\langle \psi |$;
- scalar products, which are by Lemma 3.1.9 the application of some functional to some vectors, are written as usual: $\langle \psi | \phi \rangle$.

3.2.1 Quantum Bits

One Quantum Bit

In classical computation, the smallest unit of data is the bit, element of the two-elements set $\{0, 1\}$. In quantum computation, the smallest unit of data is a quantum bit, or qubit, defined as a ray in a 2-dimensional Hilbert space. We write the canonical basis of this space as $\{|0\rangle, |1\rangle\}$.

Using the results of Section 3.1.5, one says that

\[
\begin{align*}
(|0_x\rangle, |1_x\rangle) &= \left(|0\rangle, |1\rangle\right) \quad \text{is the basis along } z, \\
(|0_x\rangle, |1_x\rangle) &= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|1\rangle - |1\rangle)\right) \quad \text{is the basis along } x, \\
(|0_y\rangle, |1_y\rangle) &= \left(\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|1\rangle - i|1\rangle)\right) \quad \text{is the basis along } y.
\end{align*}
\]

Several Quantum Bits

When considering a system of $n$ quantum bits, the state of the system is a ray in $\mathcal{H}^\otimes n = \mathcal{H} \otimes \cdots \otimes \mathcal{H}$, where $\mathcal{H}$ is the 2-dimensional Hilbert space. As stated in Definition 3.1.17, we take the canonical basis for $\mathcal{H}^\otimes n$ to be

\[ \{|i_1 \ldots i_n\rangle | i_1, \ldots, i_n \in \{0, 1\}\}, \]

where we write $|i_1 \ldots i_n\rangle$ for $|i_1\rangle \otimes \cdots \otimes |i_n\rangle$.

3.2.2 Operations

Measurements

Observables. In quantum physics, a measurement in a Hilbert space $\mathcal{H}$ is associated with a self-adjoint operator $A$ of $\mathcal{H}$. Physicists call $A$ an observable.

As we saw in Theorem 3.1.8, to a self-adjoint operator one can associate a set of orthogonal eigenspaces with their corresponding eigenvalues. If $|\phi\rangle$ is an eigenvector of $A$ with eigenvalue $a$, the numerical outcome of the measurement of $|\phi\rangle$ with the observable $A$ is the value $a$. 

What does happen if $\phi$ is not an eigenvector? For simplicity assume that $\mathcal{H}$ is finite and that the basis of eigenvectors of $A$ is $(|\phi_1\rangle, \ldots, |\phi_N\rangle)$ such that the eigenvalue corresponding to $|\phi_i\rangle$ is $a_i$. Then $|\phi\rangle$ can be re-written as $|\phi\rangle = \sum_{i=1}^N \alpha_i|\phi_i\rangle$, and measuring with $A$ makes the system randomly collapse to a new state, namely a basis vector $|\phi_i\rangle$. This new state is $|\phi_i\rangle$ with probability $|\alpha_i|^2 = |\langle \phi|\phi_i\rangle|^2$. In this situation, the measurement outputs the numerical value $a_i$.

For the purpose of measurement the numerical eigenvectors have little importance. What is really important is that two eigenvalues corresponding to two distinct eigenspaces differ. When measuring a state of $n$ quantum bits, we say that the outcome of the measurement of the state is $x_1 \ldots x_n$ if the state collapsed to $|x_1 \ldots x_n\rangle$. For example, we say:

\begin{quote}
\text{"The measurement of the state } |\phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \text{ in the standard basis results in the outcome 01 with probability } |\langle 01|\phi\rangle|^2 = |\beta|^2."
\end{quote}

Pauli matrices. Given a quantum bit state $|\phi\rangle$, for $i = x, y, z$ the Pauli matrix $\sigma_i$ provides an observable, whose measurement projects the state $|\phi\rangle$ in the basis along axis $i$.

From Section 3.1.5, the bases along $x, y$ and $z$ have special properties: if a quantum bit is in one of the basis element of the base along $i$, for some $i = x, y$ or $z$, then measuring the observable $\sigma_j$, $j \neq i$ will yield 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. Thus somehow the information stored in the basis along $i$ is not accessible from the two other ones.

**Convention 3.2.2.** In the remainder of the thesis, when speaking of “a measurement” without further precision, we always consider the measurement to be along the basis $z$.

Unitary gates

A quantum mechanical system, if not measured (by the operator or by the environment), evolves along a unitary path. That is, loosely speaking, all we can do is to apply rotations on the system. We call these actions unitary gates.

The ability to perform one gate or another depends on the physical implementation of the quantum bits. In general, only a few gates are needed to approximate any given unitary matrix, a result known as the Solovay-Kitaev Theorem. We already met the Pauli matrices in Section 3.1.5.

The matrix $\sigma_z$ is also called the not gate:

\[
N = \left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right).
\]

Two other usual gates are the Hadamard gate and the phase-shift gate:

\[
H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad V_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.
\]

Finally, written in the canonical basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$, we have the exchange gate and the controlled-not gate:

\[
X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad N_C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.
\]

The $N_C$-gate comes from a generic process: If $U$ is a one-qubit gate, one constructs $U_C$, called controlled $U$, to be the two-qubits gate:

\[
U_C (|0\rangle \otimes |\phi\rangle) = |0\rangle \otimes |\phi\rangle, \quad U_C (|1\rangle \otimes |\phi\rangle) = |1\rangle \otimes U|\phi\rangle.
\]

The gate $U$ is applied on the second qubit depending on the value of the first qubit.
Quantum Circuit

It is possible to write tensors and compositions of gates as wires and boxes on wires. For example, the map $H \otimes V_\theta$ can be written as

\[ \begin{array}{c}
H \\
V_\theta
\end{array} \]

Some gates have specific representations:

- The gate $N$ is written as $\oplus$.
- A controlled-$U$ gate is written as $U$.
- The gate $N_C$ is written as $\oplus$.
- The gate $X$ is simply $\cdot$.
- Measurements will be represented by dashed boxes followed by a dashed wire, to indicate that we now have a classical bit, as follows:

\[ \begin{array}{c}
M_b \\
\rightarrow
\end{array} \]

3.2.3 Mixed States

The representation of a state of a system of quantum bits as a ray in some Hilbert space is a valid description of an isolated quantum system. It does not work when only part of the system is considered. Indeed, suppose we are given a two-qubit system $|\phi_{AB}\rangle$ in the state

\[ \alpha |0_A\rangle \otimes |0_B\rangle + \beta |0_A\rangle \otimes |1_B\rangle + \gamma |1_A\rangle \otimes |0_B\rangle + \delta |1_A\rangle \otimes |1_B\rangle, \]

where $(|0_A\rangle, |1_A\rangle)$ and $(|0_B\rangle, |1_B\rangle)$ are some basis of $\mathbb{C}^2$ and suppose we only have access to qubit $A$.

Consider an observable $M$ on $A$. Using the formalism developed with isolated systems, if we perform a measurement with this observable, the total expectation of the measurement is

\[ \langle \phi_{AB} | (M \otimes I_B) | \phi_{AB} \rangle = \left( \alpha^* \langle 0_A | + \gamma^* \langle 1_A | \right) M \left( \alpha |0_A\rangle + \gamma |1_A\rangle \right) = \text{tr}(M \rho_A), \]

where $\rho_A$ is the density matrix (as in Definition 3.1.14) equal to

\[ \left( \beta |0_A\rangle + \delta |1_A\rangle \right) \left( \beta^* |0_A\rangle + \delta^* |1_A\rangle \right) + \left( \alpha |0_A\rangle + \gamma |1_A\rangle \right) \left( \alpha^* |0_A\rangle + \gamma^* |1_A\rangle \right), \]

that is

\[ \begin{pmatrix}
|\alpha|^2 & \gamma \alpha^* \\
\gamma^* \alpha & |\gamma|^2
\end{pmatrix} + \begin{pmatrix}
|\beta|^2 & \delta \beta^* \\
\delta^* \beta & |\delta|^2
\end{pmatrix} \]

in the basis $(|0_A\rangle, |1_A\rangle)$. Note that if $M$ is the projection onto $|0_A\rangle$, as expected we get $|\alpha|^2 + |\beta|^2$. And if it is the projection onto $|1_A\rangle$, we get $|\delta|^2 + |\gamma|^2$. 
Thus, if we are only considering the quantum bit $A$, one can safely work with the density matrix $\rho_A$ in place of the whole system. This representation is called a mixed state: Since $|\alpha|^2 + |\gamma|^2 + |\beta|^2 + |\delta|^2 = 1$, if

$$\alpha' = \frac{\alpha}{|\alpha|^2 + |\gamma|^2}, \quad \gamma' = \frac{\gamma}{|\alpha|^2 + |\gamma|^2}, \quad \beta' = \frac{\beta}{|\beta|^2 + |\delta|^2}, \quad \delta' = \frac{\delta}{|\beta|^2 + |\delta|^2},$$

then the matrix $\rho_A$ represents a probability distribution over pure states

$$\frac{|\alpha|^2 + |\gamma|^2}{\alpha'}|0_A\rangle\langle\alpha'\rangle + \frac{|\beta|^2 + |\delta|^2}{\beta'}|1_A\rangle\langle\beta'|.$$  

We can re-encode the state of an $n$-quantum bit system $|\phi\rangle$ as the $2^n \times 2^n$ density matrix $\rho = |\phi\rangle\langle\phi|$. A unitary operation $U$ on this state yields the density matrix $U\rho U^*$, and the measurement of an observable $M$ yields the expected value $\text{tr}(M\rho)$.

### 3.3 Quantum Effects

We list in this section a few specifics of quantum computation, following [Preskill, 1999].

#### 3.3.1 No Cloning

Consider a quantum bit in some unknown state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then it is not possible to “clone” the state and get the two-qubit state $|\phi\rangle \otimes |\phi\rangle$. The reason is simple: the only operations we are allowed to perform are unitaries and measurements, which are linear maps. The cloning operation being non-linear, it is therefore not implementable.

It is however possible to build a “copying” map $G$

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|00\rangle + \beta|11\rangle.$$

But it does not satisfy the usual commutativity rule for duplication: if $f : \mathcal{H} \rightarrow \mathcal{H}$ is any linear map, then $G \circ f \neq (f \otimes f) \circ G$.

#### 3.3.2 Entanglement

Another special property of quantum information is the superposition: the 2-qubit state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (3.3.1)$$

is a valid state, but cannot be written as $|\phi\rangle \otimes |\psi\rangle$. We say the two quantum bits are entangled.

The interesting aspect of entanglement is that the measurements of the qubits will be correlated. For example, measuring the first qubit in the state (3.3.1) with respect to the standard basis yields 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. In the former case, the state of the 2-qubit system is $|00\rangle$, thus measuring the second qubit yields 0 with probability 1. In the latter, the state of the system is $|11\rangle$, and measuring the second qubit yields 1 with probability 1.

A useful basis for 2-qubit systems is the following set of entangled states:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$
3.3.3 Bell’s Inequalities

This section is taken from (Preskill, 1999).

From a classical perspective, a measurement is a special form of coin-toss. A hidden variable theory is a theory where a probability $\lambda$ is associated to each state and to each axis such that the measurement along this axis outputs $\lambda$. The question is then whether it is possible to build a hidden variable theory that would agree with the prediction of quantum theory while still satisfying the strong locality criterion (Einstein et al., 1935), stating:

“Suppose that $A$ and $B$ are space-like separated systems. Then in a complete description of physical reality an action performed on system $A$ must not modify the description of system $B$."

Bell (1964) shows that it is not possible. The argument goes as follows. Consider a quantum machine that maximally entangles two quantum bits $A$ and $B$

$$|\phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$$

and sends qubit $A$ to Alice and qubit $B$ to Bob. Suppose that they can independently choose one of the following axes (in the Bloch sphere, see Figure 3.1) to measure:

$$a = (0, 0, 1), \quad b = \left(\frac{\sqrt{3}}{2}, 0, \frac{1}{2}\right), \quad c = \left(\frac{\sqrt{3}}{2}, 0, -\frac{1}{2}\right).$$

They live in the $xz$-plane of the Bloch sphere and correspond respectively to the bases in $\mathbb{C}^2$:

$$|0_a\rangle = |0\rangle, \quad |0_b\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle, \quad |0_c\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle,$$

$$|1_a\rangle = |1\rangle, \quad |1_b\rangle = \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle, \quad |1_c\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle.$$

What is the probability of obtaining the same output when measuring $A$ and $B$ with respect to two different bases?

In a local hidden variable theory, the result of measuring $A$ and $B$ along each of the possible axis is predetermined. Let $P_{x,y}$ be the probability of obtaining the same output while measuring $A$ along $x$ and $B$ along $y$. For any local hidden variable theory,

$$P_{a,b} + P_{b,c} + P_{c,a} \geq 1, \quad (3.3.2)$$

since for any possible distribution of measurement values, there will always be two values that will be equal (see (Preskill, 1999) for a complete discussion). However, the quantum theory provides the value

$$P_{x,y} = \langle \phi_{AB}|(0_x\langle 0_x| \otimes |0_y\rangle\langle 0_y|)|\phi_{AB}\rangle + \langle \phi_{AB}|(1_x\langle 1_x| \otimes |1_y\rangle\langle 1_y|)|\phi_{AB}\rangle.$$

The computation shows that $P_{x,y} = \frac{1}{4}$ for $x \neq y, x, y = a, b, c$. In particular,

$$P_{a,b} + P_{b,c} + P_{c,a} = \frac{3}{4} < 1,$$

which violates Equation (3.3.2).
3.4 Some Algorithms and Uses of Quantum Effects

The main power of quantum computation comes from entanglement. We describe in the following three algorithms that we will consider in the remainder of the thesis. For more algorithms, such as the quantum fast Fourier transform, or Shor’s factorization algorithm [Shor, 1994], a good reference is [Aharanov, 1999].

3.4.1 Teleportation

One use of entanglement is the “teleportation” of a quantum bit state via a classical channel. The idea is the following: Alice and Bob share an entangled pair of qubits

\[
\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle).
\]

Alice wants to send a qubit in an unknown state \( |\phi\rangle = \alpha|0\rangle + \beta|1\rangle \) to Bob. The teleportation procedure, summarized in Figure 3.2, can be described in three steps:

1. At location A, create the initial entangled state \( \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \) with the two last qubits using the circuit

\[
|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle).
\]

Alice keeps qubit 2 and stays at location A, while Bob takes qubit 3 and goes to location B.

2. Alice, to send qubit 1 in state \( |\phi\rangle \) to Bob, applies a rotation on her two qubits 1 and 2, using

Figure 3.2: Quantum teleportation protocol.
the circuit

She then measures the 2-qubit resulting state, gets two classical bits \((x, y)\) and sends them to Bob.

3. Bob, to transform qubit 3 to state \(|\phi\rangle\) applies on it the transformation \(U_{xy}\) defined as follows:

\[
\begin{align*}
\text{if } M \text{ outputs } 00, & \quad U_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
\text{if } M \text{ outputs } 01, & \quad U_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\
\text{if } M \text{ outputs } 10, & \quad U_{10} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \\
\text{if } M \text{ outputs } 11, & \quad U_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.
\end{align*}
\] (3.4.1)

Note that the entanglement of qubits 2 and 3 can be done ahead of time (so long as they stay entangled).

**Proof of the correctness of the protocol.** The rotation of step (2) performs the following computation

\[
\begin{align*}
\text{CNOT} & \implies \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle), \\
H \otimes id & \implies \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle), \\
\text{CNOT} & \implies \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle), \\
H \otimes id & \implies \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle).
\end{align*}
\]

If we apply it to the two first qubits of

\[
(a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)
\]

we get

\[
\frac{1}{2} \left( a(|000\rangle + |100\rangle) + a(|011\rangle + |111\rangle) + b(|010\rangle - |110\rangle) + b(|001\rangle - |101\rangle) \right)
\]

\[
= \frac{1}{2} \left( |00\rangle \otimes (a|0\rangle + b|1\rangle) + |01\rangle \otimes (b|0\rangle + a|1\rangle) + |10\rangle \otimes (a|0\rangle - b|1\rangle) + |11\rangle \otimes (a|1\rangle - b|0\rangle) \right)
\]

If we measure the two first qubits, the third qubit becomes

\[
\begin{align*}
a|0\rangle + b|1\rangle & \quad \text{if } 00 \text{ was measured}, \\
b|0\rangle + a|1\rangle & \quad \text{if } 01 \text{ was measured}, \\
a|0\rangle - b|1\rangle & \quad \text{if } 10 \text{ was measured}, \\
a|1\rangle - b|0\rangle & \quad \text{if } 11 \text{ was measured}.
\end{align*}
\]

Finally note that if \(U_{xy}\) is applied in the case where \(x, y\) was measured, then the state of the last qubit is \(a|0\rangle + b|1\rangle\). □
3.4. Some Algorithms and Uses of Quantum Effects

3.4.2 Dense Coding

The teleportation algorithm allows to “send” one qubit using two classical bits. It is possible to perform the reverse operation, namely to send two classical bits using an entangled pair and a quantum channel.

The situation is similar. Alice and Bob share an entangled state of 2 qubits, Alice has qubit 1, Bob has qubit 2. This time, Bob wants to send the two classical bits \((x,y)\) to Alice. He can use the protocol summarized in Figure 3.3, called dense coding. Like the teleportation algorithm, the procedure is again in three steps:

1. At location B, Alice and Bob create an entangled state of two quantum bits 1 and 2, using the circuit

   \[
   |0\rangle \xrightarrow{H} |0\rangle \oplus |0\rangle .
   \]

   Then, Alice goes to location A with qubit 1, while Bob stays at location B with qubit 2.

2. If Bob wants to send two classical bits \((x,y)\) to Alice, he needs to apply the gate \(U_{x,y}\) as defined in the teleportation protocol (Equation (3.4.1)), and send the modified qubit 2 to Alice.

3. Alice, to retrieve the two classical bits, applies a rotation on qubits 1 and 2 using the gate

   \[
   H
   \]

   and a measurement, retrieving the two bits \((x,y)\).
3.4. Some Algorithms and Uses of Quantum Effects

3.4.3 The Deutsch Algorithm

The Deutsch algorithm is for finding out whether a boolean function is balanced or constant. In classical computation, two calls to the function are needed. In quantum computation, one can find it out in only one call. The algorithm takes as input an unknown circuit $U_f$ computing

$$U_f(|x⟩ ⊗ |y⟩) = |x⟩ ⊗ |y ⊕ f(x)⟩$$

for some boolean function $f$, where $⊕$ stands for the boolean addition. The quantum circuit for the algorithm is the following:

$$\begin{align*}
|0⟩ & \xrightarrow{H} |0⟩ \otimes |0⟩ \\
|1⟩ & \xrightarrow{H} |1⟩ \otimes |1⟩ \\
& \xrightarrow{U_f} |00⟩ \otimes |0⟩ + |10⟩ \otimes |0 ⊕ f⟩ + |01⟩ \otimes |1⟩ + |11⟩ \otimes |1 ⊕ f⟩.
\end{align*}$$

where we write $fx$ in place of $f(x)$. To retrieve the answer, we have to measure the first qubit: it is 0 when the function is balanced and 1 when it is not. Note that the input of this algorithm is a “black-box”, in other terms a function from two qubits to two qubits.

Proof that the procedure is correct. This will compute the following thing:

$$\begin{align*}
(H \otimes id)(U_f)(H \otimes H)(|0⟩ \otimes |1⟩) \\
= (H \otimes id)(U_f) \left( \frac{1}{\sqrt{2}}(|0⟩ + |1⟩) \otimes \frac{1}{\sqrt{2}}(|0⟩ - |1⟩) \right) \\
= \frac{1}{2}(H \otimes id)(U_f)((|00⟩ + |10⟩) - |01⟩ - |11⟩) \\
= \frac{1}{2}(H \otimes id) \begin{pmatrix}
|0⟩ \otimes |0 ⊕ f⟩ + |1⟩ \otimes |0 ⊕ f1⟩ \\
-|0⟩ \otimes |1 ⊕ f⟩ - |1⟩ \otimes |1 ⊕ f1⟩
\end{pmatrix} \\
= \frac{1}{2\sqrt{2}} \begin{pmatrix}
(|0⟩ + |1⟩) \otimes |f⟩ + (|0⟩ - |1⟩) \otimes |f1⟩ \\
-(|0⟩ + |1⟩) \otimes (|1 ⊕ f⟩ - |0 ⊕ f⟩ - |1 ⊕ f1⟩)
\end{pmatrix} \\
= \frac{1}{2\sqrt{2}} \begin{pmatrix}
|0⟩ \otimes (|f⟩ - |f1⟩ - |1 ⊕ f⟩) + |1⟩ \otimes (|f1⟩ - |1 ⊕ f⟩)
\end{pmatrix}.
\end{align*}$$

If $f0 = f1$, then $|f0⟩ - |f1⟩ - |1 ⊕ f0⟩ + |1 ⊕ f1⟩ = 0$ and the result is

$$\frac{1}{\sqrt{2}}|0⟩ \otimes (|f1⟩ - |1 ⊕ f1⟩).$$

If $f0 = 1 ⊕ f1$, then $|f0⟩ + |f1⟩ - |1 ⊕ f0⟩ - |1 ⊕ f1⟩ = 0$ and the result is

$$\frac{1}{\sqrt{2}}|1⟩ \otimes (|1 ⊕ f1⟩ - |f1⟩).$$

So the value of the measurement of the first qubit is 0 if the function $f$ is balanced, and 1 in the other case. □
Chapter 4

A Tour in Existing Models of Quantum Computation

Chapter 3 developed the formalism and the techniques needed to perform quantum computation. This chapter surveys a few selected models for manipulating quantum programs and protocols. A more complete set can be found in e.g. (Gay, 2006).

The goal is twofold. First, we want to be able to write programs and codes manipulating quantum data. Numerous attempts have been done in the past years to provide a more easy way to write (and read) quantum algorithms. Second, we aim at a deeper understanding of the structure of quantum information by developing a semantics for quantum computation.

4.1 The Various Paradigms

For building languages and understanding algorithms, several paradigms of computation have been studied.

4.1.1 Unitary Gates as Computation.

Families of Quantum Circuits

One formal system for writing quantum algorithms is the quantum circuit formalism described by Deutsch (1989) and sketched in Section 3.2.2. In this formalism, the driving forces in the computation are the unitary operations. An algorithm is composed of three steps:

1. allocation of $n$ quantum bits;
2. application of a list of unitary gates;
3. measurement of all or a part of the $n$ quantum bits.

The description of an algorithm is a family of quantum circuits, one for each possible number of input qubits. The family needs to be uniform, i.e. efficiently computable by a classical computer. As for classical boolean circuits, it is then possible to speak of the complexity of an algorithm by taking the limit of the ratio of the number of gates used in the circuit versus the number of input quantum bits.
4.1. The Various Paradigms

The Quantum Turing Machine

A Turing machine (Turing, 1936) is an automaton consisting of the following elements:

1. an infinite tape, divided into cells, each cell containing a letter from a given alphabet;
2. a head, able to read and write into cells, and to move to the left or to the right along the tape;
3. a finite set of states and a state register, recording the state of the machine. One of the states is called initial and a subset of the states are called final;
4. a transition table, mapping each possible pair (letter, state) to a triple consisting of a new state, a letter and a direction (left or right).

At the beginning the state register is in the initial state. At each time-step, the automaton reads the cell of tape below the head. Based on the letter read and its state, using the transition table, it writes on the tape the corresponding letter and moves in the given direction. It iterates this course of action until a final state is reached. A program consists of a given alphabet, a set of states and a transition table.

Benioff (1980) and Deutsch (1985) describe a Turing machine where the tape, the head, and the states of the automaton are encoded as a quantum state. The transition table is described in a unitary operation. This model provides a tool to reason about expressiveness and complexity of quantum algorithms: As was shown by Nishimura and Ozawa (2002), the resulting notion of computation is equivalent to that of the quantum circuit model.

QML or the Quantum Test

Altenkirch and Grattage (2005a,b) describe a first-order language for manipulating quantum bits. This calculus understands duplication as sharing, or copying:

\[
\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|00\rangle + \beta|11\rangle.
\]

The language is written on a classical device and compiles into a quantum circuit. Due to the copying operation, contraction can be done blindly but weakening (that is, measurement) has to be kept track of.

The language features superposition of quantum states, leading to a “quantum” test. For example, the gate \(N_C\) is defined as:

\[
\begin{align*}
N x &= \text{if}^a x \text{ then } 0 \text{ else } 1, \\
N_C \langle c, x \rangle &= \text{if}^c c \text{ then } \langle c, N x \rangle \text{ else } \langle c, x \rangle.
\end{align*}
\]

The main drawback of this formalism is that the quantum test

\[
\text{if}^a x \text{ then } M \text{ else } N
\]

is well defined if and only if \(M\) and \(N\) have orthogonal representations. Therefore, in general one cannot say before running the computation whether a program is valid or not.

Van Tonder’s Quantum Lambda Calculus

Van Tonder (2004) describes a lambda calculus where the terms are encoded on strings of quantum bits. The language is built using the terms

\[
\begin{align*}
\text{Term } M, N \ ::= & \ x \mid c \mid MN \mid \lambda x. M, \\
\text{Constant } c \ ::= & \ 0 \mid 1 \mid H \mid \cdots.
\end{align*}
\]
4.1. The Various Paradigms

where the constants $c$ contain booleans 0 and 1, as representatives of the quantum bits $|0⟩$ and $|1⟩$, and representatives for a chosen set of unitary gates. For example, the identity is $|λx.x⟩$. The unitaries apply on 0 and 1 in the naive way: $|H0⟩$ should reduce to $\frac{1}{\sqrt{2}}(|0⟩ + |1⟩)$. This language is purely quantum, and the reduction is encoded as a unitary map.

A trick needs to be used to overcome the fact that the reduction is not in general a reversible operation (Consider for example $(λx.1)0 → 1$). Given any function $β : X → Y$, it is possible to produce a reversible map $X → X × Y$ invertible on its range by mapping $x → (x, β(x))$. If $β$ is a reduction of terms, we can make it reversible by appending to the successive terms in the reduction its history:

$$M → (M, β(M)) → (M, β(M), β^2(M)) → \cdots$$

However, a naive implementation of the lambda calculus into quantum bits does not provide a consistent equational theory. Indeed the term $\frac{1}{\sqrt{2}}(|λx.0)0⟩ + |(λx.0)1⟩)$ should be $β$-equivalent to $\frac{1}{\sqrt{2}}(|0⟩ + |1⟩)$, which is not valid since its norm is greater than 1.

As it turns out, one needs to distinguish between terms that are in superposition (such as $\frac{1}{\sqrt{2}}(|0⟩ + |1⟩)$) and the ones that are not. For the system to be consistent, terms in superposition should not be duplicated nor erased, and should be the same, modulo the 0’s and the 1’s.

4.1.2 Concurrent Quantum Computation

Quantum computation has important implications in cryptography. The design of quantum protocols to securely communicate data is a field of ongoing research.

From a theoretic side, a question one might ask is whether the tools that were developed to analyse the safety of classical distributed systems can be used in the context of quantum systems.

The simultaneous works of [Lalire and Jorrand, 2004] and [Gay and Nagarajan, 2005] develop a process algebraic approach to concurrent quantum computation. Starting from the π-calculus, quantum features, such as quantum bits, unitaries and measurements, are added to the syntax, and an operational semantics is developed. [Gay and Nagarajan, 2005] gives a typed language and prove some safety properties for well-typed protocols; for example the fact that a quantum bit cannot be shared among several processes, and the soundness of the type system.

4.1.3 Measurement-Based Quantum Computation

The unitary operations are one side of the quantum coin. The other side is the measurement. It turns out that it is possible to perform quantum computation with “only” measurements, as it was described first by [Briegel and Raussendorf, 2002]; [Raussendorf and Briegel, 2001] and then computationally by [Danos et al. 2007].

The idea is the following: A state of highly entangled quantum bits is prepared and then a series of measurements are performed. The computation is “run” by the projections occurring during the measurements. In its most general formulation, the calculus happens to be as powerful as the regular quantum-circuit computational model, and is slightly better in terms of time complexity.

Formally, one works with a pattern, composed of a finite set $V$, a set of inputs $I ⊂ V$, a set of outputs $O ⊂ V$, and a sequence of operations of the following kinds (where $i,j ∈ V$):

- 1-quantum measurements $M^α_i$: measurement of qubit $i$ in the $xy$-plane, along the axes

$$\frac{1}{\sqrt{2}}(|0⟩ + e^{iα}|1⟩), \quad \frac{1}{\sqrt{2}}(|0⟩ − e^{iα}|1⟩).$$
4.2 Formalism of Hilbert Spaces

A recent research thread initiated by Abramsky and Coecke (2004) aims at providing an abstract framework in which one could interpret quantum computation. The goal is to extract from the
category of Hilbert spaces the required structures for performing quantum computation.

### 4.2.1 Dagger Compact-Closed Categories

Abstract notions of adjointness, self-adjointness, unitaries, bases and scalar products arise in the context of dagger compact-closed categories with biproducts:

**Definition 4.2.1** (Selinger, 2005). A **dagger category** is a category $\mathcal{C}$ together a functor $\dagger : \mathcal{C}^{op} \to \mathcal{C}$ such that for every $f : A \to B$, $f^{\dagger\dagger} = f$ and for every object $A$, $A^{\dagger} = A$.

**Definition 4.2.2** (Selinger, 2005). A **dagger compact-closed category** is a dagger symmetric monoidal category that is also compact closed (see e.g. Kelly and Laplaza, 1980), and such that the following diagram commutes for all $A$:

\[
\begin{array}{ccc}
\top & \xrightarrow{\epsilon_A} & A \otimes A^* \\
\downarrow \eta_A & & \downarrow \sigma_{A,A^*} \\
A^* \otimes A.
\end{array}
\]

Various notions of Hilbert spaces can be defined in the context of dagger compact-closed categories with biproducts:

- A **scalar** is a morphism $s : \top \to \top$.
- A **vector** is a morphism $v : \top \to A$.
- The **adjoint** of a morphism $f : A \to B$ is the morphism $f^{\dagger} : B \to A$.
- The **scalar product** of $v, w : \top \to A$ is $v; w^{\dagger} : \top \to \top$.
- A **unitary morphism** is a morphism $f : A \to B$ such that $f^{\dagger}$ is its inverse.
- A **basis** for an object $A$ is a unitary morphism $b_A : n \cdot \top \to A$, where $n \cdot \top$ is a sum of $n \top$‘s. In this case, the **dimension** of $A$ is said to be $n$.
- We can define the **matrix** of a morphism $f : A \to B$ where $A$ and $B$ are finite dimensional as the map $n_{A} \cdot \top \xrightarrow{b_{A}} A \xrightarrow{f} B \xrightarrow{b_{B}} n_{B} \cdot \top$.

These definitions satisfy various equations related to Hilbert spaces and hermitian positive operators. For example, (Selinger, 2005) shows that completely positive maps can be defined in this context. The paper provides a categorical construction for building a category of completely positive maps out of any dagger compact-closed category.

Although no formal syntax comes with the semantics, a colourful graphical language is provided, making proofs of properties relatively easy to follow. However, this graphical language does not mix well with the need for biproducts: in the desired quantum computational applications, the notion of bases is heavily used.
4.2.2 Classical Objects

In an attempt to remove biproducts, Coecke and Pavlovic (2007) describe a new notion called classical objects. A classical object is an object \( X \) in the category together with a map \( \delta_X : X \to X \otimes X \), a map \( \epsilon_X : X \to \top \), and a few equations. In particular, these equations make \((X, \epsilon_X, \delta_X)\) a commutative comonoid object, as in Definition 2.7.3. The notion of classical object captures the notion of basis without the needs for biproducts. The idea is the following. A generic object \( X \) in the category is like a generic finite dimensional Hilbert space, with no associated basis. Associating a structure \((\delta_X, \epsilon_X)\) to the object \( X \) is the same thing as associating a basis to \( X \). In Hilbert spaces, the maps \( \delta_X \) and \( \epsilon_X \) are

\[
\delta_X : e_i \mapsto e_i \otimes e_i, \quad \epsilon_X : e_i \mapsto 1,
\]

for some basis \((e_1, \ldots, e_n)\) of \( X \). With enough structure, it is possible to simulate what was done with biproducts. In particular, as was shown by Coecke and Paquett (2006), an abstract version of the Naimark theorem can be proved using the graphical language.

4.3 A Flow-Chart Language

Selinger (2004b) describes a semantics for QRAM-based first-order quantum computation. Instead of starting from the category of Hilbert spaces, the paper describes computations as maps in the category of superoperators.

4.3.1 The language

The language is described by a flow-chart notation: it is a super-set of a classical flow-chart language. A program is a graph together with a cursor that follows the wires, with data attached to it. A graph is constructed from the rules in Table 4.1. The box `new qbit b = i` creates a new quantum bit of name \( b \) with value \( |i\rangle \). The box `new bit b = i` creates a new boolean variable named \( b \) with value \( i \). The gate \( q_1, \ldots, q_n \mapsto U_n \) applies the unitary gate \( U_n \) on the corresponding variables. The gate `permute \phi` permutes the context \( \Delta \) according to the permutation \( \phi \). The gate `branch b` performs a test on the boolean \( b \) and `meas q` measures the quantum bit \( q \) and performs a test on the output.

4.3.2 The Category of Superoperators

The language has a full and complete representation in the category \( \mathbb{Q} \) of superoperators. This category is defined as the refinement of the category \( \mathbb{CPM} \).

Definition 4.3.1. The category \( \mathbb{CPM} \) is defined as follows:

- The objects are signatures \( \sigma = n_1, \ldots, n_k \), i.e., finite tuples of positive integers,
- the morphisms \( \sigma \to \tau \) are completely positive maps \( V_\sigma \to V_\tau \), where \( V_{n_1, \ldots, n_k} \) is the Hilbert space \( \mathbb{C}^{n_1 \times n_1} \times \cdots \times \mathbb{C}^{n_k \times n_k} \).

We use the notation \( B_\sigma \) for the canonical basis of \( V_\sigma \).

The objects in this category can be seen as spaces of block matrices. Following the construction in Lemma 3.1.18, one can define a tensor and a coproduct structure, as follows:

Definition 4.3.2. Given two signatures \( \sigma = (n_1, \ldots, n_k) \) and \( \tau = (m_1, \ldots, m_l) \), we define \( \sigma \otimes \tau \) and \( \sigma \oplus \tau \) to be respectively

\[
\sigma \otimes \tau = (n_1m_1, \ldots, n_1m_l, n_2m_1, \ldots, n_km_l), \quad \sigma \oplus \tau = (n_1, \ldots, n_k, m_1, \ldots, m_l).
\]
4.3. A Flow-Chart Language

Table 4.1: Rules for constructing quantum flow-charts

Lemma 4.3.3. Let $\sigma$ and $\tau$ be two signatures. Then we have $V_{\sigma \otimes \tau} \cong V_{\sigma} \otimes V_{\tau}$ and $V_{\sigma \oplus \tau} \cong V_{\sigma} \oplus V_{\tau}$.

Definition 4.3.4. We define a map between arrows

$$\Phi : \text{CPM}(\sigma \otimes \tau, \sigma') \xrightarrow{\cong} \text{CPM}(\sigma, \tau \otimes \tau')$$

as in Lemma 4.1.18 using the canonical basis.

Lemma 4.3.5. The category $(\text{CPM}, \otimes, (1))$ is a symmetric monoidal category. The map $\Phi$ makes CPM symmetric monoidal closed. The structure $\oplus$ and the signature $(0)$ provide a structure of biproducts.

Definition 4.3.6. Given a signature $\sigma = (n_1, \ldots, n_k)$, a tuple $A = (A_1, \ldots, A_k)$ in $V_{\sigma}$ is hermitian (respectively positive) if each matrix $A_i$ is hermitian (respectively positive). We extend the Löwner order of Definition 3.1.25 to tuples of matrices by letting $A \leq B$ if $B - A$ is positive. We define the trace of the matrix tuple $A$ to be the sum of the traces of its components:

$$\text{tr}(A) = \sum \text{tr}(A_i).$$

Definition 4.3.7. Let $\sigma = (n_1, \ldots, n_k)$ and $\tau = (m_1, \ldots, m_l)$ be two signatures. A linear function $F : V_{\sigma} \rightarrow V_{\tau}$ is a tuple $(F_{1,1}, \ldots, F_{1,k}, \ldots, F_{n,1}, \ldots, F_{n,k})$, where $F_{i,j}$ is the component $C^{n_i} \rightarrow C^{m_j}$. The characteristic matrix tuple $\chi_F$ of the function $F$ is

$$(\chi_{F_{1,1}}, \ldots, \chi_{F_{1,k}}, \ldots, \chi_{F_{n,1}}, \ldots, \chi_{F_{n,k}}).$$

Note that since $F : V_{\sigma} \rightarrow V_{\tau}$, $\chi_F \in V_{\sigma \otimes \tau}$.

Definition 4.3.8. The category $Q$ has the same objects as $\text{CPM}$ and as arrows superoperators. A superoperator is, as in Definition 4.1.26, a completely positive map $f : \sigma \rightarrow \tau$ such that for all $A \in V_{\sigma}$, $\text{tr}(f(A)) \leq \text{tr}(A)$.
Lemma 4.3.9. The category $Q$ is symmetric monoidal and has coproducts, with the same construct as for CPM. It is not, however, closed.

Definition 4.3.10. The trace characteristic matrix tuple of a linear function $F : V_\sigma \to V_\tau$ is defined to be $\chi_F^{(tr)} = \chi_{\text{tr} \circ F} \in \mathcal{V}_\sigma$, that is, the characteristic matrix tuple of $\text{tr} \circ F$. Equivalently, $\chi_F^{(tr)} = (\text{id}_\sigma \otimes \text{tr}_\tau)(\chi_F)$.

Completely positive maps and superoperators in this generalized context still satisfy a version of Theorem 3.1.27.

Theorem 4.3.11 (Generalized Kraus Representation Theorem). Consider the signatures $\sigma$ of the form $(n_1, \ldots, n_s)$ and $\tau$ of the form $(m_1, \ldots, m_t)$. Let $F : V_\sigma \to V_\tau$ be a linear function. Then the following holds:

1. $F$ is completely positive if and only if $\chi_F$ is positive.
2. $F$ is a superoperator if and only if $\chi_F^{(tr)}$ is positive and $\chi_F^{(tr)} \subseteq I_\sigma$, where $I_\sigma \in \mathcal{V}_\sigma$ is the tuple consisting of identity matrices.
3. $F$ is a superoperator if and only if it can be written in the form

$$F(A_1, \ldots, A_s) = (\sum_{i,l} U_{1i} A_i U_{i1}^*, \ldots, \sum_{i,l} U_{si} A_s U_{is}^*),$$

for matrices $U_{ij} \in \mathbb{C}^{m_i \times n_i}$ where $\sum_{i,l} U_{ij}^* U_{ij} \subseteq I_{n_i}$ for all $i$. Here, $l$ ranges over a finite set. \qed

### 4.3.3 Interpretation of the Flow-Chart Language

It is possible to interpret a flow chart diagram as a superoperator. We state in this section the few results of \cite{Selinger2004} used in Chapter 3.

Definition 4.3.12. Let $\sigma = (n_1, \ldots, n_s)$ be a signature, and let $\sigma' = n_1 + \ldots + n_s$ be an integer regarded as a simple signature. The measurement operator $\mu_\sigma : V_\sigma \to V_\tau$ is defined as

$$\mu_\sigma \left( \begin{array}{ccc} A_{1,1} & \cdots & A_{1,s} \\ \vdots & \ddots & \vdots \\ A_{s,1} & \cdots & A_{s,s} \end{array} \right) = (A_{1,1}, A_{2,2}, \ldots, A_{s,s}),$$

where $A_{i,j} \in \mathbb{C}^{n_i \times n_j}$.

Definition 4.3.13. We extend the definition of partial trace of Definition 3.1.31 to any map of the form $(\text{tr}_\sigma \otimes \text{id}_\tau) : V_\sigma \otimes V_\tau \to V_\tau$.

Definition 4.3.14. We extend the definition of contractions of Definition 3.1.28 to linear maps. We say that $f : V_\sigma \to V_\tau$ is a contraction if it is of the form

$$f(A_1, \ldots, A_s) = (U_1 A_1 U_1^*, \ldots, U_s A_s U_s^*),$$

for contractions $U_i \in \mathbb{C}^{m_i \times n_i}$, where $\sigma = (n_1, \ldots, n_s)$ and $\tau = (m_1, \ldots, m_s)$.

Theorem 4.3.15. Every superoperator $F : V_\sigma \to V_\tau$ can be factored as $F = M \circ E \circ G$, where $G$ is a contraction, $E$ is a partial trace operator, and $M$ is a measurement operator. \qed

Theorem 4.3.16. The interpretation of any flow-chart in CPM yields a superoperator. Conversely, any superoperator is the image of a flow chart diagram under the interpretation. \qed
4.4 Extension to Higher-Order

A natural avenue of research for finding a model of higher-order quantum computation is the generalization of the category of superoperators. Selinger (2004c) investigated possible categories of normed vector spaces as model of higher order quantum computation. A challenging problem turns out to be the matching between the norm for the tensor of two spaces and the required norm on the space of functions. This study did not find any satisfactory model.

Another work in this direction is the paper of Girard (2004). In this paper, the author describes models of linear logic based on normed vector spaces, following the same constructions as for coherent spaces (Girard, 1987). The resulting category, although based on the right sort of spaces, does not yield the correct answer at base types, as pointed out by Selinger (2004c).
Chapter 5

Lambda Calculus and Semantics of Higher-Order Computation

In this chapter I will briefly describe the semantics for classical higher-order computation. The canonical tool for this purpose is a semantics, a mathematical model that will allow us to exhibit underlying structures and invariants.

For an complete introduction on lambda calculus, see [Barendregt, 1984]. An in-depth survey of categorical logic can be found in [Lambek and Scott, 1989]. Finally, references on linear logic and its semantics can be found in [Bierman, 1995; Girard, 1987; Troelstra, 1992].

5.1 Lambda Calculus

The origin of higher-order computation lies in the 1930’s when [Kleene, 1935a,b] described a formal system called lambda calculus, in order to capture the notion of computable function. Lambda calculus was shown [Church, 1936] universal in the sense that any computable function can be interpreted as an expression in the language.

In this section we briefly describe the core lambda calculus. For a thoughtful development of the theory see for example [Barendregt, 1984].

5.1.1 The Language

In the lambda calculus, functions are described explicitly as formulae. The function \( f : x \mapsto f(x) \) is written as the lambda-abstraction \( \lambda x. f(x) \). The application of a function to an argument is simply the juxtaposition of the two expressions. Thus

“let \( f : x \mapsto x^2 \) in \( f(2) \) ”

becomes \( (\lambda x.x^2)(2) \) in lambda calculus.

Formally, a lambda-term is an expression made of the following grammar, written in BNF form:

\[
\text{Term, } M, N \ ::= \ x \mid (\lambda x.M) \mid (MN) \mid \langle M, N \rangle \mid \text{fst}(M) \mid \text{snd}(M) \mid *,
\]

where \( x \) ranges over an infinite set of variables. The term \( \lambda x.M \) stands for the function that inputs \( x \) and outputs \( M \), the term \( MN \) represents the application of a function \( M \) to an argument \( N \), the term \( \langle M, N \rangle \) represents the pair composed of \( M \) and \( N \), \( * \) is the 0-tuple, and \( \text{fst}(M) \) and \( \text{snd}(M) \)

\(^1\)The BNF formulation was first introduced by [Naur et al., 1960] for a formal definition of the language ALGOL’60.
the left and right projections of the pairing. We speak of term combinator or term operator when referring to each token in the grammar definition.

The formalism extends transparently to higher-order functions: In lambda calculus, we can simply write $\lambda f.\lambda g.\lambda x.f(g(x))$ for the composition operator $f,g \mapsto f \circ g$. And the expression

\[
\text{“ let } H : (f,g) \mapsto (x \mapsto f(g(x))) \text{ in } \\
\text{let } a : x \mapsto x^2 \text{ in } \\
\text{let } b : x \mapsto x + 3 \text{ in } (H(a,b))(z) \text{ ”}
\]

for some variable $z$ simply becomes

\[
(\lambda f.\lambda g.\lambda x.f(g(x)))(\lambda x.x^2)(\lambda x.x + 3)(z).
\]

### 5.1.2 Free and Bound Variables

In (5.1.1), in the term $(\lambda f.\lambda g.\lambda x.f(g(x)))$ it should be understood that $x$ is local, and that the $x$ in $(\lambda x.x^2)$ does not interfere with the one of the previous formula. We say that the variable $x$ in $\lambda x.x^2$ is bound by the lambda-abstraction. On the other hand, the variable $z$ is not bound by anything: we say it is free. We define the set of free variables of a given term by induction as follows:

\[
\begin{align*}
FV(x) & = \{x\}, \\
FV(\lambda x.M) & = FV(M) \setminus \{x\}, \\
FV(MN) & = FV(M) \cup FV(N), \\
FV(fst(M)) & = FV(snd(M)) = FV(M), \\
FV(*) & = \{\}.
\end{align*}
\]

A variable that is not free is said to be bound. A term is called closed if it does not have any free variable, and open if it has at least one free variable.

### 5.1.3 $\alpha$-Equivalence

It should be understood that $\lambda x.x^2$ is the same term as, say, $\lambda t.t^2$. We say that the two terms are $\alpha$-equivalent. However, $\lambda f.\lambda g.\lambda x.f(g(x))$ and $\lambda g.\lambda g.\lambda x.g(g(x))$ are not $\alpha$-equivalent: the $g$ in the expression refers to the innermost $\lambda g$.

**Definition 5.1.1** (Barendregt, 1984). For any term $M$, we define the syntactic variable substitution $M[x := y]$ as the term $M$ where all syntactic occurrences of $x$ (whether they are free or not) are replaced by $y$. We define a change of bound variables in $M$ to be the replacement of a subterm $\lambda x.N$ by $\lambda t.N[x := t]$, provided that $t$ does not occur anywhere in $N$.

We say that $M$ is $\alpha$-equivalent to $N$, written $M \approx_{\alpha} N$, if $N$ results from $M$ by a series of changes of bound variables.

**Convention 5.1.2.** Terms are considered up to $\alpha$-equivalence from now on.

### 5.1.4 Operational Meaning of Lambda Calculus

We now discuss the operational meaning of the calculus by defining a rewriting system.

**Substitution**

A term of the form $(\lambda x.M)N$ is understood as “$M$ with $N$ in place of $x$”. The process of replacing $N$ by $x$ is called substitution, and we write the resulting term by $M[N/x]$. Of course, we are only allowed to modify the free occurrences of $x$, and one should check that the process does not bind any free variables. For example, the term $(\lambda x.yx)[(fx)/y]$ is not the same as $\lambda x.(fx)x$: indeed, the variable $x$ in $fx$ is free. Instead, using the $\alpha$-equivalent formulation $(\lambda t.yt)[(fx)/y]$ one sees that the term is in fact $\lambda t.(fx)t$. 

5.1. Lambda Calculus

Definition 5.1.3. Given a term $M$ and a term $P$, we define the substitution of $x$ in $M$ by $P$, written $M[P/x]$, by the following:

- $x[P/x] = P$,
- $*[P/x] = *$,
- $(MN)[P/x] = (M[P/x])(N[P/x])$,
- $((M,N))[P/x] = (M[P/x],N[P/x])$,
- $(\text{fst}(M))[P/x] = \text{fst}(M[P/x])$,
- $(\text{snd}(M))[P/x] = \text{snd}(M[P/x])$,
- $(\lambda y.M)[P/x] = \lambda y.(M[P/x])$ (if $y \neq x$ and $y \notin \text{FV}(P)$).

We write $M[M_1/x_1, \ldots, M_n/x_n]$ for $M[M_1/x_1] \ldots [M_n/x_n]$.

Reduction of Terms

The simply-typed lambda calculus is a language describing operations: application of a function to an argument, projection of a pair. To express these operations we develop a set of rules, called reduction rules. They come in two flavors: the $\beta$-reductions, which perform operations and enforce the implicit meaning of the term:

- $(\lambda x.M)N \rightarrow_\beta M[N/x]$,
- $\text{fst}((M,N)) \rightarrow_\beta M$,
- $\text{snd}((M,N)) \rightarrow_\beta N$,

and $\eta$-reductions simplifying terms:

- $\lambda x.(Mx) \rightarrow_\eta M$,
- $(\text{fst}(M), \text{snd}(M)) \rightarrow_\eta M$.

Each term on the left side of these rule is called a redex.

A context is a “term with a hole”, defined formally by the syntax

$$C[-] ::= [-] | (\lambda x.C[-]) | (C[-]M) | (MC[-]) | (C[-],M) | \text{fst}(C[-]) | \text{snd}(C[-]),$$

where $M$ stands for any term. Given a term $N$ and a context $C[-]$, we write $C[N]$ for the context $C[-]$ where $[-]$ is syntactically replaced with $N$. In this setting, we naturally extend the notion of reduction, as follows: Given any context $C[-]$, if $N$ is a redex reducing to $N'$, then the reduction $\rightarrow_i$ extends to $C[N] \rightarrow_i C[N']$, for $i = \beta, \eta$. A term with no subterm in redex form is said to be in normal form.

We denote by $\rightarrow^*$ the reflexive transitive closure of the relation $\rightarrow$. The relation $\rightarrow^*_\beta$ satisfies a property called the Church-Rosser theorem that we only mention here. For a proof of this result consult e.g. [Barendregt 1984].

Theorem 5.1.4 (Church-Rosser theorem). Suppose that $M$, $N$ and $P$ are lambda-terms such that $M \rightarrow^*_\beta N$ and such that $N \rightarrow^*_\beta P$. Then there exists a lambda-term $Z$ such that $N \rightarrow^*_\beta Z$ and $P \rightarrow^*_\beta Z$.

5.1.5 Typed Lambda Calculus

In mathematics, to a function one usually associates a domain and a codomain. So for example, when we mention the identity function $id$, it is always associated to a given space. Although one may lose some generality, we gain in legibility.
5.1. Lambda Calculus

Type System
Similarly, in order to be able to manipulate lambda-terms more easily, one can associate a type to each lambda-term. A type is an expression providing some information about the term. One can associate a type system to the untyped lambda calculus defined in Section 6.1 as follows:

\[
\text{Type } A, B \quad ::= \quad \iota \mid \top \mid A \times B \mid A \Rightarrow B.
\]

We choose an arbitrary constant type \( \iota \), and types are constructed by induction. If \( A \) and \( B \) are types, then \( A \times B \) is the type for binary products, and \( A \Rightarrow B \) is the type for functions from \( A \) to \( B \). Finally, \( \top \) stands for the type of the 0-tuple.

A typed term is the data consisting of the term and its type. The type of an open term is a function of the type of its free variables. For example, the type of \( \lambda x. (yx) \) should be a function type \( A \Rightarrow B \), depending on the type of \( y \). We define the notion of a typing judgement to formalize the concept. A typing judgement is an expression

\[
x_1 : A_1, \ldots, x_n : A_n \triangleright M : B
\]

where the free variables of \( M \) are contained in \( \{x_1, \ldots, x_n\} \), and \( B \) is the type of \( M \) when each \( x_i \) has type \( A_i \). The set \( \{x_1 : A_1, \ldots, x_n : A_n\} \) is called the typing context of the judgement, and it might be empty.

Typing Rules
The typed version of the lambda calculus presented in Section 6.1 is called the simply-typed lambda calculus. A typing judgement is said to be valid if it is derived from a typing derivation, or typing tree. A valid typing derivation is constructed using the following inductive rules:

\[
\begin{align*}
\Delta, x : A \triangleright x : A & \quad (ax), \\
\Delta \triangleright M : A & \quad \Delta \triangleright \lambda x.M : A \Rightarrow B \quad (\lambda), \\
\Delta \triangleright M : A \Rightarrow B & \quad \Delta \triangleright N : A \\ 
\Delta \triangleright (M, N) : A \times B & \quad (\times, I), \\
x : A \triangleright \ast : \top & \quad (\top, I), \\
\Delta \triangleright M : A \times B & \quad \Delta \triangleright \text{fst}(M) : A \quad (\times, E_1), \\
\Delta \triangleright M : A \times B & \quad \Delta \triangleright \text{snd}(M) : B \quad (\times, E_2).
\end{align*}
\]

Properties of Typed Terms
On one hand, we have a description of some intended properties of the language through a type system: for example, a term \( M \) of type \( A \Rightarrow B \) can only by applied to an argument of type \( A \). On the other hand, we have a rewriting system by means of reduction rules, accounting for the operational behavior of the language. Are these two descriptions compatible?

The main results that should be satisfied (and are verified in the case of the simply-typed lambda calculus) are the following.

**Lemma 5.1.5** (Substitution). If \( \Delta \triangleright N : A \) and \( \Delta, x : A \triangleright M : B \) are valid typing judgements, then \( \Delta \triangleright M[N/x] : B \) is valid.

**Theorem 5.1.6** (Subject reduction). If \( \Delta \triangleright M : A \) and if \( M \rightarrow_{\beta\eta} M' \) then \( \Delta \triangleright M' : A \) is valid.

They state that the type of a term remains constant along the reduction process. A third important result states the consistency of well-typed closed terms, in the sense that a well-typed closed term will reduce until reaching a normal form. The result is stated as follows:
Theorem 5.1.7 (Progress). If $M$ is a closed, well-typed term, then either $M$ is a normal form or $M \rightarrow_{\beta} M'$.

Axiomatic Equivalence

We say that two valid typing judgements $\Delta \vdash M : A$ and $\Delta \vdash N : A$ are axiomatically equivalent, written $\Delta \vdash M \approx_{ax} N : A$, if the relation can be derived from

\[
\begin{align*}
&\Delta \vdash (\lambda x. M) N \quad \approx_{ax} M[N/x] : A, & &\Delta \vdash \lambda x. (M x) \quad \approx_{ax} M : A \rightarrow B, \\
&\Delta \vdash \text{fst}(M, N) \quad \approx_{ax} M : A, & &\Delta \vdash \text{snd}(M, N) \approx_{ax} N : B, \\
&\Delta \vdash (\text{fst}(M), \text{snd}(M)) \approx_{ax} M : A \times B, & &\Delta \vdash x \quad \approx_{ax} * : \top,
\end{align*}
\]

and from one congruence rule per term constructor, such as

\[
\Delta \vdash M \approx_{ax} M' : A \quad \Delta \vdash N \approx_{ax} N' : B
\]

\[
\Delta \vdash MN \approx_{ax} M'N' : B.
\]

Curry Style Versus Church Style

While defining the type system, we wrote “A typed term is the data consisting of the term and its type.” There are actually two distinct ways of typing a term. One can adopt the Church-style typing convention, and consider that all of its subterms are typed. Or one can adopt the Curry-style typing convention, and see only the outside term as typed. From the point of view of the programmer, it is simpler to type a lambda-term in a Curry-style fashion. However, to be able to check whether a typed term is valid or not it is easier to have it Church-style typed.

These two ways of typing terms might or might not be equivalent: it is a question of understanding the meaning of the term. For example, consider the Curry-style typing judgement

\[
x : A \vdash (\lambda f. x)(\lambda y. y) : A.
\]

The type of the variable $x$ is given. However, the type of the variable $y$ is not mentioned anywhere and might be anything. For each possible type $B$, the typing derivation

\[
\begin{align*}
x : A, f : B \Rightarrow B \Rightarrow x : A & & x : A, y : B \Rightarrow y : B \\
x : A \Rightarrow \lambda f. x : (B \Rightarrow B) \Rightarrow A & & x : A \Rightarrow \lambda y. y : B \Rightarrow B \\
x : A \Rightarrow (\lambda f. x)(\lambda y. y) : A
\end{align*}
\]

is valid. Therefore the data consisting of a set of typed variables, a term and a type does not uniquely determine a typing derivation. In a Curry-style type system, the axiomatic equivalence is really defined on typing derivations, and not typing judgements. Obviously, in this simple example the term reduces to $x$, and thus all possible typing derivations live in the same axiomatic equivalence class. But in some more complicated language, this might not be the case, and the correspondence between typing derivations and typing judgements might not be one-to-one.

5.2 Proofs as Computations

Let us consider a typing derivation. We can concentrate on the meaning of terms, and understand the typing tree as a computation. But it is also possible to focus on the types, and see the typing tree as a proof in some logical system.
5.2. Proofs as Computations

5.2.1 Intuitionistic Logic

The logic behind the simply typed lambda calculus described in Section 5.1.5 is called intuitionistic logic. Formulae are constructed as expressions coming from the grammar

\[
A, B ::= \iota | \top | A \times B | A \Rightarrow B,
\]

where \(\iota\) ranges over a set of constants, \(\times\) is the conjunction, and \(\Rightarrow\) is the implication.

A sequent in intuitionistic logic is a pair \((\Gamma, B)\), written as \(\Gamma \vdash B\), where \(\Gamma\) is a multiset (possibly empty) of formulae \(\{A_1, \ldots, A_n\}\) and \(B\) is a formula. We read the sequent as “\(A_1\) and \(A_2\) and... and \(A_n\) implies \(B\)”, and we call \(\Gamma\) the context of the sequent.

A sequent is called valid if it can be derived from a proof. Proofs are trees of formulae defined inductively. In intuitionistic logic a proof is said to be constructive: the proof of \(A \times B\) should include the proof of \(A\) and the proof of \(B\). The proof of \(A \Rightarrow B\) should be a map from the proofs of \(A\) to the proofs of \(B\).

We will concentrate on natural deduction style proof rules, first introduced by by Gentzen (1934), where we mainly deal with the right side of the sequents. The proofs associated with the formulae presented above are constructed using the rules in Table 5.1. The rules come in two flavors:

1. the axiom \(Ax\) and two structural rules: the weakening rule \(W\) and the contraction rule \(C\),
2. introduction and elimination for each connective (except for the null-ary connective \(\top\) which has only an introduction rule).

5.2.2 Curry-Howard Isomorphism

Being able to write proofs, we now turn to the question of an equivalence relation of proofs. Given two proofs of the same sequent, when can we say that they are equal? For example, it is reasonable to expect that

\[
\begin{align*}
\frac{A, B \triangleright A}{A, B \triangleright A \times B} & \quad \frac{A, B \triangleright B}{A \times B \triangleright A} \quad \text{and} \quad \frac{A, B \triangleright A}{A \triangleright A} \quad \text{Ax}\end{align*}
\]

are the same proof. Indeed, in the first case we do not use \(A, B \triangleright B\): the proof only “forgets” it in the last step.

By comparing the rules for building proofs and the typing rules of the simply-typed lambda calculus, one can give a computational interpretation of proofs. It is known as the Curry-Howard isomorphism. Under this scheme, one can say that two proofs are equivalent if they represent two axiomatically equivalent lambda-terms.
If we re-interpret the reduction rules for the lambda calculus in the context of proof of intuitionistic linear logic, one finds a formal definition of the “similar look” of the two proofs of Equation 5.2.1. The first proof correspond to the typing judgement $x : A, y : B \vdash \pi_1((x, y)) : A$ and the second to the typing judgement $x : A, y : B \vdash x : A$.

Interpreted in the context of proofs, the $\beta$-reduction rules correspond to the removal of an introduction followed by an elimination. We can construct the following rewrite system of proofs:

\[ \begin{align*}
\pi_1 & \quad \pi_2 \\
\vdots & \quad \vdots \\
\Gamma \triangleright A & \quad \Gamma \triangleright B \\
\Gamma \triangleright A \times B & \quad \times_{I} \\
\Gamma \triangleright A & \quad \sim \\
\pi_1 & \quad \pi_2 \\
\vdots & \quad \vdots \\
\Gamma \triangleright A & \quad \Gamma \triangleright B \\
\Gamma \triangleright A \times B & \quad \times_{I} \\
\Gamma \triangleright B & \quad \sim \\
\end{align*} \]

Interpreted in the context of proofs, the $\beta$-reduction rules correspond to the removal of an introduction followed by an elimination. We can construct the following rewrite system of proofs:

\[ \begin{align*}
\pi_1 & \quad \pi_2 \\
\vdots & \quad \vdots \\
\Gamma, A \triangleright B & \quad \Rightarrow_I \\
\Gamma \triangleright A \Rightarrow B & \quad \times_{E_1} \\
\Gamma \triangleright A & \quad \sim \\
\pi_1 & \quad \pi_2 \\
\vdots & \quad \vdots \\
\Gamma, A \triangleright B & \quad \Rightarrow_E \\
\Gamma \triangleright B & \quad \sim \\
\end{align*} \]

where $\pi_1^*$ is $\pi_1$ without the $A$ in the context and whenever an axiom of $\pi_1$ is of the form $\Gamma, A, \Delta \triangleright A$ it is replaced by the proof

\[ \begin{align*}
\pi_2 \\
\vdots \\
\Gamma, \Delta \triangleright A.
\end{align*} \]

5.3 Categorical Logic

A proof can be set in relation with a term in a suitable language. However, while this describes the equivalence classes of proofs, it does not give out the internal structure of the theory.

The structure of the proof system can be extracted using a categorical description of the situation. In categorical logic, we consider a category whose objects are formulae and whose arrows $A \rightarrow B$ are equivalence classes of proofs of the sequent $A \triangleright B$. Equivalently, objects are types and arrows are equivalence classes of typing judgements $x : A \vdash M : B$.

In this section we describe the category generated by the language of Section 5.2.1 (or, equivalently, of the proof theory defined in Section 5.2.1).

**Definition 5.3.1.** Given a cartesian closed category $(\mathcal{C}, \times, \rightarrow, T)$, let $\Phi : \text{hom}(A \times B, C) \cong \text{hom}(A, B \Rightarrow C)$ be the canonical isomorphism and $\varepsilon_{A,B} : (A \Rightarrow B) \times A \rightarrow B$ the counit of the adjunction.

Given a map $\psi$ from type variables to objects of $\mathcal{C}$, one defines an interpretation of any type by induction:

\[ [A \times B]_\psi = [A]_\psi \times [B]_\psi, \quad [A \Rightarrow B]_\psi = [A]_\psi \Rightarrow [B]_\psi, \]

and one can interpret valid typing judgements of the simply-typed lambda calculus as morphisms in $\mathcal{C}$:

\[ [x_1 : A_1, \ldots, x_n : A_n \vdash M : B]_\psi : [A_1]_\psi \times \cdots \times [A_n]_\psi \rightarrow [B]_\psi. \]
5.4 Lambda Calculus and Side Effects

Axiom:
\[ \Delta, x : A \triangleright x : A \]
\[ \pi^2 : [\Delta] \times [A] \to [A] \]

Unit:
\[ \Delta \triangleright \ast : \top \]
\[ \bigcirc_{[\Delta]} : [\Delta] \to T \]

Product:
\[ \Delta \triangleright M : A \quad \Delta \triangleright N : A \]
\[ \Delta \triangleright \langle M, N \rangle : A \times B \]
\[ f : [\Delta] \to [A] \quad g : [\Delta] \to [B] \]
\[ \langle f, g \rangle : [\Delta] \to [A] \times [B] \]

Application:
\[ \Delta \triangleright M : A \Rightarrow B \quad \Delta \triangleright N : A \]
\[ \Delta \triangleright MN : B \]
\[ f : [\Delta] \to [A] \Rightarrow [B] \quad g : [\Delta] \to [A] \]
\[ \Phi(f) : [\Delta] \to [A] \Rightarrow [B] \]

Abstraction:
\[ \Delta, x : A \triangleright M : B \]
\[ \Delta \triangleright \lambda x. M : A \Rightarrow B \]
\[ f : [\Delta] \times [A] \to [B] \]
\[ \Phi(f) : [\Delta] \to [A] \Rightarrow [B] \]

Table 5.2: Interpretation of the simply typed lambda calculus

They are defined by induction as in Table 5.2. The denotation of a context \( \Delta = x_1 : A_1, \ldots, x_n : A_n \) is defined by
\[ [\Delta]_{\psi} = [A_1]_{\psi} \times \cdots \times [A_n]_{\psi}. \]
If the context \( \Delta \) is empty, then \([\Delta] = \top\). For legibility one drops the \( \psi \) on the symbol \([\cdot]_{\psi}\).

Lemma 5.3.2. The interpretation is sound: If \( \Delta \triangleright M \approx_{ax} M' : A \) then
\[ [\Delta \triangleright M : A] = [\Delta \triangleright M' : A]. \]

Definition 5.3.3. Let \( C^\text{st}_\lambda \) be the category defined as follows:
- Objects are types of the simply typed lambda calculus.
- Arrows from \( A \) to \( B \) are \( \beta \)-equivalence classes of typing judgements \( x : A \triangleright M : B \).
- The identity map on \( A \) is \( x : A \triangleright x : A \), and the composition of \( x : A \triangleright M : B \) and \( y : B \triangleright N : C \) is \( x : A \triangleright (\lambda y.N)M : C \).

Lemma 5.3.4. The category \( C^\text{st}_\lambda \) is cartesian closed.

Theorem 5.3.5. The simply-typed lambda calculus is an internal language for cartesian categories: In \( C^\text{st}_\lambda \), we have
\[ [x : A \triangleright M : B]_{C^\text{st}_\lambda} \approx_{ax} (x : A \triangleright M : B). \]

5.4 Lambda Calculus and Side Effects

5.4.1 Pure Versus Impure Calculus.

The simply typed lambda calculus as model of computation is slightly restrictive: It allow only pure computations, that is, computations with no side effects. A program is said to produce some side effect if the returned value does not entirely describe the behaviour of the program. Here are several examples of side effects:
5.4. Lambda Calculus and Side Effects

1. Probabilistic choice. A program that tosses a coin along the computation will have side effects: two runs of the program might not give the same output value.

2. Non-termination. A program that can diverge (i.e. not return anything) will have side effects, since no value can describe the behaviour of the program.

3. External state. A program that read and/or write some data on some external state is subject to side-effects: the value the program output might depend on the external state.

5.4.2 Reduction Strategies

In the event of side effects, the order of reduction of the redexes might influence the output, or even the behaviour of the program (in the case of divergence, for example). The description of a program allowing side effects has to come with a description of values and a choice of reduction strategy. The values are special terms that do not reduce anymore under the chosen strategy. For a simply-typed lambda calculus with side effects, the values are defined as

\[ \text{Value} \ V, W \ ::= x | \lambda x.M | \langle V, W \rangle | \ast. \]

Two main strategies are the following:

1. Call-by-name. In this strategy, one first applies functions to arguments before evaluating them. The rules for the application is

\[ \frac{M \to M'}{MN \to M'N} \quad (\lambda x.M)N \to M[N/x]. \]

2. Call-by-value. In this strategy, one reduces arguments to values before applying a function to them. Rules for application can be written as follows:

\[ \frac{N \to N'}{MN \to MN'} \quad \frac{M \to M'}{MV \to MV} \quad (\lambda x.M)V \to M[V/x]. \]

In the following we will concentrate on a model for call-by-value based computation.

5.4.3 Towards a Semantics

The categorical analysis developed in Section 5.3 does not apply to a lambda calculus with side effects. In order to make categorical sense of the calculus, one has to separate the analysis of the values from the analysis of the computations (that is, the arbitrary terms).

The semantics is due to Moggi (1988, 1989, 1991). A categorical model for a lambda calculus with side effects is a cartesian category \((\mathcal{C}, \times, T)\) together with a strong monad \((T, \mu, \eta, t)\).

Definition 5.4.1 [Moggi 1991]. A strong monad over a monoidal category \(\mathcal{C}\) is a monad \((T, \eta, \mu)\) together with a natural transformation \(t_{A,B} : A \otimes TB \to T(A \otimes B)\), call the tensorial strength, such
that the diagrams

\[
\begin{array}{c}
\begin{array}{c}
\vspace{0.5em}
\text{Lemma 5.4.1}
\end{array}
\end{array}
\end{equation}
\]

\[
\begin{array}{c}
\begin{array}{c}
\vspace{0.5em}
\text{Remark 5.4.2 [Moggi 1991]. If the category } C \text{ is symmetric, the tensorial strength } t \text{ induces two natural transformations } T A \otimes T B \rightarrow T(A \otimes B) \text{, namely}
\end{array}
\end{array}
\end{equation}
\]

\[
\begin{array}{c}
\begin{array}{c}
\vspace{0.5em}
\text{Lemma 5.4.3. If } T \text{ is a commutative strong monad on a symmetric monoidal category } C, \text{ then the two natural transformations } \Psi_1 \text{ and } \Psi_2 \text{ make both } T \text{ monoidal.}
\end{array}
\end{array}
\end{equation}
\]

\[
\begin{array}{c}
\begin{array}{c}
\vspace{0.5em}
\text{Definition 5.4.4. A symmetric monoidal category } (C, \otimes, \top) \text{ together with a strong monad } (T, \eta, \mu) \text{ is said to have } T\text{-exponentials [Moggi 1991], or Kleisli exponentials, if it is equipped with a bifunctor } \Rightarrow : C^{op} \times C \rightarrow C, \text{ and a natural isomorphism}
\end{array}
\end{array}
\end{equation}
\]

\[
\begin{array}{c}
\begin{array}{c}
\vspace{0.5em}
\text{Lemma 5.4.5. The map } \Phi \text{ induces a natural transformation } \varepsilon_{A,B} : (A \Rightarrow B) \otimes A \rightarrow TB \text{ defined by } \Phi(id_{A \Rightarrow B}).
\end{array}
\end{array}
\end{equation}
\]

\[
\begin{array}{c}
\begin{array}{c}
\vspace{0.5em}
\text{5.4.4 Computational Model for Call-By-Value}
\end{array}
\end{array}
\end{equation}
\]

The typed lambda calculus developed by [Moggi 1991] for dealing with side-effects is called a computational lambda calculus. It is interpreted in a computational model, that is:

- a cartesian category \((C, \times, T)\),
- with a strong monad \((T, \mu, \eta, t)\) satisfying the mono requirement,
- and Kleisli exponentials \(A \Rightarrow B\) for every \(A, B\) objects in \(C\).

The values are interpreted as maps in \(C\), and the computations in \(C_T\). The category \(C\) is called the category of values and the category \(C_T\) the category of computations.
5.5 Intuitionistic Linear Logic

Linear logic is a resource-sensitive logic developed by Girard [1987]. It tries to address the fact that in classical logic, the introduction rule for the conjunction $\times$

$$\frac{\Delta \triangleright A \quad \Delta \triangleright B}{\Delta \triangleright A \times B} \times_I$$

can be derived from two distinct rules, respectively an additive and a multiplicative one:

$$\frac{\Delta \triangleright A \quad \Delta \triangleright B}{\Delta \triangleright A \times B} \times^a_I, \quad \Delta \triangleright A \quad \Gamma \triangleright B \quad \Delta, \Gamma \triangleright A \times B \times^m_I,$$

where $\Delta$ and $\Gamma$ are disjoint. If these two rules are “the same” in classical logic, it is because of the existence of the weakening and contraction rules

$$\frac{\Delta \triangleright B}{\Delta, A \triangleright B} W, \quad \frac{\Delta, A, A \triangleright B}{\Delta, A \triangleright B} C.$$

Using ($W$) and ($\times^m_I$) one can recover ($\times^a_I$):

$$\frac{\Delta, \Gamma \triangleright A \quad \Delta, \Gamma \triangleright B}{\Delta, \Gamma, \Delta, \Gamma \triangleright A \times B} \times^m_W, \quad \frac{\Delta, \Gamma \triangleright A \times B}{\Delta, \Gamma \triangleright A} W,$$

and using ($C$) and ($\times^a_I$) one can recover ($\times^m_I$):

$$\frac{\Delta, \Gamma \triangleright A}{\Delta, \Gamma \triangleright A \times B} W, \quad \frac{\Gamma \triangleright A}{\Delta, \Gamma \triangleright A \times B} \times^a_W.$$

In linear logic, the contraction and weakening rules are not valid in general, so for example $A$ and $A \times A$ are not isomorphic, and the product is split into its additive and multiplicative components $\times$ and $\otimes$.

In the intuitionistic multiplicative fragment, formulae are defined by

$$A, B \quad ::= \quad \iota \mid \top \mid A \otimes B \mid A \multimap B \mid !A,$$

where $\iota$ ranges over a set of constants, $\otimes$ is the multiplicative conjunction, called the tensor, $\top$ stands for the unit of the tensor, and $A \multimap B$ is the implication corresponding to the tensor. $!(\cdot)$ is a unary constructor for allowing weakening and contraction:

$$\frac{!A, !A \triangleright B}{!A \triangleright B} (C), \quad \frac{\triangleright B}{!A \triangleright B} (W).$$

5.6 Linear Calculi and their Interpretations

Numerous interpretations of intuitionistic linear logic have been proposed, both at an abstract level and at a computational level.

Very good references for this section are the Ph.D. theses of Bierman [1993] and Maneggia [2004] and the review of Melliès [2002].
5.6. Linear Calculi and their Interpretations

5.6.1 Earlier Models

One of the first well-known categorical descriptions of the system of proofs of linear logic was (Seely, 1989). The paper discusses the required structures for a model of linear logic, where the structure of the operator “!” is captured by a comonad arising in the context of an adjunction between a cartesian category and a symmetric monoidal category.

In his thesis, Lafont (1988a,b) also describes a model of intuitionistic linear logic where the modality ! is this time defined in terms of a comonoid structure. The logic is thought of as a type system. In that spirit, the type !A is defined via its constructors and destructors, as would be the types of integers or booleans.

Abramsky (1993) and Wadler (1992) describe a computational interpretation of intuitionistic linear logic, with a typed lambda calculus whose typing rules follow closely the inference rules of the logic. The calculus is a lambda calculus with special term constructs to account for duplicable terms.

5.6.2 Bierman’s Linear Category

The formulation generalizing all of the above descriptions is the one proposed by Bierman (1993) in his Ph.D. thesis, simplified afterward by Benton et al. (1992, 1993). The categorical description comes with a complete lambda calculus that we skip for the purpose of this thesis.

For the definition of the category, we prefer here the terminology given in Schalk (2004), and use the concept of linear exponential comonad.

**Definition 5.6.1.** Let \((C, \otimes, \top, \alpha, \lambda, \rho, \sigma)\) be a symmetric monoidal category. Let \((L, \delta, \epsilon, d^L_A, d^L_B)\) be a monoidal comonad. We say that \(L\) is a linear exponential comonad provided that

1. each object in \(C\) of the form \(LA\) is equipped with a commutative comonoid \((LA, \triangle_A, \diamond_A)\), where \(\triangle_A : LA \to LA \otimes LA\) and \(\diamond_A : LA \to \top\);
2. \(\triangle_A\) and \(\diamond_A\) are monoidal natural transformations, i.e. the following diagram

\[
\begin{array}{ccc}
LA \otimes LB & \xrightarrow{\triangle_A \otimes \triangle_B} & (LA \otimes LA) \otimes (LB \otimes LB) \\
\downarrow d^L_{A,B} & & \downarrow \swarrow \\
L(A \otimes B) & \xrightarrow{\Delta_{(A \otimes B)}} & L(A \otimes B) \otimes L(A \otimes B)
\end{array}
\]

and the diagrams

\[
\begin{array}{c}
\delta^L_A \downarrow \quad \Delta^L \otimes \Delta^L \downarrow \quad \Delta^L \otimes \Delta^L \downarrow \quad \delta^L_A \downarrow
\\
d^L_A \downarrow \quad d^L_A \otimes d^L_B \downarrow \quad d^L_A \otimes d^L_B \downarrow \quad \lambda_{\top}
\\
L \top \quad \Delta^L \otimes L \top \quad L(A \otimes B) \quad \phi_{AB}
\end{array}
\]

commutes.
3. The maps
\[ \triangle_A : (LA, \delta_A) \to (LA \otimes LA, (\delta_A \otimes \delta_A); d_A), \]
\[ \triangledown_A : (LA, \delta_A) \to (\top, d^L_\top) \]
are L-coalgebra morphisms, i.e.

\[ \begin{array}{ccc}
LA & \xrightarrow{\triangle_A} & LA \otimes LA \\
\downarrow{\delta_A} & & \downarrow{\delta_A \otimes \delta_A} \\
L^2A & \xrightarrow{\delta^L_{\otimes A}} & L^2A \otimes L^2A \\
\downarrow{d^L_{\otimes A}} & & \downarrow{d_A}
\end{array} \]

4. Every map \( \delta_A \) is a comonoid morphism \((LA, \triangledown_A, \triangle_A) \to (L^2A, \triangledown_{LA}, \triangle_{LA})\), i.e.

\[ \begin{array}{ccc}
LA & \xrightarrow{\delta_A} & L^2A \\
\downarrow{\triangle_A} & & \downarrow{\triangle_{LA}} \\
LA \otimes LA & \xrightarrow{\delta_A \otimes \delta_A} & L^2A \otimes L^2A
\end{array} \]

Definition 5.6.2 (Bierman, 1993). A linear category is a symmetric monoidal category \((C, \otimes, \top)\) with finite products \((\times, 1)\), together with a linear exponential comonad \(L\).

Barbero (1994) gave a clean formulation of the above category in terms of adjunctions. We follow Barber (1997) by not mentioning the cartesian closedness, and use the exposition of Meli\`es (2002) as reference.

Definition 5.6.3. A linear-non-linear category consists of
- A symmetric monoidal closed category \((C, \otimes, \top)\);
- a category \((M, \times, 1)\) with finite products;
- a symmetric monoidal adjunction

\[ M \xrightarrow{U} \perp \xleftarrow{F} C. \]

Lemma 5.6.4. Every linear category defines a linear-non-linear category, where \((M, \times, 1)\) is the category of coalgebras of the comonad.

Theorem 5.6.5. Every linear-non-linear category is a linear category.
Chapter 6

A Lambda Calculus for Quantum Computation

The question this thesis tries to address is the question of the meaning and the description of higher-order quantum information, in the paradigm of the QRAM model. That is, programs are written on a classical device but are given access to quantum information.

In this chapter we will describe a typed lambda calculus for quantum computation, together with an operational semantics. The requirements we have in mind for the language are the following:

1. The language should have classical control. That is, the structural aspect of the programs (pairing, tests, etc.) should be classical. Such a language will be described in Section 6.1.

2. We want the program to manipulate quantum data. So quantum information should be thought of as part of the code as much as possible. We give in Section 6.2 an abstract machine and an operational semantics for giving sense to the language.

3. We want the language to be as natural as possible for the programmer. In particular, the compiler should be the one to make sure that valid programs do not duplicate quantum variables. We do not want to have special term constructs for this. In Section 6.3 we define a type system to rule out invalid programs.

The work presented in this chapter appeared in my M.Sc. thesis [Valiron, 2004a]. It was also published in [Selinger and Valiron, 2006a, 2007].

6.1 The Language

We adapt the lambda calculus described in Section 5.1 to manipulate classical data and quantum data. We focus primarily on the classical booleans 0 and 1, on the measurement, the creation of quantum bits and the unitary operations.

Definition 6.1.1. A lambda-term is an expression made of the following core grammar, written in BNF form:

\[
\text{Term} \quad M, N, P \quad ::= \quad x \mid M \cdot N \mid \lambda x. M \mid \text{if } M \text{ then } N \text{ else } P \mid 0 \mid 1 \mid \text{meas} \mid \text{new} \mid U \mid *
\mid \langle M, N \rangle \mid \text{let } \langle x, y \rangle = M \text{ in } N,
\]

where \(x\) ranges over an infinite set of term variables and \(U\) a set of unitary gates; the term \(\text{if } M \text{ then } N \text{ else } P\) stands for a test on \(P\) with output \(M\) if true, \(N\) else; the constant terms 0 and 1 stand for the
Definition 6.1.4. Given a term $H$ for example, a fair coin can be implemented as follows:

Using this calculus, one can produce terms that compute quantum algorithms.

Example 6.1.5. 6.1. The Language 55

Convention 6.1.2. We sometimes use the shorthand notations

$$
\langle M_1, \ldots, M_n \rangle = (M_1, (M_2, \ldots)),
$$

$$
M_1M_2 \ldots M_n = ((M_1M_2)M_3) \ldots M_n
$$

We identify terms up to $\alpha$-equivalence, defined as in Section 5.3.

The notions of free and bound variables and of substitution are defined as in Chapter 5. We give the full definition for further reference.

Definition 6.1.3. The set $FV(M)$ of free variables of a term $M$ is defined as follows:

$$
FV(*) = \emptyset,
$$

$$
FV(U) = \emptyset,
$$

$$
FV(new) = \emptyset,
$$

$$
FV(meas) = \emptyset,
$$

$$
FV(0) = \emptyset,
$$

$$
FV(1) = \emptyset,
$$

$$
FV(\lambda x.M) = FV(M) \cup \{x\},
$$

$$
FV(MN) = FV(M) \cup FV(N),
$$

$$
FV(\langle M, N \rangle) = FV(M) \cup FV(N),
$$

$$
FV(\langle \langle x, y \rangle \rangle \ M in N) = FV(M) \cup (FV(N) \setminus \{x, y\}).
$$

Definition 6.1.4. Given a term $M$ and a term $P$, we define the substitution of $x$ in $M$ by $P$, written $M[P/x]$, by the following:

$$
x[P/x] = P
$$

$$
c[P/x] = c
$$

$$
*P/x = *
$$

$$
(MN)[P/x] = (M[P/x])(N[P/x])
$$

$$
((M, N))[P/x] = (M[P/x], N[P/x])
$$

$$
(\text{if } M \text{ then } N_1 \text{ else } N_2)[P/x] = \text{if } M[P/x] \text{ then } N_1[P/x] \text{ else } N_2[P/x]
$$

$$
(\lambda x.M)[P/x] = \lambda x.M
$$

$$
(\lambda y.M)[P/x] = \lambda y.(M[P/x]) \quad (if \ y \neq x \ and \ y \not\in FV(P))
$$

If $y = x$ or $z = x$:

$$
(\text{let } \langle y, z \rangle = M \text{ in } N)[P/x] = (\text{let } \langle y, z \rangle = (M[P/x]) \text{ in } N)
$$

If $y \neq x$ and $z \neq x$ (and $y, z \not\in FV(P)$):

$$
(\text{let } \langle y, z \rangle = M \text{ in } N)[P/x] = (\text{let } \langle y, z \rangle = (M[P/x]) \text{ in } (N[P/x])).
$$

Example 6.1.5. Using this calculus, one can produce terms that compute quantum algorithms. For example, a fair coin can be implemented as follows:

$$
\text{meas}(H(new\ 0)),
$$

where $H$ is the Hadamard gate.
6.2 Operational Semantics

Although we want the language to perform quantum computation, no quantum bit was added into the terms of the language. For example we might want to represent the constant function outputting a quantum bit, as follows:

\[ \lambda x. (\alpha|0\rangle + \beta|1\rangle). \]

The reason why we do not allow such a notation is the problem of entanglement. As noted in Section 3.3.2, it is not always possible to write a two quantum bit system in the form \(|\phi\rangle \otimes |\psi\rangle\).

Therefore, if \(x\) is the variable corresponding to the first quantum bit and \(y\) the one corresponding to the second in an entangled state, it is not possible to write classically the term \((\lambda f.fx)(\lambda t. (gy)t)\), as there is no means of writing \(x\) and \(y\).

6.2.1 Abstract Machine

This non-local nature of quantum information forces us to introduce a level of indirection for representing the state of a quantum program. Following the scheme of the QRAM model, we describe an abstract machine consisting of a lambda-term \(M\), a array of quantum bits \(Q\) (the QRAM), and a map linking variables in \(M\) to quantum bits in \(Q\):

**Definition 6.2.1.** A quantum closure is represented by a triple \([Q, L, M]\), where

- \(Q\) is a normalized vector of \(\otimes_{i=1}^{n} C^2\), for some \(n \geq 0\), called the quantum array.
- \(M\) is a lambda term,
- \(L\) is an injective function from a set \(|L|\) of term variables to \(\{1, \ldots, n\}\), where \(FV(M) \subseteq |L|\).

\(L\) is called the linking function.

We write \(|Q| = n\). If \(L(x_i) = i\), we will sometimes write \(L\) as the ordered list \(|x_1 \cdots x_n|\). The idea is that the variable \(x_i\) is bound in the term \(M\) to qubit number \(L(x_i)\) of the state \(Q\). We also call the pair \((Q, L)\) a quantum context. If there are no quantum bits, i.e. if \(Q \in \mathbb{C}\), we write \(Q = \mid\rangle\).

Similarly, if \(L\) is empty we write \(L = \mid\rangle\).

The purpose of the linking function is to assign specific free variables of \(M\) to specific quantum bits in \(Q\). The notion of \(\alpha\)-equivalence extends naturally to quantum closure, for instance, the states \([|1\rangle, |x\rangle, \lambda y.x\] and \([|1\rangle, |z\rangle, \lambda y.z\] are equivalent. We therefore extend the notion of \(\alpha\)-equivalence to quantum closures:

\[ [Q, |x \cdots y \cdots z\rangle, M] =_\alpha [Q, |x \cdots y' \cdots z\rangle, M[y'/y]] \]

if \(y' \notin FV(M) \cup \{x, \ldots, y, \ldots, z\}\).

6.2.2 Evaluation Strategy

Although we solved the problem of entanglement, there is another issue that prevents us from blindly using substitution, namely the probabilistic nature of the measurement.

Consider the term \(\text{plus}\) to be the boolean addition function, defined as

\[ \text{plus} = \lambda xy. \text{if } x \text{ then } (\text{if } y \text{ then } 0 \text{ else } 1) \text{ else } (\text{if } y \text{ then } 1 \text{ else } 0). \]

Now, consider the term \(M = (\lambda x. \text{plus } x x)(\text{meas}(H(new \ 0)))\). Depending of the choice made in reducing the term, we obtain a different answer, as shown below, using an intuitive reduction system.
6.2. Operational Semantics

Call-By-Value.
Reducing this in the empty environment, using the call-by-value reduction strategy (as defined in Section 5.4.2), we obtain the following reductions:
\[
[|\rangle, |\rangle, M] \rightarrow [|0\rangle, |p\rangle, (\lambda x. \text{plus} \ x \ x)(\text{meas}(H \ p))]
\rightarrow \left\{ \begin{array}{l}
\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |p\rangle, (\lambda x. \text{plus} \ x \ x)(\text{meas} \ p) \\
|1\rangle, |p\rangle, (\lambda x. \text{plus} \ x \ x)(\text{meas} \ p) 
\end{array} \right. \] (6.2.1)

where the two branches are taken with probability \( \frac{1}{2} \) each. Thus, under call-by-value reduction, this program produces the boolean value 0 with probability 1.

Call-By-Name
Reducing the same term under the call-by-name strategy, we obtain in one step
\[
[|\rangle, |\rangle, M] \rightarrow [|\rangle, |\rangle, \text{plus} \ (\text{meas}(H(\text{new} \ 0)) \ (\text{meas}(H(\text{new} \ 0)))],
\]
and then with probability \( \frac{1}{4} \),
\[
[|01\rangle, |pq\rangle, 1], [|10\rangle, |pq\rangle, 1], [|00\rangle, |pq\rangle, 0], [|11\rangle, |pq\rangle, 0].
\]
Therefore, the boolean output of this function is 0 or 1 with equal probability.

Mixed Strategy
Finally, if we mix the two reduction strategies, the program can even reduce to an ill-formed term. Namely, reducing by call-by-value until we reach the term
\[
[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |p\rangle, (\lambda x. \text{plus} \ x \ x)(\text{meas} \ p)],
\]
and then changing to call-by-name, we obtain in one step the term
\[
\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |p\rangle, \text{plus}(\text{meas} \ p)(\text{meas} \ p),
\]
which is not a valid program since there are two occurrences of the quantum bit \( p \).

Remark 6.2.2. In call-by-name, a measurement of the form \( \text{meas} \ M \) is carried over along \( \beta \)-reductions. There is no possible way to “force” the measurement to happen. Therefore, one cannot obtain the behavior of the reductions in (6.2.1) using a call-by-name procedure. However, it is possible to simulate a call-by-name reduction in call-by-value by encapsulating terms in lambda-abstractions. For example, to carry over the term \( \text{meas} \ M \) using a call-by-value reduction strategy, one can write the term as \( \lambda y. \text{meas} \ M \), with \( y \) a fresh variable.

Convention 6.2.3. Following Remark 6.2.2 we consider the call-by-value reduction strategy in the remainder of this chapter.
6.2.3 Probabilistic Reduction Systems

In order to formalize the operational semantics of the quantum lambda calculus, we introduce the notion of a probabilistic reduction system. Note that several notions of probabilistic rewrite systems have been studied in the literature (see e.g. Bournez and Hovrup, 2003; Sen et al., 2003). However, these works study rewrite system in a very general setting. For the purpose of this work, where our probabilistic reduction is quite simple, we define an abstract notion of probabilistic reduction only to capture the notion of value and error state and not to study the system itself.

Definition 6.2.4. A probabilistic reduction system is a tuple \((X, U, R, \text{prob})\) where \(X\) is a set of states, \(U \subseteq X\) is a subset of value states, \(R \subseteq (X \setminus U) \times X\) is a set of reductions, and \(\text{prob} : R \rightarrow [0, 1]\) is a probability function, where \([0, 1]\) is the real unit interval. Moreover, we impose the following conditions:

- For any \(x \in X\), \(R_x = \{ x' \mid (x, x') \in R \}\) is finite.
- \(\sum_{x' \in R_x} \text{prob}(x, x') \leq 1\)

We call \(\text{prob}\) the one-step reduction, and denote \(x \rightarrow_p y\) to be \(\text{prob}(x, y) = p\). Let us extend \(\text{prob}\) to the \(n\)-step reduction

\[
\text{prob}^0(x, y) = \begin{cases} 
0 & \text{if } x \neq y \\
1 & \text{if } x = y
\end{cases}
\]

\[
\text{prob}^1(x, y) = \begin{cases} 
\text{prob}(x, y) & \text{if } (x, y) \in R \\
0 & \text{else}
\end{cases}
\]

\[
\text{prob}^{n+1}(x, y) = \sum_{z \in R_x} \text{prob}(x, z)\text{prob}^n(z, y),
\]

and the notation is extended to \(x \rightarrow^*_p y\) to mean \(\text{prob}^n(x, y) = p\).

Definition 6.2.5. We say that \(y\) is reachable in one step with non-zero probability from \(x\), denoted \(x \rightarrow_{>0} y\) when \(x \rightarrow_p y\) with \(p > 0\). We say that \(y\) is reachable with non-zero probability from \(x\), denoted \(x \rightarrow_{\geq 0} y\) when there exists \(n \geq 0\) such that \(x \rightarrow_p^* y\) with \(p > 0\).

Definition 6.2.6. We can then compute the probability to reach \(u \in U\) from \(x\): It is a function from \(X \times U\) to \(\mathbb{R}\) defined by \(\text{prob}_U(x, u) = \sum_{n=0}^{\infty} \text{prob}^n(x, u)\). The total probability for reaching \(U\) from \(x\) is

\[
\text{prob}_U(x) = \sum_{n=0}^{\infty} \sum_{u \in U} \text{prob}^n(x, u).
\]

On the other hand, there is also the probability to diverge from \(x\), or never reaching anything. This value is

\[
\text{prob}_\infty(x) = \lim_{n \rightarrow \infty} \sum_{y \in X} \text{prob}^n(x, y).
\]

We define the error probability of \(x\) to be the number

\[
\text{prob}_{err}(x) = 1 - \text{prob}_U(x) - \text{prob}_\infty(x).
\]

Lemma 6.2.7. For all \(x \in X\), \(\text{prob}_U(x) + \text{prob}_\infty(x) \leq 1\). That is, \(0 \leq \text{prob}_{err}(x) \leq 1\). \(\square\)

Definition 6.2.8. In addition to the notion of reachability with non-zero probability, there is also a weaker notion of reachability, given by \(R\): We will say that \(y\) is reachable in one step from \(x\), written \(x \leadsto y\), if \(xRy\). By the properties of \(R\), \(x \rightarrow_{>0} y\) implies \(x \leadsto y\). As usual, \(\leadsto^*\) denotes the transitive reflexive closure of \(\leadsto\), and we say that \(y\) is reachable from \(x\) if \(x \leadsto^* y\).
Definition 6.2.9. In a probabilistic reduction system, a state \( x \) is called an error-state if \( x \not\in U \) and \( \sum_{x' \in X} \text{prob}(x, x') < 1 \). An element \( x \in X \) is consistent if there is no error-state \( e \) such that \( x \xrightarrow{e} e \).

Lemma 6.2.10. If \( x \) is consistent, then \( \text{prob}_{\text{err}}(x) = 0 \). \( \square \)

Remark 6.2.11. We need the weaker notion of reachability \( x \xrightarrow{\_} y \), in addition to reachability with non-zero probability \( x \xrightarrow{\_ \_} y \), because a null probability of getting a certain result is not an absolute warranty of its impossibility. In the QRAM, suppose we have a qubit in state \(|0\rangle\). Measuring it cannot theoretically yield the value 1, but in practice, this might happen with small probability, due to imprecision of the physical operations and decoherence. Therefore, when we prove subject reduction (see Theorem 6.4.5), we will use the stronger notion. In short: a type-safe program should not crash, even in the event of random QRAM errors.

Remark 6.2.12. The converse of Lemma 6.2.10 is false. For instance, if \( X = \{a, b\} \), \( U = \emptyset \), \( a \xrightarrow{\_} a \), and \( a \xrightarrow{\_} b \), then \( b \) is an error state, and \( b \) is reachable from \( a \), but only with probability zero. Hence \( \text{prob}_{\text{err}}(a) = 0 \), although \( a \) is inconsistent.

6.2.4 Reduction System

We define a probabilistic call-by-value reduction procedure for the quantum lambda calculus. Note that, although the reduction itself is probabilistic, the choice of which redex to reduce at each step is deterministic.

Definition 6.2.13. A value is a term of the following form:

\[
\text{Value} \quad V, W ::= x \mid \lambda x. M \mid \text{0} \mid \text{1} \mid \text{meas} \mid \text{new} \mid U \mid \star \mid \langle V, W \rangle.
\]

A quantum closure of the form \([Q, L, V]\) where \( V \) is a value is called a quantum value-state.

The reduction rules are shown in Table 6.1. We write \([Q, L, M] \xrightarrow{p} [Q', L', M']\) for a single-step reduction of states which takes place with probability \( p \). In the rule for reducing the term \( U(x_1, \ldots, x_n) \), \( U \) is an \( n \)-ary built-in unitary gate, \( j_1, \ldots, j_n \) are pairwise distinct, and \( Q' \) is the quantum state obtained from \( Q \) by applying this gate to qubits \( j_1, \ldots, j_n \). In the rule for measurement, \(|Q_0\rangle\) and \(|Q_1\rangle\) are normalized states of the form

\[
|Q_0\rangle = \sum_j \alpha_j |\phi_j^0\rangle \otimes |0\rangle \otimes |\psi_j^1\rangle, \quad |Q_1\rangle = \sum_j \beta_j |\phi_j^1\rangle \otimes |1\rangle \otimes |\psi_j^1\rangle,
\]

where \( \phi_j^0 \) and \( \phi_j^1 \) are \( i \)-qubit states (so that the measured qubit is the one pointed to by \( x_i \)). In the rule for \text{new}, \( Q \) is an \( n \)-qubit state, so that \( Q \otimes |i\rangle \) is an \((n + 1)\)-qubit state.

Definition 6.2.14. We define a weaker relation \( \sim \). This relation models the transformations that can happen in the presence of decoherence and imprecision of physical operations. We define \([Q, M] \sim [Q', M']\) to be \([Q, M] \xrightarrow{p} [Q', M']\), even when \( p = 0 \), plus the additional rule, if \( Q \) and \( Q' \) are vectors of equal dimensions: \([Q, M] \sim [Q', M]\).

Lemma 6.2.15. Let \( X \) be the state of all quantum closures and \( U \) the set of quantum value-states. Let \( \text{prob} \) be the function such that for \( x, y \in X \), \( \text{prob}(x, y) = p \) if \( x \rightarrow_p y \) and 0 else. Then \((X, U, \xrightarrow{\_}, \xrightarrow{\_})\) is a probabilistic reduction system. \( \square \)

Remark 6.2.16. This probabilistic reduction system has error states, for example, the states \([Q, L, H(x.x)]\) or \([Q, (xyz), U(x, x)]\). Such error states correspond to run-time errors. In the next section, we introduce a type system designed to rule out such error states.
6.3 Type System

We will now define a type system designed to eliminate all run-time errors arising from the reduction system of the previous section, such as the ones shown in Remark 6.2.16.

6.3.1 Types

In the lambda calculus we just defined, we need to be able to account for higher-order, products (and unit), classical booleans and quantum booleans. Since we do not want to have specific term construct for dealing with duplication and non-duplication, the information has to be encoded into the type system. We use a type system inspired from linear logic. By default, a term of type \( A \) is assumed to be non-duplicable, and duplicable terms are given the type \( A' \).

### Definition 6.3.1

Formally, we define the following type system for the lambda calculus of Section 6.1 as follows:

\[
qType A, B \defeq bit | qbit | !A | (A \to B) | \top | (A \otimes B).
\]

The constant types \( bit \) and \( qbit \) stand respectively for the classical and the quantum booleans; the type \( !A \) is for duplicable elements of type \( A \); the type \( A \to B \) for functions from \( A \) to \( B \); the type \( A \otimes B \) for pairs of elements of types \( A \) and \( B \); finally \( \top \) stands for the type of the term *.

We call the operator “!” the *exponential*.

### Convention 6.3.2

We write \(!!A\) for \(!!!\ldots！！A\), with \( n \) repetitions of \( ! \). We also use the notation \( A^{\otimes n} \) for the \( n \)-fold tensor product \( A \otimes \ldots \otimes A = \ldots (A \otimes A) \ldots \otimes A \).

The typing rules will ensure that any value of type \( !A \) is duplicable. However, there is no harm in using it only once; thus, such a value should also have type \( A \). We use a subtyping relation \cite{Breazu-Tannen1988, Pierce2002} to capture this notion.
Definition 6.3.3. We define a subtyping relation $<$ on types as follows, using the overall condition on $n$ and $m$ that $(m = 0) \lor (n \geq 1)$:

\[
\begin{align*}
\text{Ext bit} &<: \text{Ext bit} \quad \text{(bit)}, \\
\text{Ext qbit} &<: \text{Ext qbit} \quad \text{(qbit)}, \\
\text{Ext} &<: \text{Ext} \quad \text{((,)},
\end{align*}
\]

\[
\begin{align*}
A_1 &<: B_1 \quad A_2 &<: B_2 \quad (\otimes), \\
\text{Ext}(A_1 \otimes A_2) &<: \text{Ext}(B_1 \otimes B_2) \quad (\otimes), \\
A &<: A' \quad B &<: B' \quad (\rightarrow) \quad A' &<: B' \quad (\rightarrow).
\end{align*}
\]

Lemma 6.3.4. ($qType, <:)$ is reflexive and transitive. If we define an equivalence relation $\equiv$ by $A \equiv B$ if $A <: B$ and $B <: A$, ($qType/\equiv, <:)$ is a poset.

Proof. The proof uses the fact that $(m = 0) \lor (n \geq 1)$ can be rewritten as $(n = 0) \Rightarrow (m = 0)$ (where $\Rightarrow$ means “implies”). Then the result follows from the reflexivity and the transitivity of the implication.

Lemma 6.3.5. If $A <: \text{Ext}$, then $A = \text{Ext}$ for some type $A'$. Dually, if $A$ is not of the form $\text{Ext}$ and if $A <$: $\text{Ext}$, then $B$ is not of the form $\text{Ext}$.

Proof. By inspection of the cases. 

6.3.2 Typing Rules

In their definition in Section 6.3.2, we implicitly considered the terms to be typed in a Church-style fashion. Considering terms this way is closer to the programmer approach: the types of the internal subterms have to be figured out by the compiler.

Definition 6.3.6. A typing judgement is the given of a set $\Delta = \{x_1 : A_1, \ldots, x_n : A_n\}$ of typed variables, of a term $M$ and of a type $B$, written as $\Delta \vdash M : B$. We call the set $\Delta$ the typing context, or simply the context.

Given two contexts $\Delta_1$ and $\Delta_2$, we write $(\Delta_1, \Delta_2)$ for the context consisting of the variables in $\Delta_1$ and in $\Delta_2$. When described in this form, it is assumed that $|\Delta_1| \cap |\Delta_2| = \emptyset$.

A typing derivation is called valid if it can be inferred from the rules of Table 6.2. We write $\Delta$ for a context of the form $\{x_1 : A_1, \ldots, x_n : A_n\}$. We use the notation $|\Delta|$ to represent the set of (untyped) variables $\{x_1, \ldots, x_n\}$ contained in $\Delta$. In the table, the symbol $c$ spans the set of term constants $\{\text{meas, new, } U, 0, 1\}$. To each context $c$ we associate a term $A_c$, as follows:

\[
A_0, A_1 = \text{bit,} \\
A_{\text{new}} = \text{bit} \rightarrow \text{qbit}, \\
A_T = \text{qbit}^\otimes \rightarrow \text{qbit}^\otimes, \\
A_{\text{meas}} = \text{qbit} \rightarrow \text{Ext}.
\]

Remark 6.3.7. The type $\text{Ext}$ is understood as being the “most generic” one for $c$, as enforced by the typing rule ($\Delta x_2$). For example, we defined $A_{\text{new}}$ to be $\text{bit} \rightarrow \text{qbit}$. Since $\text{new}$ can take any type $B$ such that $\text{Ext} \ll B$, the term $\text{new}$ can be typed with all the types in the poset:

\[
\begin{align*}
\text{Ext} &<: \text{Ext} \\
\text{Ext} &<: \text{Ext} \rightarrow \text{Ext} \\
\text{Ext} &<: \text{Ext} \rightarrow \text{Ext} \\
\text{Ext} &<: \text{Ext} \rightarrow \text{Ext}.
\end{align*}
\]

This implies, as expected, that no created quantum bit can have the type $\text{Ext}$.

Remark 6.3.8. Note that the type system enforces the requirement that variables holding quantum data cannot be freely duplicated; thus $\lambda x.\langle x, x \rangle$ is not a valid term of type $\text{qbit} \rightarrow \text{qbit} \otimes \text{qbit}$. On the other hand, we allow variables to be discarded freely.

Note also that due to rule ($\lambda x_2$) the term $\lambda x.M$ is duplicable only if all the free variables of $M$ (other than $x$) are duplicable. This follows the call-by-value approach: since $\lambda x.M$ is a value, if it is duplicated it will be duplicated as a syntactic string of symbols, thus duplicating every single free variable of it (other than $x$).
6.4. Properties of the Type System

We briefly state the properties of the type system that are similar to the properties of the simply-typed lambda calculus of Section 5.1.5. For a full development, we refer the reader to (Valiron, 2004a).

6.4.1 Safety Properties

Lemma 6.4.1. If $\Gamma \vdash A : B$ and if $\Delta \vdash M : A$ is a valid typing judgement, then $\Gamma \vdash M : B$.

Lemma 6.4.2. If $V$ is a value and if $\Delta \vdash V : A$ is a valid typing judgement, where for all $x \in FV(V)$ then $x$ is duplicable (i.e. there exists a type $B$ such that $\{x : !B\} \subseteq \Delta$), then $\Delta \vdash V : !A$ is valid.

Lemma 6.4.3 (Substitution). If $V$ is a value, and if $\Delta, \Gamma_1, x : A \vdash M : B$ and $\Delta, \Gamma_2 \vdash V : A$ are two valid typing judgements, then $\Delta, \Gamma_1, \Gamma_2 \vdash M[V/x] : B$ is valid.
Remark 6.4.4. Note that all the rules of affine intuitionistic logic (Troelstra 1992) are derived rules of our type system except for a general promotion rule: Indeed, although the typing judgement \( \triangleright \text{meas} 0 : qbit \) is valid, the judgement \( \triangleright \text{meas} 0 : !qbit \) is not valid. However, as stated in Lemma 6.4.2, the promotion rule is true for values:

\[
\frac{!\Delta \triangleright V : A}{!\Delta \triangleright V : !A}.
\]

This point will be further developed in Chapter 8 when we will look for a categorical model of the language.

Theorem 6.4.5 (Subject reduction). Given a program \([Q, L, M]\) of type \(B\) such that there exists \([Q', L', M']\) with \([Q, L, M] \rightarrow^* [Q', L', M']\), then \([Q', L', M']\) is a program of type \(B\).

Theorem 6.4.6 (Progress). Let \([Q, L, M]\) be a program of type \(B\). Then \([Q, L, M]\) is not in an error state in the sense of Definition 6.2.9. In particular, either it is a value, or there exists some state \([Q', L', M']\) such that \([Q, L, M] \rightarrow_p [Q', L', M']\). Moreover, the total probability of all possible single-step reductions from \([Q, L, M]\) is 1.

6.4.2 Type Inference Algorithm

The fact that a well-typed term behaves well is a good property. However, it still remains to provide a type for the term. For a large class of classical lambda calculus, such a task can be automated using a type inference algorithm.

In these cases, the algorithm is built on the fact that each term admits a principal type, that is, a most general type from which all the other types can be derived. For example, in simply typed lambda calculus, the term \(M = \lambda fx.fx\) admits a principal type of the form \((X \Rightarrow Y) \Rightarrow (X \Rightarrow Y)\). Here, \(X\) and \(Y\) are type variables, and any valid type can be written in this form, for some value of \(X\) and \(Y\).

The quantum lambda calculus we defined does not satisfy the principal type property. Indeed, consider again the term \(M = \lambda fx.fx\). Naively, a principal type would be (1) the most general and (2) the smallest with respect to the subtyping relation. The most general type would have a structure of the form \((X \Rightarrow Y) \Rightarrow (X \Rightarrow Y)\). Since \(!((X \Rightarrow Y) \Rightarrow (X \Rightarrow Y))\) and \((X \Rightarrow Y) \Rightarrow (X \Rightarrow Y)\) are not valid types for \(M\), the valid types for the term \(M\), ordered by the subtyping relation (from left to right) are as follows:

\[
\frac{!((X \Rightarrow Y) \Rightarrow (X \Rightarrow Y))}{((X \Rightarrow Y) \Rightarrow (X \Rightarrow Y))}
\]

\[
\frac{!(X \Rightarrow Y) \Rightarrow (X \Rightarrow Y)}{!(X \Rightarrow Y) \Rightarrow (X \Rightarrow Y)}
\]

Note that there is no smallest element.

It is however possible to find a type inference algorithm for the quantum lambda calculus. Indeed, well-typed terms in the quantum lambda calculus are well-typed in a simply-typed version of the language. That is to say, a valid typing derivation in the quantum lambda calculus is an intuitionistic typing derivation indexed with "!". Following this idea it is possible to extract a type inference algorithm for the quantum lambda calculus. The algorithm proceeds by first finding the most general intuitionistic type for the given term, and then placing "!" whenever it is necessary. We refer the reader to (Valiron, 2004a) for the full discussion.
6.5 Examples of Algorithms

It turns out that some quantum algorithms can be efficiently understood as elements of higher-order types. We give in this section the implementation of two non-trivial quantum algorithm, the Deutsch algorithm and the teleportation procedure.

The latter one is of particular interest, since the usual formulation (see Section 6.4.1) is completely sequential.

6.5.1 The Deutsch Algorithm

The simplest example to interpret in a higher-order setting is the Deutsch algorithm. We refer the reader to Section 6.4.3 for its definition. It can be implemented in the quantum lambda calculus in the following way:

```lambda

let Deutsch U_f =
  let tens f g = \langle x,y \rangle . \langle fx, gy \rangle in
  let \langle x,y \rangle = (tens H (\lambda x.x))(U_f(H(new 0), H(new 1))) in
  meas x,

```

using the notations of Convention 6.1.2. Note that \(U_f\) is a variable that stands for a function from a two-qubit state to a two-qubit state. And indeed the function \(Deutsch\) is a higher-order function:

\[ \gg Deutsch : !((qbit \otimes qbit \multimap qbit \otimes qbit) \multimap bit) \]

is a well-typed typing judgment. Note that \(Deutsch\) is duplicable, and that \(U_f\) does not need to be duplicable, since it is used only once.

Also note that ideally, instead of \(U_f\) the algorithm takes the Boolean function \(f\). Although one can write the type of the function \(U_f: f \mapsto U_f\) as

\[ (bit \multimap bit) \multimap (qbit \otimes qbit \multimap qbit \otimes qbit), \]

this function is not representable in the quantum lambda calculus.

6.5.2 The Teleportation Procedure

Consider the teleportation algorithm as it is described in Section 6.4.1. We can embed each quantum circuit part of the procedure in a function. There is a function \(EPR : !((\top \multimap qbit \otimes qbit))\) that creates an entangled state, as in the step (1):

\[ EPR = \lambda x. \text{CNOT}(H(new 0), new 0). \]

There is a function \(\text{BellMeasure} : !(qbit \multimap (qbit \multimap bit \otimes bit))\) that takes two qubits, rotates and measures them, as in step (2):

\[ \text{BellMeasure} = \lambda q_2. \lambda q_1. (\text{let } \langle x, y \rangle = \text{CNOT}(q_1, q_2) \text{ in } \langle \text{meas}(Hx), \text{meas} y \rangle) \]

We also can define a function \(U : !(qbit \multimap (bit \otimes bit \multimap qbit))\) that takes a qubit \(q\) and two bits \(x, y\) and returns \(U_{x,y}q\), as in step (3):

\[ U = \lambda q. \lambda (x, y). \text{if } x \text{ then } (\text{if } y \text{ then } U_{11}q \text{ else } U_{10}q) \text{ else } (\text{if } y \text{ then } U_{01}q \text{ else } U_{00}q), \]
6.5. Examples of Algorithms

where the operators $U_{xy}$ are defined as in Section 3.1. The teleportation procedure can be seen as the creation of two non-duplicable functions $f$ and $g$
\[
\begin{align*}
f & : \text{qbit} \rightarrow \text{bit} \otimes \text{bit}, \\
g & : \text{bit} \otimes \text{bit} \rightarrow \text{qbit},
\end{align*}
\]
such that $(g \circ f)(x) = x$ for an arbitrary qubit $x$. We can construct such a pair of functions by the following code:
\[
\begin{align*}
\text{let } \langle x, y \rangle &= \text{EPR} \ast \text{in} \\
\text{let } f &= \text{BellMeasure } x \text{ in} \\
\text{let } g &= U y \\
\text{in } \langle f, g \rangle.
\end{align*}
\]

Note that, since $f$ and $g$ depend on the state of the qubits $x$ and $y$, respectively, these functions cannot be duplicated, which is reflected in the fact that the types of $f$ and $g$ do not contain a top-level ‘!’.

The Dense Coding Procedure

Note that the two functions $f$ and $g$ defined in the previous section also satisfy a dual property, namely that $(f \circ g)(x, y) = (x, y)$ for an arbitrary pair of classical bits. It turns out that this is precisely the higher-order description of the dense coding protocol of Section 3.1.

The pair of functions $(f, g)$ creates an isomorphism between $\text{qbit}$ and $\text{bit} \otimes \text{bit}$. This is not in contradiction with the non-duplicability of quantum information since the functions are non-duplicable: one can use the function $g$ only once to “retrieve” the quantum bit encoded into two classical booleans.

Tensor and Space-Like Separation

These two protocols have in common the fact that two parts of the algorithm take place in two different places. This space-like separation is modeled in the type system by the tensor product. It is interesting to note that an interpretation of these two complex protocols can be efficiently interpreted as one single higher-order term.

6.5.3 Type Derivation of the Teleportation Protocol

To illustrate the linear type system from Section 6.3.2, we give a complete derivation of the type of the quantum teleportation term. The notation $(L.x.y.z)$ means that Lemma $x.y.z$ is used. Computing some subtypes:

\[
\begin{array}{ll}
1 & \alpha_2 \quad !^n \alpha <: \alpha \\
2 & \alpha_2 \quad !^m \beta <: \beta \\
3 & \rightarrow, 1, 2 \quad !^k (\alpha \rightarrow !^m \beta) <: (!^n \alpha \rightarrow \psi \beta) \\
4 & (L.\text{BellMeasure}) \quad A <: A \\
5 & D, 4 \quad !A <: A
\end{array}
\]

Computing the type of $\text{EPR}$:

\[
\begin{array}{ll}
6 & \text{const}, 3 \quad \triangleright \text{new : bit} \rightarrow \text{qbit} \\
7 & \text{const}, 5 \quad \triangleright 0:\text{bit}
\end{array}
\]
Computing the type of BellMeasure:

\[
\begin{align*}
8 & \text{ app, 6, 7 } \triangleright \text{ new 0:qbit} \\
9 & \text{ const, 3 } \triangleright \text{ H:qbit} \rightarrow \text{ qbit} \\
10 & \text{ app, 9, 8 } \triangleright \text{ H(new 0):qbit} \\
11 & \otimes I, 10, 9 \triangleright \langle \text{H(new 0), new 0} : \text{qbit} \otimes \text{qbit} \\
12 & \text{ const, 3 } \quad x : \top \triangleright \text{ CNOT(qbit} \otimes \text{qbit}) \rightarrow \text{(qbit} \otimes \text{qbit)} \\
13 & \text{ app, 12, 11 } \quad x : \top \triangleright \text{ CNOT(H(new 0), new 0):qbit} \otimes \text{qbit} \\
14 & \lambda_2, 13 \quad \triangleright \lambda x. \text{CNOT(H(new 0), new 0):!(} \top \rightarrow (\text{qbit} \otimes \text{qbit}))
\end{align*}
\]

Computing the type of BellMeasure:

\[
\begin{align*}
15 & \text{ var, 1 } \quad y : \text{qbit} \triangleright y : \text{qbit} \\
16 & \text{ const, 3 } \quad \triangleright \text{ meas:qbit} \rightarrow \text{ bit} \\
17 & \text{ app, 16, 15 } \quad y : \text{qbit} \triangleright \text{ meas y:bit} \\
18 & \text{ var, 1 } \quad x : \text{qbit} \triangleright x : \text{qbit} \\
19 & \text{ app, 9, 18 } \quad x : \text{qbit} \triangleright \text{ Hx:qbit} \\
20 & \text{ app, 16, 19 } \quad x : \text{qbit} \triangleright \text{ meas(Hx):bit} \\
21 & \text{ var, 1 } \quad q_1 : \text{qbit} \triangleright q_1 : \text{qbit} \\
22 & \text{ var, 1 } \quad q_2 : \text{qbit} \triangleright q_2 : \text{qbit} \\
23 & \otimes I, 21, 22 \quad q_2 : \text{qbit}, q_1 : \text{qbit} \triangleright \langle q_1, q_2 : \text{qbit} \otimes \text{qbit} \\
24 & \text{ const, 3 } \quad \triangleright \text{ CNOT:(qbit} \otimes \text{qbit}) \rightarrow (\text{qbit} \otimes \text{qbit}) \\
25 & \text{ app, 24, 23 } \quad q_2 : \text{qbit}, q_1 : \text{qbit} \triangleright \text{ CNOT(q1, q2):qbit} \otimes \text{qbit} \\
26 & \otimes I, 20, 17 \quad x : \text{qbit}, y : \text{qbit} \triangleright \langle \text{meas(Hx), meas(y):bit} \otimes \text{bit} \\
27 & \otimes E, 25, 26 \quad q_2 : \text{qbit}, q_1 : \text{qbit} \triangleright \text{let } \langle x, y \rangle = \text{CNOT(q1, q2)} \\
& \quad \text{in } \langle \text{meas(Hx), meas(y):bit} \otimes \text{bit} \\
28 & \lambda_1, 27 \quad q_2 : \text{qbit} \triangleright \lambda q_1. \text{(let } \langle x, y \rangle = \text{CNOT(q1, q2)} \\
& \quad \text{in } \langle \text{meas(Hx), meas(y):bit} \otimes \text{bit} \\
29 & \lambda_2, 28 \quad \triangleright \lambda q_2. \lambda q_1. \text{(let } \langle x, y \rangle = \text{CNOT(q1, q2)} \\
& \quad \text{in } \langle \text{meas(Hx), meas(y):!(qbit} \otimes \text{bit} \rightarrow \text{bit} \otimes \text{bit}))}
\end{align*}
\]

Computing the type of U:

\[
\begin{align*}
30 & \text{ var, 1 } \quad q : \text{qbit} \triangleright q : \text{qbit} \\
31 & \text{ const, 3 } \quad \triangleright U_{ij}:qbit \rightarrow qbit \\
32 & \text{ app, 30, 31 } \quad q : \text{qbit} \triangleright U_{ij} : q : \text{qbit} \\
33 & \text{ var, 1 } \quad y : \text{bit} \triangleright y : \text{!bit} \\
34 & \text{ var, 1 } \quad x : \text{bit} \triangleright x : \text{!bit} \\
35 & \text{ if, 33, 32, 32 } \quad q : \text{qbit}, y : \text{bit} \triangleright \text{if } y \text{ then } U_{11}q \text{ else } U_{10}q : \text{qbit} \\
36 & \text{ if, 34, 35, 35 } \quad q : \text{qbit}, x : \text{bit}, y : \text{bit} \triangleright \text{if } x \text{ then } (\text{if } y \text{ then } U_{11}q \text{ else } U_{10}q) \\
& \quad \text{else } (\text{if } y \text{ then } U_{01}q \text{ else } U_{00}q):qbit \\
37 & \lambda_1, 36 \quad q : \text{qbit} \triangleright \lambda (x, y). \text{if } x \text{ then } (\text{if } y \text{ then } U_{11}q \text{ else } U_{10}q) \\
& \quad \text{else } (\text{if } y \text{ then } U_{01}q \text{ else } U_{00}q):qbit \otimes \text{bit} \rightarrow \text{qbit} \\
38 & \lambda_2, 37 \quad \triangleright \lambda q. \lambda (x, y). \text{if } x \text{ then } (\text{if } y \text{ then } U_{11}q \text{ else } U_{10}q)
6.5. Examples of Algorithms


e (if y then \(U_{01}q\) else \(U_{00}q\)):!(qbit \(\rightarrow\) (bit \(\otimes\) bit \(\rightarrow\) qbit))

Finally, computing the type of the pair \((f, g)\):

\[
\begin{align*}
39 & \quad T \\
40 & \quad (L 6.4.2), 14, 5 \quad \Downarrow \text{EPR}: T \rightarrow (qbit \otimes qbit) \\
41 & \quad \text{app}, 40, 39 \quad \Downarrow \text{EPR}*: qbit \otimes qbit \\
42 & \quad (L 6.4.2), 29, 5 \quad \Downarrow \text{BellMeasure}: qbit \rightarrow (qbit \rightarrow (bit \otimes bit)) \\
43 & \quad \text{var}, 1 \quad x: qbit \triangleright x: qbit \\
44 & \quad \text{app}, 42, 43 \quad x: qbit \triangleright \text{BellMeasure} \quad x: qbit \rightarrow (bit \otimes bit) \\
45 & \quad \text{var}, 1 \quad y: qbit \triangleright y: qbit \\
46 & \quad (L 6.4.2), 38, 5 \quad \Downarrow U: qbit \rightarrow (bit \otimes bit \rightarrow qbit) \\
47 & \quad \text{app}, 46, 45 \quad y: qbit \triangleright U \quad y: bit \otimes bit \rightarrow qbit \\
48 & \quad \text{var}, 1 \quad f: qbit \rightarrow bit \otimes bit \triangleright f: qbit \rightarrow bit \otimes bit \\
49 & \quad \text{var}, 1 \quad g: bit \otimes bit \rightarrow qbit \triangleright g: bit \otimes bit \rightarrow qbit \\
50 & \quad \otimes, 48, 49 \quad g: bit \otimes bit \rightarrow qbit, f: qbit \rightarrow bit \otimes bit \triangleright (f, g): \quad (qbit \rightarrow bit \otimes bit) \otimes (bit \otimes bit \rightarrow qbit) \\
51 & \quad \text{let}, 47, 50 \quad f: qbit \rightarrow bit \otimes bit, y: qbit \triangleright \text{let} g = U \quad y \quad \text{in} \quad (f, g): \quad (qbit \rightarrow bit \otimes bit) \otimes (bit \otimes bit \rightarrow qbit) \\
52 & \quad \text{let}, 44, 51 \quad x: qbit, y: qbit \triangleright \text{let} f = \text{BellMeasure} \quad x \quad \text{in} \quad \text{let} g = U \quad y \quad \text{in} \quad (f, g): (qbit \rightarrow bit \otimes bit) \otimes (bit \otimes bit \rightarrow qbit) \\
53 & \quad \text{let}, 41, 52 \quad \triangleright \text{let} (x, y) = \text{EPR}^* \quad \text{in} \quad \text{let} f = \text{BellMeasure} \quad x \quad \text{in} \quad \text{let} g = U \quad y \quad \text{in} \quad (f, g)): \quad (qbit \rightarrow bit \otimes bit) \otimes (bit \otimes bit \rightarrow qbit)
\end{align*}
\]

6.5.4 Reduction of the Teleportation Term

As an illustration of the reduction rules of the quantum lambda calculus we show the detailed reduction of the term from the teleportation example from Section 6.5.2. The reduction of the teleportation term corresponds to the equality \(g \circ f = id\). We use the following abbreviations:

\[
\begin{align*}
M_{p,p'} & := \text{let } f = \text{BellMeasure} \quad p \quad \text{in} \quad g = U \quad p' \quad \text{in} \quad g(f \quad p_0) \\
B_{p_1} & := \lambda q_1. (\text{let } (p, p') = \text{CNOT}(q_1, p_1) \quad \text{in} \quad \text{meas}(H(p), \text{meas} \quad p')) \\
U_{p_2} & := \lambda (x, y). \quad (\text{if } x \quad \text{then} \quad (y \quad \text{then} \quad U_{11}p_2 \quad \text{else} \quad U_{10}p_2) \quad \text{else} \quad (y \quad \text{then} \quad U_{01}p_2 \quad \text{else} \quad U_{00}p_2))
\end{align*}
\]

The reduction of the term is then as follows:

\[
\begin{align*}
& \quad \begin{bmatrix}
\alpha(0) + \beta(1), \\
\text{let } (p, p') = \text{EPR}^* \quad \text{in} \quad g = U \quad p' \quad \text{in} \quad g(f \quad p_0)
\end{bmatrix} \\
& \quad \rightarrow_1 (\alpha(0) + \beta(1)), \text{let } (p, p') = \text{CNOT}(H(00), \text{new} \quad 0) \quad \text{in} \quad M_{p,p'} \\
& \quad \rightarrow_1 ([\alpha(0) + \beta(1)] \otimes \langle 0 \rangle), \text{let } (p, p') = \text{CNOT}(H(p_1), \text{new} \quad 0) \quad \text{in} \quad M_{p,p'}
\end{align*}
\]
→₁ \[ (α|0⟩ + β|1⟩) \otimes \frac{1}{\sqrt{2}}(|0⟩ + |1⟩), let ⟨p, p'⟩ = CNOT⟨p₁, new 0⟩ in M_{p,p'} \]
→₁ \[ (α|0⟩ + β|1⟩) \otimes \frac{1}{\sqrt{2}}(|0⟩ + |1⟩) \otimes |0⟩, let ⟨p, p'⟩ = CNOT⟨p₁, p₂⟩ in M_{p,p'} \]
→₁ \[ (α|0⟩ + β|1⟩) \otimes \frac{1}{\sqrt{2}}(|00⟩ + |11⟩), let ⟨p, p'⟩ = ⟨p₁, p₂⟩ in M_{p,p'} \]
→₁ \[ (α|0⟩ + β|1⟩) \otimes \frac{1}{\sqrt{2}}(|00⟩ + |11⟩), let f = \text{BellMeasure} \ p₁ \]
\[ \text{in let } g = \text{U} \ p₂ \text{ in } g(f \ p₀) \]
→₁⁺ \[ (α|0⟩ + β|1⟩) \otimes \frac{1}{\sqrt{2}}(|00⟩ + |11⟩), U_{p₂}(B_{p₀}p₀) \]
→₁ \[ (α|0⟩ + β|1⟩) \otimes \frac{1}{\sqrt{2}}(|00⟩ + |11⟩), U_{p₂} \left( \begin{array}{c}
\text{let } ⟨p, p'⟩ = CNOT⟨p₀, p₁⟩ \\
\text{in } \langle \text{meas}(H_{p₀}), \text{meas} p' \rangle
\end{array} \right) \]
→₁ \[ \frac{1}{\sqrt{2}} \left( \begin{array}{c}
α|000⟩ + α|011⟩ \\
+ β|110⟩ + β|101⟩
\end{array} \right), U_{p₂} \left( \begin{array}{c}
\text{let } ⟨p, p'⟩ = ⟨p₀, p₁⟩ \\
\text{in } \langle \text{meas}(H_{p₀}), \text{meas} p' \rangle
\end{array} \right) \]
→₁ \[ \frac{1}{\sqrt{2}} \left( \begin{array}{c}
α|000⟩ + α|011⟩ \\
+ β|110⟩ + β|101⟩
\end{array} \right), U_{p₂} \langle \text{meas} p₀, \text{meas} p₁ \rangle \]
→₁ \[ \frac{1}{2} \left( \begin{array}{c}
α|000⟩ + α|011⟩ \\
+ α|100⟩ + α|111⟩ \\
+ β|110⟩ + β|101⟩ \\
+ β|110⟩ - β|101⟩
\end{array} \right), U_{p₂} \langle \text{meas} p₀, \text{meas} p₁ \rangle \]

6.5.5 Reduction of the Superdense Coding Term

As another example of the reduction rules, we give the reduction of the superdense coding example from Section 6.5.2. This reduction shows the equality \( f \circ g = id \). Of the four possible cases, we only give one case, namely \( (f \circ g)(0,1) = (0,1) \); the remaining cases are similar. We use the same abbreviations as above.

\[ \left[ \begin{array}{c}
\text{let } ⟨p, p'⟩ = \text{EPR}^* \\
\text{let } f = \text{BellMeasure} \ p \\
\text{in let } g = \text{U} \ p' \\
\text{in } f(g(0,1))
\end{array} \right] \]
In this chapter, we described a lambda calculus for dealing with quantum information. Given a typing judgement
\[ x : A \vdash M : B, \]
we can now give an operational description of the behavior of the term \( M \).

Another approach for understanding the language is to understand this expression as the syntactic representation of a function from some space \( A \) to some space \( B \). A denotational semantics is the description of a theory of mathematically structured spaces, where types are interpreted as spaces and typing judgements as structure-preserving maps between these spaces.

The difficulty in the case of the quantum lambda calculus is two-fold:

1. We need to account for probabilistic and quantum effects,
2. while keeping track of duplicable and non-duplicable data.

The remainder of this thesis is devoted to the study of these problems.
Chapter 7

The Linear Fragment

In this chapter, we restrict the quantum lambda calculus to the purely linear case, namely the fragment of the language where each value, classical and quantum, must be used exactly once. The linear quantum lambda calculus differs from its nonlinear cousin in that it is less sensitive to the evaluation order of terms. We give a denotational semantics for this language in a category of completely positive maps, and we show that it is fully abstract with respect to the operational semantics.

The plan of the chapter is as follows. First we briefly describe the language and the type system. Then we develop for it an operational semantics similar to the one developed in Section 6.2.4, and we define a notion of axiomatic equivalence of terms. Finally we build a denotational semantics for the language, and we show the soundness of the axiomatic equivalence with respect to the operational semantics, as well as the full abstraction of the denotational semantics. An extended abstract of the results presented in this chapter has been published in Selinger and Valiron (2006b).

7.1 A Linear Lambda Calculus for Quantum Computation

In Chapter 6 we defined a lambda calculus for quantum computation with classical control. This language was defined in a Curry-style manner. Although this makes sense from the point of view of the programmer, this typing paradigm is harder to tackle for the semantics. Indeed, we shall define the interpretation of a valid typing judgement by induction on its typing derivation. A one-to-one correspondence between typing judgements and typing derivation is therefore required.

We begin by re-adapting the definitions and results from Chapter 6 to the requirements of this study.

Definition 7.1.1. The linear quantum lambda calculus has the following (explicitly typed) terms:

Types $A, B ::= \text{bit} \mid \text{qbit} \mid A \rightarrow B \mid \top \mid A \otimes B,$

Terms $M, N, P ::= x^A \mid MN \mid \lambda x^A.M \mid (M, N) \mid \text{let } (x^A, y^B) = M \text{ in } N \mid$

if $M$ then $N$ else $P \mid 0 \mid 1 \mid \text{new} \mid \text{meas} \mid U \mid$

let $\ast = M \text{ in } N \mid \ast \mid \Omega^A_{x^A_1, \ldots, x^A_n}$.

$\Omega$ is a non-terminating term and let $\ast = M \text{ in } N$ is used to match 0-tuples. The remaining terms are as in Definition 6.1.1. We identify terms up to $\alpha$-equivalence. The set of free variables of a term $M$ is written $FV(M)$. In the following, we often write $c$ for an arbitrary constant of the language, i.e., 0, 1, meas, new, $U$, or $\ast$. 

70
7.1. A Linear Lambda Calculus for Quantum Computation

We use the same shortcuts as in Conventions 6.1.2 and 6.3.2. Also, as we did in the previous chapter, to each term constant \( c \), we associate a fixed type \( A_c \), namely

\[
\text{meas} : \text{qbit} \rightarrow \text{bit}, \quad 0, 1 : \text{bit}, \quad \text{new} : \text{bit} \rightarrow \text{qbit}, \quad U : \text{qbit}^\otimes n \rightarrow \text{qbit}^\otimes n.
\]

The only difference is the suppression of the type constructor "!", and therefore of subtyping.

As before, a typing context \( \Delta \) is a set of typed variables, written as \( \Delta = \{x_1 : A_1, \ldots, x_n : A_n\} \). A typing judgement is an expression \( \Delta \vdash M : A \), where \( \Delta \) is a list of distinct typed variables called a typing context, \( M \) is a term, and \( A \) is a type. We say that a typing judgement is valid if it follows from the typing rules given in Table 7.1. In this table, if \( \Delta = \{x_1 : A_1, \ldots, x_n : A_n\} \) we write \( \Omega^{\Delta}_{\otimes} \) in place of \( \Omega^{A_1 \otimes \cdots \otimes A_n}_{x_1, \ldots, x_n} \).

Remark 7.1.2. Note that, unlike the language of the previous chapter, there is no type constructor \(!A\). Also note that we added the term construct \( \text{let } * = M \text{ in } N \). Operationally, if we understand a “command” as a function that outputs the unit term *, this term is used for being able to “use” a command in a program. Semantically, it is simply the destructor associated to \( \top \).

Definition 7.1.3. Given a term \( M \), we define the set of its free variables using the same definition as in Definition 6.1.3, modulo the indexing on the term. We extend the definition of \( \text{FV} \) to the terms \( \Omega \) and \( \text{let } * = M \text{ in } N \) as follows:

\[
\text{FV}(\Omega^A_{x_1, \ldots, x_n}) = \{x_1, \ldots, x_n\}, \quad \text{FV(\text{let } * = M \text{ in } N)} = \text{FV}(M) \cup \text{FV}(N).
\]

Lemma 7.1.4. Suppose that \( \Delta \vdash M : A \) is a valid typing judgement. Then the set of free variables \( \text{FV}(M) \) is equal to \(|\Delta|\).

Proof. Consider a typing derivation \( \pi \) of \( \Delta \vdash M : A \). We prove the result by induction on \( \pi \).

(\( \text{ax}_1 \)). The derivation is of the form \( x : A \vdash x : A \), and \( \text{FV}(x) = \{x\} \).

(\( \text{ax}_2 \)). The derivation is of the form \( \vdash c : A \), and \( \text{FV}(c) = \emptyset \).

(\( \otimes J \)). The derivation is of the form \( \vdash * : \top \), and \( \text{FV}(* ) = \emptyset \).
(if). The derivation is of the form $\Delta, \Gamma \vdash \text{if } P \text{ then } N_1 \text{ else } N_2 : A$, where

$$\Delta \vdash P : \text{bit}, \quad \Delta \vdash N_1 : A, \quad \Delta \vdash N_2 : A.$$ 

By induction hypothesis, $FV(P) = |\Delta|$, $FV(N_1) = |\Gamma|$ and $FV(N_2) = |\Gamma|$. Therefore,

$$FV(\text{if } P \text{ then } N_1 \text{ else } N_2) = FV(P) \cup FV(N_1) \cup FV(N_2) = |\Delta| \cup |\Gamma| = |\Delta, \Gamma|.$$ 

(Ω). The derivation is of the form $\Delta \vdash \Omega^A_\Delta : A$, and $FV(\Omega^A_\Delta) = |\Delta|$.

(λ). The derivation is of the form $\Delta \vdash \lambda x.N : A \rightarrow B$, where $\Delta, x : A \vdash N : B$. By induction, $FV(N) = |\Delta, x : A|$, which is $|\Delta| \cup \{x\}$. Thus $FV(\lambda x. N) = |\Delta|$.

(app). The derivation is of the form $\Gamma_1, \Gamma_2 \vdash N_1 N_2 : A$, where $\Gamma_1 \vdash N_1 : C$ and $\Delta_2 \vdash N_2 : A$. By induction hypothesis, $FV(N_1) = |\Gamma_1|$ and $FV(N_2) = |\Gamma_2|$. Therefore, $FV(N_1 N_2) = FV(N_1) \cup FV(N_2) = |\Gamma_1, \Gamma_2|$.

(⊗). The derivation is of the form $\Gamma_1, \Gamma_2 \vdash \langle N_1, N_2 \rangle : B \otimes c$, where $\Gamma_1 \vdash N_1 : C$ and $\Delta_2 \vdash N_2 : D$. By induction hypothesis, $FV(N_1) = |\Gamma_1|$ and $FV(N_2) = |\Gamma_2|$. Therefore, $FV(\langle N_1, N_2 \rangle) = FV(N_1) \cup FV(N_2) = |\Gamma_1, \Gamma_2|$.

(⊲). The derivation is of the form $\Gamma_1, \Gamma_2 \vdash \text{let } * = N_1 \text{ in } N_2 : A$, where $\Gamma_1 \vdash N_1 : A$ and $\Delta_2 \vdash N_2 : A$. By induction hypothesis, $FV(N_1) = |\Gamma_1|$ and $FV(N_2) = |\Gamma_2|$. Therefore, $FV(\text{let } * = N_1 \text{ in } N_2) = FV(N_1) \cup FV(N_2) = |\Gamma_1, \Gamma_2|$.

Lemma 7.1.5. Consider a valid typing judgement $\Delta \vdash M : A$. Then the type $A$ is completely determined by $\Delta$ and $M$, and there exists only one derivation for the typing judgement.

Proof. The proof is done by induction on the size of the term $M$, using Lemma 7.1.4 and noticing that for every term construct only one possible typing rule does apply.

Definition 7.1.6. Let $\Gamma \vdash N : A$ be a valid typing judgement, let $M$ be a term such that $FV(M) \cap |\Gamma| = \emptyset$, and let $x$ be a term variable. We define the substitution of $x$ in $M$ by $N$, written $M[N/x]$, as we did it in Definition 7.1.4 (modulo the type indexation). We extend this definition to the two term constructs $\Omega^A_\xi$ and let $* = M$ in $N$ as follows. If $\Delta = (\Delta', x : B)$ for some type $B$, we define $\Omega^A_{\Delta,x,B}[N/x]$ as the term $\Omega^A_{\Delta',B}$. If $x \notin |\Delta|$, the substitution $\Omega^A_{\Delta}[N/x]$ is simply equal to $\Omega^A_{\Delta}$. Finally, the rule for the last construct is (let $* = M_1$ in $M_2$) $[N/x] = (\text{let } * = M_1[N/x] \text{ in } M_2[N/x])$. Note that we only make use of the typing context of $N$ in the rule concerning $\Omega$.

Lemma 7.1.7. In the context of Definition 7.1.6, suppose that the variable $x$ does not belong to $FV(M)$. Then $M[N/x] = M$.

Proof. The proof is done by induction on $M$.

$M \equiv y$. Then $y \neq x$, and for all $N$, $y[N/x] = y$.

$M \equiv c$ and $M \equiv *$. In both cases, $M[N/x] = N$ by definition.

$M \equiv \Omega^A_{\Delta}$. By definition, $FV(M) = |\Delta|$. Since $x$ does not belong to $FV(M)$, it does neither belong to $|\Delta|$. Therefore, from the definition of the substitution, $\Omega^A_{\Delta[N/x]} = \Omega^A_{\Delta}$. 

7.1. A Linear Lambda Calculus for Quantum Computation

$M \equiv \lambda y. P$. If $y = x$, then $x \notin \text{FV}(\lambda y. P)$ and by definition $\text{FV}(\lambda y. P)[N/x] = \lambda y. P$. If $y \neq x$, for $x$ not being a free variable of $M$ one needs $x$ not to be a free variable of $P$. In which case induction hypothesis applies: $P[N/x] = P$. Therefore, $M[N/x] = N$.

$M \equiv P_1 P_2$. Since $\text{FV}(P_1 P_2) = \text{FV}(P_1) \cup \text{FV}(P_2)$, if $x \notin \text{FV}(M)$, $x$ is neither in $\text{FV}(P_1)$ nor in $\text{FV}(P_2)$. Since $(P_1 P_2)[N/x] = (P_1[N/x])(P_2[N/x])$, by induction hypothesis this means that $(P_1 P_2)[N/x] = P_1 P_2$.

$M \equiv \text{if } P_1 \text{ then } P_2 \text{ else } P_3$. Since $\text{FV}(\text{if } P_1 \text{ then } P_2 \text{ else } P_3) = \text{FV}(P_1) \cup \text{FV}(P_2) \cup \text{FV}(P_3)$, if $x \notin \text{FV}(M)$, $x$ is neither in $\text{FV}(P_1)$ nor in $\text{FV}(P_2)$ nor in $\text{FV}(P_3)$. Since $(\text{if } P_1 \text{ then } P_2 \text{ else } P_3)[N/x] = P_1[N/x]$ then $P_2[N/x]$ else $P_3[N/x])$, by induction hypothesis this means that $(\text{if } P_1 \text{ then } P_2 \text{ else } P_3)[N/x] = (\text{if } P_1 \text{ then } P_2 \text{ else } P_3)$.

$M \equiv (\text{let } * = P_1 \text{ in } P_2)$. Since $\text{FV}(\text{let } * = P_1 \text{ in } P_2) = \text{FV}(P_1) \cup \text{FV}(P_2)$, if $x \notin \text{FV}(M)$, $x$ is neither in $\text{FV}(P_1)$ nor in $\text{FV}(P_2)$. Since

\[
(\text{let } * = P_1 \text{ in } P_2)[N/x] = (\text{let } * = P_1[N/x] \text{ in } P_2[N/x]),
\]

by induction hypothesis this means that $(\text{let } * = P_1 \text{ in } P_2)[N/x] = (\text{let } * = P_1 \text{ in } P_2)$.

$M \equiv (P_1, P_2)$. Since $\text{FV}((P_1, P_2)) = \text{FV}(P_1) \cup \text{FV}(P_2)$, if $x \notin \text{FV}(M)$, $x$ is neither in $\text{FV}(P_1)$ nor in $\text{FV}(P_2)$. Since $((P_1, P_2))[N/x] = (P_1[N/x], P_2[N/x])$, by induction hypothesis this means that $(P_1, P_2)[N/x] = (P_1, P_2)$.

$M \equiv (\text{let } \langle y^C, z^D \rangle = P_1 \text{ in } P_2)$. Since

\[
\text{FV}(\text{let } \langle y^C, z^D \rangle = P_1 \text{ in } P_2) = \text{FV}(P_1) \cup (\text{FV}(P_2) \setminus \{y, z\}),
\]

if $x \notin \text{FV}(M)$, $x$ is neither in $\text{FV}(P_1)$ nor in $\text{FV}(P_2) \setminus \{y, z\}$. By induction hypothesis $P_1[N/x] = P_1$. There are two cases:

If $x = y$ or $x = z$. Then $(\text{let } \langle y^C, z^D \rangle = P_1 \text{ in } P_2)[N/x] = (\text{let } \langle y^C, z^D \rangle = P_1[N/x] \text{ in } P_2)$, and we have the result.

If $x \neq y$ and $x \neq z$. Then since $x$ is not in $\text{FV}(P_2) \setminus \{y, z\}$, it is not in $\text{FV}(P_2)$. By induction hypothesis $P_2[N/x] = P_2$. Since $(\text{let } \langle y^C, z^D \rangle = P_1 \text{ in } P_2)[N/x] = (\text{let } \langle y^C, z^D \rangle = P_1[N/x] \text{ in } P_2[N/x])$, we have the result.

\[\Box\]

Lemma 7.1.8 (Substitution). Suppose that $\Delta, x : A \triangleright M : B$ and $\Gamma \triangleright N : A$ are two valid typing judgements such that $|\Delta| \cap |\Gamma| = \emptyset$. Then $\Delta, \Gamma \triangleright M[N/x] : B$ is a valid typing judgement.

Proof. We prove the result by induction on the size of $M$.

Case $M \equiv y$. The typing rule for obtaining $\Delta, x : A \triangleright M : B$ is $(ax_1)$. That is $A = B, x = y$ and $\Delta$ is empty. Thus $\Delta, \Gamma \triangleright M[N/x] : B$ becomes $\Gamma \triangleright N : A$, which is valid by hypothesis.

Case $M \equiv c$. The typing rule for obtaining $\Delta, x : A \triangleright M : B$ is $(ax_2)$. Thus $\Delta, x : A \triangleright c : B$ is valid if $(\Delta, x : A)$ is empty, and it is not. This case is therefore not to be considered.

Case $M \equiv \Omega^\Delta_{\Delta'}$. The typing rule for obtaining $\Delta, x : A \triangleright M : B$ is $(\Omega)$. Thus $\Delta' = (\Delta, x : A)$. Since $\Omega^\Delta_{\Delta', \Delta'}[N/x] = \Omega^\Delta_{\Delta, \Gamma}[N/x]$, the result is obtained by applying back the typing rule $(\Omega)$.

Case $M \equiv \lambda y^C.P$. The typing rule for obtaining $\Delta, x : A \triangleright M : B$ is $(\lambda)$. Thus $B = C \rightarrow D$ and $\Delta, x : A, y : C \triangleright P : D$. A corollary is that $y \neq x$, thus that $M[N/x] = \lambda y^C.(P[N/x])$.

By induction hypothesis, $\Delta, \Gamma, y : C \triangleright P[N/x] : D$ is valid. Applying rule $(\lambda)$, we get $\Delta, \Gamma \triangleright \lambda y^C.(P[N/x]) : C \rightarrow D$, which is the desired result.
Case $M \equiv if \text{P then } N_1 \text{ else } N_2$. The only possible typing rule for obtaining $\Delta, x : A \vdash M : B$ is (if). Then $(\Delta, x : A)$ splits into $(\Delta_1, \Delta_2)$, where

$$\Delta_1 \vdash P : \text{bit}, \quad \Delta_2 \vdash N_1 : B, \quad \Delta_2 \vdash N_2 : B.$$ 

Note that the contexts $\Delta_1$ and $\Delta_2$ do not intersect. There are two possible cases:

$x \in |\Delta_1|$. In this case $\Delta_0 = (\Delta_1', x : A)$. We are in the setting of the lemma: by induction hypothesis, $\Delta_1', \Gamma \vdash P[V/x] : \text{bit}$.

From Lemma 7.1.2, $FV(N_1) = |\Delta_2|$ and $FV(N_2) = |\Delta_2|$. Therefore $x$ is neither in $FV(N_1)$ nor in $FV(N_2)$. From Lemma 7.1.7, $M[N/x] = (if P[V/x] then N_1 else N_2)$.

Thus, applying (if), we get that $\Delta, \Gamma \vdash if P[V/x] then N_1 else N_2 : B$ is valid.

$x \in |\Delta_2|$. In this case $\Delta_1 = (\Delta_2', x : A)$. We are in the setting of the lemma: by induction hypothesis, $\Delta_2', \Gamma \vdash N_1[V/x] : B$ and $\Delta_2', \Gamma \vdash N_2[V/x] : B$

From Lemma 7.1.2, $FV(P) = |\Delta_1|$. Therefore $x$ is not in $FV(P)$. From Lemma 7.1.7, $M[N/x] = (if P then N_1[N/x] else N_2[N/x])$.

Thus, applying (if), we get that $\Delta, \Gamma \vdash if P then N_1[N/x] else N_2[N/x] : B$ is valid.

Cases $M \equiv N_1 N_2$, $(N_1, N_2)$ and $(let \; *= N_1 \; in \; N_2)$. In each case the term $M$ can be written in the form $f(N_1, N_2)$, and there is only one possible typing rule for obtaining $\Delta, x : A \vdash M : B$, namely respectively (app), $(\otimes.I)$ and $(\top.E)$. Then $(\Delta, x : A)$ splits into $(\Delta_1, \Delta_2)$, where $\Delta_1 \vdash N_1 : C_1$ and $\Delta_2 \vdash N_2 : C_2$, for some types $C_1$ and $C_2$ depending on the rule used:

<table>
<thead>
<tr>
<th>If the rule used is...</th>
<th>$f(N_1, N_2)$ is...</th>
<th>$C_1$ is...</th>
<th>$C_2$ is...</th>
<th>and $B$ is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>(app)</td>
<td>$N_1 N_2$</td>
<td>$C \otimes D$</td>
<td>$C$</td>
<td>$D$</td>
</tr>
<tr>
<td>(\otimes.I)</td>
<td>$(N_1, N_2)$</td>
<td>$C$</td>
<td>$D$</td>
<td>$C \otimes D$</td>
</tr>
<tr>
<td>(\top.E)</td>
<td>$let ; *= N_1 ; in ; N_2$</td>
<td>$\top$</td>
<td>$C$</td>
<td>$C$</td>
</tr>
</tbody>
</table>

Note that for $i = 1, 2$, the contexts $\Delta_i$ and $\Gamma$ do not intersect. There are two possible cases: $x \in |\Delta_1|$, or $x \in |\Delta_2|$. Since they are symmetric by exchanging the role of the indices 1 and 2, we only prove one of them.

Suppose that $x \in |\Delta_1|$. In this case $\Delta_1 = (\Delta_1', x : A)$. We are in the setting of the lemma: by induction hypothesis, $\Delta_1', \Gamma \vdash N_1[V/x] : C_1$. From Lemma 7.1.2, $FV(N_2) = |\Delta_2|$. Therefore $x$ is not in $FV(N_2)$. From Lemma 7.1.7, $M[N/x] = f(N_1[N/x], N_2)$.

Applying back the typing rule used, the judgement $\Delta, \Gamma \vdash f(N_1[N/x], N_2) : B$ is valid.

Case $M \equiv (let \; \langle y^C, z^D \rangle = N_1 \; in \; N_2)$. This case is similar to the previous ones: There is only one possible typing rule for obtaining $\Delta, x : A \vdash M : B$, namely $(\otimes.E)$. Then $(\Delta, x : A)$ splits into $(\Delta_1, \Delta_2)$, where $\Delta_1 \vdash N_1 : C \otimes D$ and $\Delta_2, y : C, y : D \vdash N_2 : B$.

Note that for $i = 1, 2$, the contexts $\Delta_i$ and $\Gamma$ do not intersect. There are two possible cases: $x \in |\Delta_1|$, or $x \in |\Delta_2|$. 

$x \in |\Delta_1|$. In this case $\Delta_1 = (\Delta_1', x : A)$. We are in the setting of the lemma: by induction hypothesis, $\Delta_1', \Gamma \vdash N_1[V/x] : C \otimes D$. From Lemma 7.1.2, $FV(N_2) = |\Delta_2, y : C, z : D|$. Therefore $x$ is not in $FV(N_2)$. From Lemma 7.1.7, $M[N/x] = (let \; \langle y^C, z^D \rangle = N_1[N/x] \; in \; N_2)$.

Applying back the typing rule $(\otimes.E)$, the judgement $\Delta, \Gamma \vdash let \; \langle y^C, z^D \rangle = N_1[N/x] \; in \; N_2 : B$ is valid.
7.2. Operational Semantics

We develop in this section an operational semantics similar to the one given in Section 6.2, and prove some of its properties.

7.2.1 Small Step Semantics

We adopt the definitions of quantum closures and programs from Section 6.2.1 to the linear case.

**Definition 7.2.1.** A quantum closure is a triple \([Q, L, M]\) where \(Q\) is a normalized vector in \(\otimes_{i=1}^{n} \mathbb{C}^{2}\), for some \(n \geq 0\), \(L\) is a bijective function from a set \(|L|\) of term variables to \(\{0, \ldots, n-1\}\), and \(M\) is a term. As before, \(Q\) is called a quantum array, and \(L\) is called a linking function. Note that the only difference from Definition 6.2.1 lies in the fact that \(L\) is a bijective function. We use the notations of Definition 6.2.1 and consider quantum closure up to \(\alpha\)-equivalence. Finally, we use the notion of well-typed quantum closure and program of Definition 6.3.4.

**Definition 7.2.2.** We define the call-by-value reduction strategy on program by structural induction. For this purpose we need the notion of a value. As in Definition 6.2.13, we define a value term to be of the form

\[
V, W ::= x \mid c \mid * \mid \lambda x. M \mid (V, W).
\]

A value program is a program of the form \([Q, L, V]\), where \(V\) is a value term. We set the rules to be the “classical” ones found in Table 6.2.13 plus the following “quantum” rules. In the first two rules, decompose \(Q\) into

\[
Q = \sum_{j} \alpha_{j} |\psi_{j}^{0}\rangle \otimes |0\rangle \otimes |\tilde{\psi}_{j}^{0}\rangle + \sum_{j} \beta_{j} |\psi_{j}^{1}\rangle \otimes |1\rangle \otimes |\tilde{\psi}_{j}^{1}\rangle,
\]

where \(|\psi_{j}^{0}\rangle, |\psi_{j}^{1}\rangle \in \mathbb{C}^{2^{n-1}}\) and \(|\tilde{\psi}_{j}^{0}\rangle, |\tilde{\psi}_{j}^{1}\rangle \in \mathbb{C}^{2^{n-1}}\) are basis vectors. Then, if

\[
\alpha = \sum_{j} |\alpha_{j}|^2, \quad \beta = \sum_{j} |\beta_{j}|^2,
\]

\[
[Q, x_1 \cdots x_n, meas\ x_1] \rightarrow_{m}^{\alpha} [\sum_{j} |\psi_{j}^{0}\rangle \otimes |\tilde{\psi}_{j}^{0}\rangle, x_1 \cdots x_{i-1} x_{i+1} \cdots x_n, 0],
\]

\[
[Q, x_1 \cdots x_n, meas\ x_1] \rightarrow_{\beta}^{m} [\sum_{j} |\psi_{j}^{1}\rangle \otimes |\tilde{\psi}_{j}^{1}\rangle, x_1 \cdots x_{i-1} x_{i+1} \cdots x_n, 1].
\]

In the second set of rules, if \(w\) is a fresh term variable not yet in use:

\[
[Q, x_1 \cdots x_n, new\ 0] \rightarrow_{=}^{m} [Q \otimes |0\rangle, x_1 \cdots x_n w, w],
\]
7.2. Operational Semantics

\[
\begin{align*}
[Q, L, \Omega] &\rightarrow_1^\gamma [Q, L, \Omega] & [Q, L, (\lambda x^B . M)V] &\rightarrow_1^\beta [Q, L, M[V/x]] \\
[Q, L, \text{let } \langle x^B, y^C \rangle = \langle V, W \rangle \text{ in } N] &\rightarrow_0^\oplus [Q, L, N[V/x, W/y]] \\
[Q, L, \text{let } * = * \text{ in } N] &\rightarrow_1^\gamma [Q, L, N] \\
[Q, L, \text{if } 0 \text{ then } M \text{ else } N] &\rightarrow_1^{if0} [Q, L, N] \\
[Q, L, \text{if } 1 \text{ then } M \text{ else } N] &\rightarrow_1^{if1} [Q, L, M] \\
[Q, L, N] &\rightarrow_{p^e} [Q', L', N'] \\
[Q, L, MN] &\rightarrow_{p^e} [Q', L', MN'] \\
[Q, L, M_1] &\rightarrow_{p^e} [Q', L', M'_1] \\
[Q, L, \langle M_1, M_2 \rangle] &\rightarrow_{p^e} [Q', L', \langle M'_1, M'_2 \rangle] \\
[Q, L, \text{let } x_1, x_2 = M \text{ in } N] &\rightarrow_{p^e} [Q', L', \text{let } x_1, x_2 = M' \text{ in } N] \\
[Q, L, M] &\rightarrow_{p^e} [Q', L', M'] \\
[Q, L, \text{let } \ast = M \text{ in } N] &\rightarrow_{p^e} [Q', L', \text{let } \ast = M' \text{ in } N]
\end{align*}
\]

Table 7.2: Reduction rules for the linear quantum lambda calculus

\[
[Q, \text{let } x_1 \ldots x_n, \text{new } 1] \rightarrow_1^{n_1} [Q \otimes [1], \langle x_1 \ldots x_n w \rangle, w].
\]

Finally, if \(Q'\) is the result of applying \(U\) to the quantum bits \(L(x_1), \ldots, L(x_n)\) in \(Q\):

\[
[Q, L, U \langle x_1, \ldots, x_n \rangle] \rightarrow_1^{U} [Q', L, \langle x_1, \ldots, x_n \rangle].
\]

Note that each reduction rule is named, and has a probability associated to it.

**Remark 7.2.3.** Note that since we want a linear language, we modified the measurement rule from the rule in Definition 6.2.13 by deleting the quantum bit measured from the quantum array. The two other differences from Table 6.1 are the (classical) rules concerning \(\Omega\) and let \(\ast = M \text{ in } N\). The former was defined to be a non-terminating term: it remains unchanged along the reduction. The latter matches 0-tuples. The rule follows the fact that the only 0-tuple is \(\ast\).

**Definition 7.2.4.** A program \([Q, L, M]\) reducing with the \(\omega\)-rule is called a fixed point.

**Lemma 7.2.5.** Suppose that \(P\) is a value program. Then it does not reduce. Now suppose that \(P\) is a fixed point. Then the only possible programs \(P'\) such that \(P \rightarrow_{p^e} P'\) are fixed points.

**Proof.** For the former, proof by case distinction. For the latter, proof by induction on the reduction \(P \rightarrow_{p^e} P'\).

**Lemma 7.2.6.** Suppose that \(V\) is a value such that \(x_1 : qbit, \ldots, x_n : qbit \triangleright V : A \rightarrow B\). Then \(V\) is either of the form \(\lambda x^A . N\) or it is one of the three term constants new, meas and \(U\). If \(V\) is of type \(A \otimes B\), then it is of the form \(\langle V_1, V_2 \rangle\). If it is of type bit, it is either 0 or 1. Finally, if it is of type qbit, it is a term variable.

**Proof.** The proof for the type \(A \rightarrow B\) is done by case distinction: \(V\) cannot be a variable \(x_i\) since qbit is not of the form \(A \rightarrow B\), it cannot be \(\ast\) and it cannot be of the form \(\langle V_1, V_2 \rangle\). Therefore it is
either a lambda-abstraction or a term constant. The only term constants with the right types are the one offered in the lemma. The proof for the type $A \otimes B$ is done similarly. The proofs for the last two cases are done by case distinction.

### 7.2.2 Safety Properties

**Theorem 7.2.7** (Subject reduction). If $P$ is a program of type $A$ such that $P \rightarrow_{\rho} P'$, then $P'$ is also a program of type $A$.

**Proof.** We prove the result by induction on the derivation of the relation $P \rightarrow_{\rho} P'$. If $P \equiv [Q, L, M]$, we suppose that $FV(M) = \{x_1, \ldots, x_n\} \subseteq |L|$. 

**Case ($\rightarrow_0^I$).** The only possible typing rule yielding $x_1 : qbit, \ldots, x_n : qbit \triangleright (\lambda x. B)M : A$ is (app). It means that there exists $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : qbit, \ldots, x_n : qbit)$ and such that $\Delta \triangleright (\lambda x. B)M : B \rightarrow A$ and $\Gamma \triangleright P : B$ are valid. The former can only be originated from typing rule $(\lambda)$. It means that $\Delta, x : B \triangleright M : A$ is valid. From Lemma 7.2.7.1, $\Delta, \Gamma \triangleright M[V/x] : B$ is valid. Therefore, $[Q, [x_1 \ldots x_n], M[V/x]]$ is a program of type $A$.

**Case ($\rightarrow_0^{=}$).** The only possible typing rule for getting $x_1 : qbit, \ldots, x_n : qbit \triangleright \langle V, W \rangle$ in $M : A$ is $(\otimes, E)$. It means that there exists $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : qbit, \ldots, x_n : qbit)$ and such that $\Gamma \triangleright \langle V, W \rangle : B \odot C$ and $\Delta, x : B, y : C \triangleright M : A$ are valid. The former can only be originated from typing rule $(\otimes)$. Thus $\Gamma = (\Gamma_1, \Gamma_2)$ with $\Gamma_1 \triangleright V : B$ and $\Gamma_2 \triangleright W : C$.

From Lemma 7.2.7.1, $\Delta, \Gamma_1, \Gamma_2 \triangleright M[W/y] : A$ is valid. From Lemma 7.2.7.1, $\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/y] : A$ is valid. Therefore the typing judgement $\Delta, \Gamma \triangleright M[V/x, W/y] : A$ is valid and the quantum context $[Q, [x_1 \ldots x_n], M[V/x, W/y]]$ is a program of type $A$.

**Case ($\rightarrow_{\triangleright}^E$).** The only possible typing rule for getting $x_1 : qbit, \ldots, x_n : qbit \triangleright \text{let } * = * \text{ in } N : A$ is $(\top, E)$. It means that there exists $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : qbit, \ldots, x_n : qbit)$ and such that $\Delta \triangleright * : \top$ and $\Gamma \triangleright M : A$ are valid.

The typing judgement $\Delta \triangleright * : \top$ being originated from $(\top, E)$, one has $|\Delta| = \emptyset$. Therefore $\Gamma = (x_1 : qbit, \ldots, x_n : qbit)$

This makes $[Q, [x_1 \ldots x_n], N]$ a program of type $A$.

**Cases ($\rightarrow_{\triangleright}^{if0}$) and ($\rightarrow_{\triangleright}^{if1}$).** The only possible typing rule yielding $x_1 : qbit, \ldots, x_n : qbit \triangleright \text{if } 0 \text{ then } M \text{ else } N : A$ is (if). It means that there exists $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : qbit, \ldots, x_n : qbit)$ and such that $\Delta \triangleright 1 : \text{bit}$, $\Gamma \triangleright M : A$ and $\Gamma \triangleright N : A$ are valid.

The typing judgement $\Delta \triangleright 1 : \text{bit}$ being originated from (ax2), one has $|\Delta| = \emptyset$. Therefore $\Gamma = (x_1 : qbit, \ldots, x_n : qbit)$

Therefore, $[Q, [x_1 \ldots x_n], M]$ and $[Q, [x_1 \ldots x_n], N]$ are programs of type $A$.

**Case ($\rightarrow_{\triangleright}^f$).** In this case, the term $P$ and the term $P'$ are the same: therefore, if $P$ is a program of type $A$, so is $P'$.

**Cases ($\rightarrow_{\triangleright}^m$) and ($\rightarrow_{\triangleright}^m_1$).** In these cases, $FV(meas x_1) = \{x_1\}$. The typing judgement $x_1 : qbit \triangleright meas x_1 : A$ being valid, since $meas : qbit \rightarrow \text{bit}$, by typing rule (app) we have $A = \text{bit}$. Therefore $\triangleright 0 : A$ and $\triangleright 1 : A$ are valid: in both cases, since one removes $x_i$ from $|L|$, the program $P'$ is of type $A$.

**Cases ($\rightarrow^{n0}$) and ($\rightarrow^{n1}$).** In these case, $FV(new 0) = FV(new 1) = \emptyset$. The judgements $\triangleright new 0 : A$ and $\triangleright new 1 : A$ are valid, thus since $A_{new} = \text{bit} \rightarrow qbit$, the type $A$ is equal to $qbit$. Thus $P'$ is a program of type $A$. 


Case $(-1^U)$. Since $A_U = qbit^\otimes n \rightarrow qbit^\otimes n$ for some $n$, one has

$$x_1 : qbit, \ldots, x_n : qbit \triangleright U(x_1, \ldots, x_n) : qbit^\otimes n.$$ 

Thus $A = qbit^\otimes n$. But we also have $x_1 : qbit, \ldots, x_n : qbit \triangleright (x_1, \ldots, x_n) : qbit^\otimes n$. Therefore, $P'$ is a program of type $A$.

The cases corresponding to the induction steps are directly coming from Lemma 7.1.4.

Theorem 7.2.8 (Progress). If $P$ is a program of type $A$, then either $P$ is a value program, or $P$ reduces using the reduction system of Definition 7.2.2.

Proof. Consider a valid program $[Q, |x_1 \ldots x_n], M]$ of type $A$. Then $x_1 : qbit, \ldots, x_n : qbit \triangleright M : A$ is valid. Let $\pi$ be a typing derivation of this typing judgement. We prove the result by induction on $\pi$.

Cases $(ax_1), (ax_2), (\top, I), (\lambda)$. In all of these cases, the term $M$ is a value. Thus $P$ is a value program.

Case $(if)$. The term $M$ is of the form $if M' then N_1 else N_2$. There exist contexts $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : qbit, \ldots, x_n : qbit)$ and such that $\Delta \triangleright M' : bit$ and $\Gamma \triangleright N_1, N_2 : A$. From Lemma 7.2.6, $|\Delta| = FV(M')$. Thus the quantum context $[Q, |x_1 \ldots x_n], M']$ is a program of type $bit$. By induction hypothesis, either it is a value program or it reduces to some closure $[Q', L', M'']$.

The only value of type $bit$ being 0 and 1, if it is a value, then $M'$ is respectively the term constant 0 and 1, and $P$ reduces using respectively rules $(-\nu_0)$ and $(-\nu_1)$. If it is not a value, then by congruence $P$ reduces to $[Q', L', if M'' N_1 N_2]$.

Thus, in any case the program $P$ reduces.

Case $(app)$. The term $M$ is of the form $N_1 N_2$. There exist contexts $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : qbit, \ldots, x_n : qbit)$ and such that $\Delta \triangleright N_1 : B \rightarrow A$ and $\Gamma \triangleright N_2 : B$ for some type $B$.

If $N_2$ is not a value: then the program $[Q, |x_1 \ldots x_n], N_2]$ reduces by induction hypothesis, and by congruence we are done.

If $N_2$ is a value, and if $N_1$ is not a value, then this time $[Q, |x_1 \ldots x_n], N_1]$ reduces by induction hypothesis, and by congruence we are done.

If $N_2$ and $N_1$ are values, then from Lemma 7.2.6 $N_1$ can only be one of the following:

$N_1 \equiv \lambda x^B . N$. Then $P$ reduces using rule $(\rightarrow_\beta)$

$N_1 \equiv new$. Then $B = bit$. The only values of type $bit$ being 0 and 1, the program $P$ reduces using either rule $(\rightarrow_{m_0})$ or $(\rightarrow_{m_1})$.

$N_1 \equiv meas$. Then $B = qbit$. The only values of type $qbit$ being variables, $N_2$ must be a term variable. Since $|\Gamma| \subseteq \{x_1 \ldots x_n\}$, $N_2 = x_j$ for some $j$. Then $P$ reduces using either rule $(\rightarrow_{m_0})$ or $(\rightarrow_{m_1})$.

$N_1 \equiv U^k$. Then $B = qbit^\otimes k$. The only values of type $qbit^\otimes k$ being of the form $\langle y_1, \ldots y_k \rangle$, and since $|\Gamma| \subseteq \{x_1 \ldots x_n\}$, $N_2 = \langle x_{\sigma(1)}, \ldots, x_{\sigma(k)} \rangle$ for some injective map $\sigma : \{1, \ldots, k\} \rightarrow \{1, \ldots, n\}$. Then $P$ reduces using rule $(\rightarrow_U)$.

Case $(\otimes, I)$. The term $M$ is of the form $\langle N_1, N_2 \rangle$ and $A = B_1 \otimes B_2$. There exist contexts $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : qbit, \ldots, x_n : qbit)$ and such that $\Delta \triangleright N_1 : B_1$ and $\Gamma \triangleright N_2 : B_2$.

If $N_1$ is not a value: then the program $[Q, |x_1 \ldots x_n], N_1]$ reduces by induction hypothesis, and by congruence we are done.
If $N_1$ is a value but not $N_2$, then this time $[Q, |x_1 \ldots x_n], N_2]$ reduces by induction hypothesis, and by congruence we are done.

If they are both value, so is $M$ and by definition $P$ is a value program.

Case ($\otimes.E$). The term $M$ is of the form let $\langle x^B, y^C \rangle = N_1$ in $N_2$. There exist contexts $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : \text{qbit}, \ldots, x_n : \text{qbit})$ and such that $\Delta \triangleright N_1 : B \otimes C$ and $\Gamma, x : B, y : C \triangleright N_2 : A$ are valid.

If $N_1$ is not a value: then since $|\Delta| \subseteq \{x_1 \ldots x_n\}$, the program $[Q, |x_1 \ldots x_n], N_1]$ reduces by induction hypothesis and $P$ reduces using congruence.

If $N_1$ is a value, then it is of the form $\langle V, W \rangle$, and then $P$ reduces using rule ($\rightarrow_\otimes$).

Case ($\top.E$). The term $M$ is of the form let $* = N_1$ in $N_2$. There exist contexts $\Delta$ and $\Gamma$ such that $(\Delta, \Gamma) = (x_1 : \text{qbit}, \ldots, x_n : \text{qbit})$ and such that $\Delta \triangleright N_1 : \top$ and $\Gamma \triangleright N_2 : A$ are valid.

If $N_1$ is not a value: then since $|\Delta| \subseteq \{x_1 \ldots x_n\}$, the program $[Q, |x_1 \ldots x_n], N_1]$ reduces by induction hypothesis and $P$ reduces using congruence.

If $N_1$ is a value, then it is equal to $*$, and then $P$ reduces using rule ($\rightarrow_\top$).

Case ($\Omega$). The term $M$ is of the form $\Omega_{\alpha_1 \ldots \alpha_n}^A$. Therefore $P$ reduces using the reduction rule ($\rightarrow_\omega$).

### 7.2.3 Normalization

The language being linear, the reduction has a strong relation on the length of the terms.

**Definition 7.2.9.** Let $l(M)$ be the length of a term $M$, defined recursively as an integer greater or equal to $1$ as follows:

$$
l(x^A) = l(c) = l(*) = l(\Omega) = 1, \n
l(\lambda x^A. M) = 1 + l(M), \n
l(\text{let } \langle x^B, y^C \rangle = M \text{ in } N) = 1 + l(M) + l(N), \n
l(\text{let } * = M \text{ in } N) = 1 + l(M) + l(N), \n
l(\text{if } P \text{ then } M \text{ else } N) = 1 + l(P) + \max(l(M), l(N)), \n
l(M \cdot N) = 1 + l(M) + l(N), \n
l(M, N)) = 1 + l(M) + l(N). \n$$

**Lemma 7.2.10.** Suppose that $\Delta, x : A \triangleright M : B$ and $\Gamma \triangleright N : A$ are valid. Then $l(M[N/x]) < l(M) + l(N)$.

**Proof.** The proof is done by structural induction on $M$.

$M \equiv x^C$. The computation goes like this: $l(x[N/x]) = l(N) < l(x) + l(N)$.

$M \equiv c, *, \Omega$, and $y^C$ (with $y \neq x$). In all of these cases, $M[N/x] = M$. Therefore $l(M[N/x]) = l(M)$, which by definition is strictly smaller than $l(M) + l(N)$.

$M \equiv \lambda y^C. M'$. If $y = x$ then $M[N/x] = M$. As in the previous case, we obtain the result using the definition.

If $y \neq x$, then $M[N/x] = \lambda y^A. (M'[N/x])$. By induction hypothesis, $l(M'[N/x]) < l(M') + l(N)$. Therefore, since $l(M) = 1 + l(M')$, $l(M[N/x]) = 1 + l(M'[N/x]) < 1 + l(M') + l(N) = l(M) + l(N)$.
M \equiv \text{if } P \text{ then } N_1 \text{ else } N_2. \text{ We have } l(M) = 1 + l(P) + \max(l(N_1), l(N_2)) \text{ and } \\
M[N/x] = \text{if } P[N/x] \text{ then } N_1[N/x] \text{ else } N_2[N/x]. \\

The valid judgement $\Delta, x : A \triangleright M : B$ can only come from the typing rule (if). That is, $(\Delta, x : A)$ splits into $(\Gamma_1, \Gamma_2)$, where $\Gamma_1 \triangleright P : \text{bit}$ and $\Gamma_2 \triangleright N_1, N_2 : A$.

If $x \in \Gamma_1$, then $x \not\in \Gamma_2$, and from Lemma 7.2.4, $x$ is neither in $\text{FV}(N_1)$ nor in $\text{FV}(N_2)$, therefore from Lemma 7.1.7, $N_2[N/x] = N_2$ and $N_1[N/x] = N_1$. The length of $M[N/x]$ is then $1 + l(P[N/x]) + \max(l(N_1), l(N_2))$. By induction hypothesis, $l(P[N/x]) < l(P) + l(N)$, thus $l(M[N/x]) < l(M) + l(N)$.

If $x \in \Gamma_2$, then $x \not\in \Gamma_1$, and from Lemma 7.2.4, $x \not\in \text{FV}(P)$, therefore from Lemma 7.1.7, $P[N/x] = N_1$. The length of $M[N/x]$ is then $1 + l(P) + \max(l(N_2[N/x]), l(N_1[N/x]))$.

By induction hypothesis, $l(N_1[N/x]) < l(N_1) + l(N)$ and $l(N_2[N/x]) < l(N_2) + l(N)$, thus as expected $l(M[N/x]) < l(M) + l(N)$.

**In the four remaining cases.** The term $M$ is respectively of the form

- **let** $(y^C, z^D) = N_1 \text{ in } N_2$, \hspace{1cm} $N_1N_2$, \hspace{1cm} $(N_1, N_2)$.

- In all of these cases, we have $l(M) = l(N_1) + l(N_2) + 1$. In the first cases, by $\alpha$-equivalence one can assume that $x \not= y$.

  - $l(M[N/x])$ becomes respectively:

    - let $(y^C, z^D) = N_1[N/x] \text{ in } N_2[N/x])$, \hspace{1cm} $N_1[N/x])N_2[N/x])$, \hspace{1cm} $(N_1[N/x], N_2[N/x])$.

The valid judgement $\Delta, x : A \triangleright M : B$ can only come from respectively the typing rule $(\otimes.E)$, $(\text{app})$, $(\lambda.E)$, $(\otimes.I)$. That is, $(\Delta, x : A)$ splits into $(\Gamma_1, \Gamma_2)$, where

$$\Gamma_1 \triangleright N_1 : C_1, \hspace{1cm} \Gamma_2, A \triangleright N_2 : C_2,$$

for some types $C_1, C_2$ and some context $\Lambda$, with $x \not\in \Lambda$.

If $x \in \Gamma_1$, then $x \not\in \Gamma_2$, and from Lemma 7.1.4, $x \not\in \text{FV}(N_2)$, therefore from Lemma 7.1.7, $N_2[N/x] = N_2$. The length of $M[N/x]$ is then $1 + l(N_1[N/x]) + l(N_2)$. By induction hypothesis, $l(N_1[N/x]) < l(N_1) + l(N)$, thus $l(M[N/x]) < l(M) + l(N)$.

If $x \in \Gamma_2$, then $x \not\in \Gamma_1$, and from Lemma 7.1.4, $x \not\in \text{FV}(N_1)$, therefore from Lemma 7.1.7, $N_1[N/x] = N_1$. The length of $M[N/x]$ is then $1 + l(N_2[N/x]) + l(N_1)$. By induction hypothesis, $l(N_2[N/x]) < l(N_2) + l(N)$, thus as expected $l(M[N/x]) < l(M) + l(N)$.

**Lemma 7.2.11.** If $[Q, L, M]$ is a program such that $[Q, L, M] \rightarrow_\kappa [Q', L', M']$, then either $x \not= \omega$ and $l(M') < l(M)$ or $\kappa = \omega$ and $l(M') = l(M)$. In the latter case, $[Q, L, M] = [Q', L', M']$.

**Proof.** The proof is done by induction on the derivation of the reduction $[Q, L, M] \rightarrow_\kappa [Q', L', M']$.

**Case ($\rightarrow_\beta$).** The term $M$ and the term $M'$ are respectively of the form $(\lambda x^A.N)N'$ and $N'[N/x]$.

Since $P$ is a program, $M$ is well-typed: By Lemma 7.2.10, since $l(M) = l(N) + l(N') + 2$, the length $l(M')$ verifies $l(M') < l(N') + l(N) < l(M)$. 


7.2. Operational Semantics

Case ($\rightarrow_0$). The term $M$ and the term $M'$ are respectively of the form (let $\langle x^A, y^B \rangle = (V, W) \in N$) and $N[W/y][V/x]$. Since $P$ is a program, $M$ is well-typed: By Lemma 7.2.5, since $l(M) = l(N) + l(V) + l(W) + 2$, the length of $M'$ verifies

$$l(M') = l(N[W/y][V/x]) < l(N[W/y]) + l(V) < l(N) + l(V) + l(W) < l(M).$$

Case ($\rightarrow_\tau$). The term $M$ and the term $M'$ are respectively of the form (let $* = * \in N$) and $N$. Since $l(M) = 2 + l(N)$, as requested $l(M') < l(M)$.

Cases ($\rightarrow_{\sigma_0}$) and ($\rightarrow_{\sigma_1}$). The term $M$ and the term $M'$ are respectively of the form if $0$ then $N$ else $N'$ and $N'$, or if $1$ then $N$ else $N'$ and $N$. In both cases $l(M) = 2 + \max(l(N), l(N'))$, this strictly larger than both $l(N)$ and $l(N')$: the inequality $l(M') < l(M)$ is verified.

Case ($\rightarrow_\omega$). In this case, $\kappa = \omega$ and $[Q, L, M] = [Q', L', M']$.

Cases ($\rightarrow_{n_0}$) and ($\rightarrow_{n_1}$). The term $M$ has the form $\text{meas} x$: $l(M) = 3$. The term $M'$ is the term constant 0 or the term constant 1: $l(M') = 1 < l(M)$.

Cases ($\rightarrow_{n_0}$) and ($\rightarrow_{n_1}$). The term $M$ has the form $\text{new} 0$ or $\text{new} 1$: $l(M) = 3$. The term $M'$ is a term variable: $l(M') = 1 < l(M)$.

Case ($\rightarrow_\eta$). The term $M$ is of the form $U(x_1, \ldots, x_n)$ and the term $M'$ the form $\langle x_1, \ldots, x_n \rangle$. Therefore

$$l(M') = l(x_1, \ldots, x_n) < 2 + l(x_1, \ldots, x_n) = 1 + l(U) + l(x_1, \ldots, x_n) = l(M).$$

The cases corresponding to the congruence are straightforward using the induction hypothesis. □

Theorem 7.2.12 (Normalization). Let $P = [Q, L, M]$ be a program, and let $(P_n)_n$ be a sequence of programs $P_n = [Q_n, L_n, M_n]$ such that $P_0 = P$ and such that for all $n$, either $P_n \rightarrow_{\rho_n} P_{n+1}$ or $P_n = P_n$. If $P$ does not reduce. Then $P_{l(M)}$ is either a value or a fixed point, and for all $n > l(M)$, $P_n = P_{l(M)}$.

Proof. If $(P_n)_n$ is the sequence described in the hypothesis, we show by induction on $n$ that either $P_n$ is a value, or it is a fixed point, or $l(M_n) \leq l(M) - n$: If $n = 0$: since $P_0 = P$, we are done. Suppose the result is true for $n$. Then either $P_n$ is a value, or from Theorem 7.2.11 there exists $P'$ such that $P_n \rightarrow P'$, and thus $P_{n+1}$ is such that $P_n \rightarrow_{\kappa_n} P_{n+1}$. From Lemma 7.2.13, either $\kappa_n = \omega$ or $l(M_{n+1}) < l(M_n)$. Since by induction hypothesis $l(M_n) \leq l(M) - n$, by definition we have $l(M_{n+1}) \leq l(M) - (n + 1)$.

We have $l(M_n) \geq 1$ for all $n$. Therefore the $n$ for which $P_n$ reduce are smaller than $l(M)$. And for $n = l(M)$, $P_n$ is either a fixed point (in which case it will remain so for all larger $n$ by Lemma 7.2.12) or a value (in which case it will remain so for all larger $n$ since values do not reduce, also by Lemma 7.2.11). □

7.2.4 Quantum Context and Reduction

When describing the reduction rules, we carefully separated the quantum context from the lambda-term. In this subsection we show that the precise order of quantum bits in the quantum array does not matter.

Definition 7.2.13. If $\sigma$ is a permutation of $\{1, \ldots, n\}$, we extend $\sigma$ to $\mathbb{N}$ with $\sigma(j) = j$ for $j > n$, and we define $\hat{\sigma}$ to be the corresponding permutation of quantum bits

$$\hat{\sigma}[x_1 \cdots x_n \cdots x_{n+k}] = [x_{\sigma(1)} \cdots x_{\sigma(n)} x_{n+1} \cdots x_{n+k}].$$
We say that \((Q_1, L_1)\) is \(\sigma\)-equivalent to \((Q_2, L_2)\) if \(Q_1\) and \(Q_2\) have the same size, \(Q_2 = \sigma(Q_1)\) and \(L_2 = \sigma^{-1} \circ L_1\). We write \((Q_1, L_1) =_\alpha (Q_2, L_2)\). We define an equivalence relation called alpha-equivalence on quantum contexts by \((Q_1, L_1) =_\alpha (Q_2, L_2)\) if there exists a \(\sigma\) such that \((Q_1, L_1) =_\alpha (Q_2, L_2)\).

The alpha-equivalence is sound with respect to the semantics:

**Lemma 7.2.14.** Suppose that \([Q, |x_1 \ldots x_n), M] \rightarrow_p [Q', |y_1 \ldots y_m), M']\). Then for all permutations \(\sigma\) on \(\{1, \ldots, n\}\), there exists a permutation \(\tau\) on \(\{1, \ldots, m\}\) such that \([\sigma Q, \sigma |x_1 \ldots x_n), M] \rightarrow_p [\tau Q', \tau |y_1 \ldots y_m), M']\). In the classical cases of Table 7.3, since the quantum context is not touched, choose \(\tau = \sigma\) and apply the same rule that was used at first. For the rules \((-\alpha^n_m)\) and \((-1_1^n)\), again, since \(\sigma\) only act on the \(n\) first quantum bits of the context, applying the permutation before or after the addition of a new quantum bit to the quantum array does not change the output. Thus, choosing \(\tau = \sigma \cup \{n + 1 \mapsto n + 1\}\) solves the problem.

Now, suppose that we are in the case of the rule \((-U, 1)\). In this situation we apply a unitary map on some quantum bits in the array, referred to by \(L\). Since we perform \(\sigma\) both on \(L\) and on \(Q\), it does not modify the actual unitary map performed. Therefore, again choosing \(\tau = \sigma\) gives us the answer.

In the cases \((-\alpha^n_m)\) and \((-\beta^m_1)\), the sizes of the quantum array and of the linking function change along the reduction by the removal of the entity number \(i\). However, in the program \([\sigma Q, \sigma |x_1 \ldots x_n), mean x_{\sigma(i)}\] the reduction operation will remove entity number \(\sigma(i)\). Therefore, if \(f\) and \(g\) are the maps

\[
\begin{align*}
  f(j) &= \begin{cases} 
  j & \text{if } j < i, \\
  j + 1 & \text{if } j \geq i,
  \end{cases} \\
  g(j) &= \begin{cases} 
  j & \text{if } j < \sigma(i), \\
  j - 1 & \text{if } j \geq i,
  \end{cases}
\end{align*}
\]

define \(\tau\) as \(g \circ \sigma \circ f\).

Finally, the induction cases are easy application of the induction hypothesis. 

### 7.2.5 Reduction to Values

In the reduction process, what we are really seeking is the final result of the computation. In this section we explicate the relation of programs to values.

**Definition 7.2.15.** We use the notion defined in Section 6.2.3. If \(X\) is the set of closed valid programs and \(U\) the set of values, let \(prob_U : X \times U \rightarrow [0, 1]\) be the map \(prob_U(P, V)\) that returns the total probability for a program \(P\) to end up on the value \(V\) in zero or more steps. This function is called the big-step reduction.

We also define the small-step reduction operation \(prob : X \times X \rightarrow [0, 1]\): for closed programs \(P, P'\), we define \(prob(P, P') = p\) if there is a single-step probabilistic reduction \(P \rightarrow_p P', prob(V, V) = 1\) if \(V\) is a value program, and \(prob(P, P') = 0\) in all other cases. Note that for all well-typed \(P\), \(\sum_{P' \in X} prob(P, P') = 1\).

**Lemma 7.2.16.** The reduction system defined in Definition 7.2.2 is a probabilistic reduction system.

**Proof.** By case distinction.

**Definition 7.2.17.** Given a set \(Z\), let \(CZ\) be the set of probability distributions over it. We curry the small-step reduction \(prob : X \times X \rightarrow [0, 1]\) to the map \(prob' : CX \rightarrow CZ : prob'(\sum_i \alpha_i P_i) = \sum_i \alpha_i \sum_{P' \in X} prob(P_i, P'_i)\). Similarly, we curry the function \(prob_U : X \times U \rightarrow [0, 1]\) to the map \(prob_U' : CX \rightarrow CU : prob_U'(\sum_i \alpha_i P_i) = \sum_i \alpha_i prob_U(P_i, V)\).
7.3 Denotational Semantics

Definition 7.2.18. If \( P \) is a closed well-typed program of type \( \text{bit} \), and \( b \in \{0, 1\} \), we define \( \downarrow_{\text{E}} b \) = \( \sum_{V \in U_b} \text{prob}'(P, V) \), where \( U_b \) is the set of valid programs with term the value \( b \). We say that \( P \) evaluates to \( b \) with probability \( \downarrow_{\text{E}} b \). The definition of \( \downarrow_{\text{E}} b \) can be extended in the same way to probability distributions of programs.

Lemma 7.2.19. Let \( P : A \) be a program such that \( P \rightarrow^* P' \). Then either \( \text{prob}'(P) = P', \rho = 1 \) and \( \kappa \neq m_0, m_1 \), or \( \text{prob}'(P) = \alpha P_0 + \beta P_1 \), with \( P \rightarrow^* P_0 \) and \( P \rightarrow^* P_1 \).

Proof. By induction on the reduction \( P \rightarrow^* P' \). □

Definition 7.2.20. We define a formal probability distribution of quantum closures to be \( \Gamma \models \sum_i \rho_i \left[ Q_i, L_i, M_i \right] : A \), where each \( \Gamma \models \left[ Q_i, L_i, M_i \right] : A \) is valid and \( \sum \rho_i \leq 1 \). The distribution is said to be closed if \( |\Gamma| = \emptyset \).

Lemma 7.2.21. If \( \models P : A \) is valid, so is \( \models \text{prob}' P : A \) and \( \models \text{prob}' U P : A \).

Proof. The lemma is a corollary of Theorem 7.2.7. □

Due to the strong normalization theorem, applying the map \( \text{prob}' U \) is applying the map \( \text{prob}' \) finitely many times.

Theorem 7.2.22. If \( \left[ Q, L, M \right] \) is a program, then the reduction satisfies

\[
\text{prob}^{d(M)}[Q, L, M] = \sum_{i=1}^{n} \rho_i \left[ Q_i, L_i, V_i \right] + \sum_{j=1}^{m} \rho'_j P_j,
\]

with \( \text{prob}'[Q, L, M] = \sum_{i=1}^{n} \rho_i \left[ Q_i, L_i, V_i \right] \), the \( P_j \) being fixed points, \( \sum \rho_i + \sum \rho'_j = 1 \), and \( n + m < 2^{d(M)} \).

Proof. Corollary of Theorem 7.2.7. □

7.3 Denotational Semantics

In Section 4.3, the notion of completely positive map is used to model the notion of quantum computation. We aim to show that the linear subset of the quantum lambda calculus has the category CPM as a fully abstract model. Note that the interpretation will not be “onto” all completely positive maps, but will only be “onto up to scalar multiplies”.

7.3.1 Modeling the Linear Quantum Lambda Calculus

We interpret the language in the category defined in Section 4.3.2.

Lemma 7.3.1. The following statements are valid.

1. Let \( \sigma, \tau \) be any signatures. Then \( 0 : \sigma \rightarrow \tau \) is completely positive.

2. The maps

\[
\iota : (a, b) \rightarrow (\begin{array}{c}
\alpha \\
\beta
\end{array}), \quad p : (\begin{array}{c}
a \\
b
\end{array}) \rightarrow (a, d)
\]

are completely positive.
Proof. The maps defined in the lemma are completely positive since they have positive characteristic matrices.

We set the denotation of types to be

\[
\begin{align*}
[x : A \triangleright x : A](v) &= v & [\triangleright 0 : \text{bit}](x) &= (x, 0) \\
[\triangleright * : \top](x) &= x & [\triangleright 1 : \text{bit}](x) &= (0, x) \\
[\Delta \triangleright \Omega : [A] = 0] &= [\Delta] \rightarrow [A] \\
[\triangleright \text{new} : \text{bit} \rightarrow \text{qbit}] &= \Phi(\iota) : 1 \rightarrow [\text{bit}] \otimes [\text{qbit}] \\
[\triangleright \text{meas} : \text{qbit} \rightarrow \text{bit}] &= \Phi(p) : 1 \rightarrow [\text{qbit}] \otimes [\text{bit}] \\
[\triangleright U : \text{qbit}^{\otimes n} \rightarrow \text{qbit}^{\otimes n}] &= \Phi(U) : 1 \rightarrow 2^{\otimes n}
\end{align*}
\]

\[
\begin{align*}
[\Delta, x : A \triangleright M : B] &= f : [\Delta] \otimes [A] \rightarrow [B] \\
[\Delta \triangleright \lambda x. M : [A \rightarrow B]] &= \Phi(f) : [\Delta] \rightarrow [A] \otimes [B] \\
[\Gamma \triangleright N : [A]] &= f : [\Gamma] \rightarrow [A]
\end{align*}
\]

\[
\begin{align*}
[\Delta, \Gamma \triangleright \text{if } P \text{ then } \text{else } N : [A]] &= x \otimes y \mapsto (x \otimes (fy)) + (q)(y) \\
[\Delta \triangleright M : [A]] &= f : [\Delta] \rightarrow [A] \\
[\Gamma \triangleright N : [B]] &= g : [\Gamma] \rightarrow [B]
\end{align*}
\]

\[
\begin{align*}
[\Delta, \Gamma \triangleright (M, N) : [A \otimes B]] &= x \otimes y \mapsto fx \otimes gy : [\Delta] \otimes [\Gamma] \rightarrow [A] \otimes [B] \\
[\Delta \triangleright M : [A \otimes B]] &= f : [\Delta] \rightarrow [A] \otimes [B] \\
[\Gamma \triangleright N : [C]] &= g : [\Gamma] \otimes [A] \otimes [B] \rightarrow [C]
\end{align*}
\]

\[
\begin{align*}
[\Delta, \Gamma \triangleright \text{let } (x, y) = M \text{ in } N : [C]] &= u \otimes v \mapsto g(v \otimes (fu)) : [\Delta] \otimes [\Gamma] \rightarrow [C] \\
[\Delta \triangleright M : [\top]] &= f : [\Delta] \rightarrow 1 \\
[\Gamma \triangleright N : [C]] &= g : [\Gamma] \rightarrow [C]
\end{align*}
\]

\[
\begin{align*}
[\Delta, \Gamma \triangleright \text{let } * = M \text{ in } N : [C]] &= u \otimes v \mapsto (fu)(gv) : [\Delta] \otimes [\Gamma] \rightarrow [C]
\end{align*}
\]

Table 7.3: Denotational semantics for typing judgements.

3. The maps

\[
\begin{align*}
1 & \mapsto 1,1 & 1 & \mapsto 1,1 \\
a & \mapsto (a,0), & a & \mapsto (0,a)
\end{align*}
\]

are completely positive.

Proof. The maps defined in the lemma are completely positive since they have positive characteristic matrices. □

**Definition 7.3.2.** We set the denotation of types to be

\[
\begin{align*}
[\text{bit}] &= (1, 1), & [A \otimes B] &= [A] \otimes [B], \\
[q\text{bit}] &= (2), & [A \rightarrow B] &= [A] \otimes [B],
\end{align*}
\]

and the denotation of contexts to be

\[
[x_1 : A_1, \ldots, x_n : A_n] = [A_1] \otimes \cdots \otimes [A_n], \quad [0] = 1.
\]

The denotation of a typing judgement of the form $\Delta \triangleright M : A$ is a linear map

\[
[\Delta \triangleright M : [A]] : [\Delta] \rightarrow [A],
\]
defined inductively on the typing derivation of $\Delta \triangleright M : A$ as in Table 7.3. Note that from Lemma 7.3.4, this typing derivation is unique, so the definition makes sense. Here, $\Phi : \text{hom}(\sigma \otimes \sigma' \otimes \tau) \rightarrow \text{hom}(\sigma, \sigma' \otimes \tau)$ is the bijection of Definition 4.3.4 and $\iota$ and $p$ are respectively the quantum bits creation and the measurement operation of Lemma 7.3.1.

**Definition 7.3.3.** We also define the denotation of a valid quantum closure. Consider a valid quantum closure $\Delta \models [Q, L, M] : A$ where $L = |x_1 \cdots x_n y_1 \cdots y_m \rangle$ and $|Q| = n + m$. The quantum context $(Q, L)$ can be seen as a map $g : 1 \rightarrow 2^{\otimes_n} \otimes 2^{\otimes_m}$ such that $g(1) = Q$. Then if $f$ is the morphism

$$[\Delta, x_1 : \text{qbit}, \ldots, x_n : \text{qbit} \triangleright M : A] : [\Delta] \otimes 2^{\otimes_n} \rightarrow [A],$$

one defines $[\Delta \models [Q, L, M] : A]$ as the composition

$$[\Delta] \xrightarrow{id[\Delta] \otimes g} [\Delta] \otimes 2^{\otimes_n} \otimes 2^{\otimes_m} f \otimes id_{2^{\otimes_m}} \rightarrow [A] \otimes 2^{\otimes_m} \xrightarrow{id[\Delta] \otimes \text{tr}} [A].$$

One extends this definition to probabilistic distributions of valid quantum closures using linearity:

$$[\Delta \models \sum_i \rho_i P_i : A] = \sum_i \rho_i [\Delta \models P_i : A].$$

**Lemma 7.3.4.** Let $\Delta \triangleright M : A$ be a valid typing judgement. Then $[\Delta \triangleright M : A]$ is a completely positive map. Let $\Gamma \models [Q, L, M] : A$ be a valid quantum closure. Then $[\Gamma \models [Q, L, M] : A]$ is a completely positive map.

**Proof.** We prove that $[\Delta \triangleright M : A]$ is a completely positive map by induction on the typing derivation of $\Delta \triangleright M : A$.

1. ($ax_1$) and ($\top. I$). The identity map is completely positive since CPM is a category.
2. ($ax_2$). The denotations of the term constants $\text{meas}, \text{new}, U, 0$ and 1 are completely positive map from Lemma 7.3.1.
3. ($\Omega$). The map 0 is completely positive from Lemma 7.3.1.
4. ($\lambda$). From the monoidal closedness of CPM, the image of $f$ by $\Phi$ is completely positive.
5. (app). Since $\Phi^{-1}$ sends completely positive matrices to completely positive matrices. Thus $g$ is completely positive. The final denotation is completely positive since composition and tensors of completely positive maps are completely positive.
6. (if). The denotation can be reformulated as

$$[\Delta] \otimes [\Gamma] \xrightarrow{[P] \otimes id} (1 \otimes 1) \otimes [\Gamma] = [\Gamma] \otimes [\Gamma] \xrightarrow{f \otimes g} [A] \otimes [A] \xrightarrow{\text{tr} \otimes id[A]} [A].$$

7. ($\otimes. I$), ($\otimes. E$) and ($\top. E$). In these three cases, the denotation is the tensor of two completely positive maps: it is therefore a completely positive map.

This proves that the denotation of a valid term is a completely positive map. The fact that the denotation of $\Gamma \models [Q, L, M] : A$ is also completely positive comes from the fact that completely positive maps are closed under composition and tensor, and that the trace operator and the identity are themselves completely positive maps.
Lemma 7.3.5 (Substitution). Suppose that $|\Gamma| \cap |\Delta| = \emptyset$ and
\[
[\Delta, x : A \triangleright M : B] = G : [\Delta] \otimes [A] \rightarrow [B],
\]
\[
[\Gamma \triangleright N : A] = F : [\Gamma] \rightarrow [A],
\]
\[
[\Delta, \Gamma \triangleright M|N/x] : B] = H : [\Delta] \otimes [\Gamma] \rightarrow [B].
\]
Then for all $d \in V_{[\Delta]}$ and all $g \in V_{[\Gamma]}$, we have $H(d \otimes g) = G(d \otimes (Fg))$.

Proof. We show that $H = (id_{[\Delta]} \otimes F) ; G$ by induction on the typing derivation of $\Delta, x : A \triangleright M : B$.

$(ax_1)$. We are considering the judgement $x : A \triangleright x : A$. We have $|\Delta| = \emptyset$, $A = B$ and $F = id_{[A]}$. Since $x[N/x] = N$, we have as required $H = G = F ; G$.

$(\Omega)$. Since $\Omega[N/x] = \Omega$, and since $(id_{[\Delta]} \otimes 0) ; G = 0$, the result is true.

$(\lambda)$. In this case, $M$ is of the form $\lambda y^C.M'$ and $A$ is of the form $C \rightarrow D$. Also, the typing judgement $\Delta, y : C, x : A \triangleright M' : D$ is valid. Note that $y \neq x$. By induction hypothesis, if $G'$ is the map $[\Delta, y : C, x : A \triangleright M' : D]$, the map $[\Delta, y : C, \Gamma \triangleright M' [N/x] : D]$ is $H'$ verifying for all $d \in V_{[\Delta]}$, for all $g \in V_{[\Gamma]}$, for all $c \in V_{[C]}$, $H'(d \otimes c \otimes g) = G'(d \otimes c \otimes F(g))$. Applying $\Phi$, we get
\[
\Phi(H')(d \otimes g) = \sum_{c \in V_{[C]}} c \otimes H'(d \otimes c \otimes g) = \sum_{c \in V_{[C]}} c \otimes G'(d \otimes c \otimes F(g)) = \Phi(G')(d \otimes F(g)),
\]
that is, $\llbracket \Delta, \Gamma \triangleright (\lambda y^C.M') [N/x] : C \rightarrow D \rrbracket$.

$(app)$. The term $M$ is of the form $M_1M_2$ and the context $(\Delta, x : A)$ splits into $(\Delta_1, \Delta_2)$, such that $\Delta_1 \triangleright M_1 : C \rightarrow B$ and $\Delta_2 \triangleright M_2 : C$ for some type $C$. Let
\[
G_1 = \llbracket \Delta_1 \triangleright M_1 : C \rightarrow B \rrbracket, \quad G_2 = \llbracket \Delta_2 \triangleright M_2 : C \rrbracket.
\]
There are two cases

$x \in |\Delta_1|$. The context $\Delta_1$ splits into $(\Delta'_1, x : A)$. From Lemma 7.3.3, the variable $x$ belongs to $FV(M_1)$ but not to $FV(M_2)$. From Lemma 7.3.4, $M[N/x] = (M_1[N/x])M_2$. Let $G_1'$ be the denotation $[\Delta'_1, \Gamma \triangleright M_1[N/x] : C \rightarrow D]$. By induction hypothesis, for all $d \in V_{\Delta'_1}$, for all $g \in V_{\Gamma}$, $G_1'(d \otimes g) = G_1(d \otimes F(g))$. If $d' \in V_{[\Delta_1]}$, this means that $H = [\Delta, \Gamma \triangleright M_1[N/x]M_2 : B]$ is
\[
H(d \otimes d' \otimes g) = \Phi^{-1}(G_1)(d \otimes G_2(d') \otimes F(g)).
\]

Since $G(d \otimes a \otimes d') = \Phi^{-1}(G_1)(d \otimes G_2(d') \otimes a)$, we have as required
\[
H(d \otimes d' \otimes g) = G(d \otimes d' \otimes F(g)).
\]

$x \in |\Delta_2|$. The context $\Delta_1frm \rightarrow e$ splits into $(\Delta'_2, x : A)$. From Lemma 7.3.4, $x$ belongs to $FV(M_2)$ but not to $FV(M_1)$. From Lemma 7.3.4, $M[N/x] = M_1(M_2[N/x])$. Let $G_2'$ be the denotation $[\Delta'_2, \Gamma \triangleright M_2[N/x] : C]$. By induction hypothesis, for all $d \in V_{\Delta'_2}$, for all $g \in V_{\Gamma}$, $G_2'(d \otimes g) = G_2(d \otimes F(g))$. If $d' \in V_{[\Delta_1]}$, this means that $H = [\Delta, \Gamma \triangleright M_1M_2[N/x] : B]$ is
\[
H(d' \otimes d \otimes g) = \Phi^{-1}(G_1)(d' \otimes G_2(d \otimes F(g))).
\]

Since $G(d \otimes a \otimes d') = \Phi^{-1}(G_1)(d' \otimes G_2(d \otimes a))$, we have as required
\[
H(d' \otimes d \otimes g) = G(d' \otimes d \otimes F(g)).
\]
(7.3. Denotational Semantics)

The term $M$ is of the form if $P$ then $M_1$ else $M_2$ and the context $(\Delta, x : A)$ splits into $(\Delta_1, \Delta_2)$, such that $\Delta_1 \triangleright P$ : bit and $\Delta_2 \triangleright M_1, M_2 : A$. Let

$$(p, q) = [\Delta_1 \triangleright P : \text{bit}], \quad G_1 = [\Delta_2 \triangleright M_1 : A], \quad G_2 = [\Delta_2 \triangleright M_2 : A].$$

There are two cases.

$x \in |\Delta_1|$. The context $\Delta_1$ splits into $(\Delta'_1, x : A)$. From Lemma 7.3.5, $x \in FV(P)$ and $x$ is either in $FV(M_1)$ nor in $FV(M_2)$. From Lemma 7.3.7, $M[N/x] = \text{if } P[N/x] \text{ then } M_1 \text{ else } M_2$.

Suppose that $g \in V[P], d' \in V[\Delta_1], d \in V[\Delta_2]$. Let $(p', q') = [\Delta'_1, \Gamma \triangleright P[N/x] : \text{bit}]$. By induction hypothesis, this is

$$(p'(d' \otimes g), q'(d' \otimes g)) = (p', q')(d' \otimes g) = (p, q)\, ((d' \otimes F(g)), q(d' \otimes F(g))),$$

thus $[\Delta'_1, \Gamma, \Delta_2 \triangleright \text{if } P[N/x] \text{ then } M_1 \text{ else } M_2 : A]$ is

$$H(d' \otimes g \otimes d) = p(d' \otimes F(g))G_1(d) + q(d' \otimes F(g))G_2(d) = G(d' \otimes d \otimes F(g)),$$

that is the requested form.

$x \in |\Delta_2|$. The context $\Delta_2$ splits into $(\Delta'_2, x : A)$. From Lemma 7.3.5, $x \in FV(P)$ and $x$ is either in $FV(M_1)$ nor in $FV(M_2)$. From Lemma 7.3.7, $M[N/x] = \text{if } P[N/x] \text{ then } M_1 \text{ else } M_2$.

Suppose that $g \in V[P], d' \in V[\Delta_2], d \in V[\Delta_1]$. Let $G'_1 = [\Delta_2, \Gamma \triangleright M_1[N/x] : A], \quad G'_2 = [\Delta_2, \Gamma \triangleright M_2[N/x] : A].$

By induction hypothesis, this is

$$G'_1 = G_1(d' \otimes F(g)), \quad G'_2 = G_2(d' \otimes F(g)).$$

thus $[\Delta_1, \Delta'_2, \Gamma \triangleright \text{if } P[N/x] \text{ then } M_1 \text{ else } M_2[N/x] : A]$ is

$$H(d \otimes d' \otimes g) = p(d)G_1(d' \otimes F(g)) + q(d)G_2(d' \otimes F(g)) = G(d \otimes d' \otimes F(g)),$$

which is in the requested form.

The three last cases are proved similarly.  

Lemma 7.3.6. Suppose that $P : A$ is a program of type $A$ such that $\text{prob}' P = \sum_i \rho_i P_i$, then

$$[P : A] = \sum_i \rho_i [P_i : A]$$

Proof. Suppose that $P = [Q, L, M]$, where $L = [x_1 \ldots x_n]$. If $P$ does not reduce, then $\text{prob}' P = P$ and we are done. If $P$ reduce to some $P'$ via some rule $\kappa$, we use Lemma 7.2.19 and proceed by case distinction.

First, suppose that $\kappa \neq m_0, m_1$. We prove the result by induction on a derivation of the reduction.

In this case, $M \equiv (\lambda x^B . N)'$, and then $P' = [Q, L, N[N'/x]]$. By definition and Theorem 7.2.20 since $P$ is of type $A$ we have

$$x_1 : \text{qbit}, \ldots, x_n : \text{qbit} \triangleright (\lambda x^B . N)' : A, \quad x_1 : \text{qbit}, \ldots, x_n : \text{qbit} \triangleright N[N'/x] : A.$$

The former being valid, its context splits as $(\Delta, \Gamma)$ where $\Delta, x : B \triangleright N : A$ and $\Gamma \triangleright N' : B$. Let $F = [\Delta, x : B \triangleright N : A]$ and $G = [\Gamma \triangleright N' : B]$. By definition, $[\Delta, \Gamma \triangleright (\lambda x^B . N)' : A]$ is equal to $d \otimes q \mapsto F(d \otimes G(g))$, if $d \in V[\Delta]$ and $g \in V[\Gamma]$. By Lemma 7.3.8 this is precisely the denotation of the latter. Thus, $[\equiv P' : A] = 1 \cdot [\equiv P : A]$. 

\(7.3.\) Denotational Semantics

In this case, \(M \equiv (let (x \in \mathbb{Q}, y \in \mathbb{Q}) \Rightarrow (V, W) \in \mathbb{N})\), and then \(P' = \{Q, L, N[V/x, W/y]\}\). By definition and Theorem 7.3, since \(P\) is of type \(A\) we have

\[x_1: \text{qbit}, \ldots, x_n: \text{qbit} \triangleright M : A, \quad x_1: \text{qbit}, \ldots, x_n: \text{qbit} \triangleright N[V/x][W/y] : A.\]

The former being valid, its context splits as \((\Delta, \Gamma_1, \Gamma_2)\) where \(\Delta, x : B, y : C \triangleright N : A, \Gamma_1 \triangleright V : B\) and \(\Gamma_2 \triangleright W : C\). Let

\[F = [\Delta, x : B, y : C \triangleright N : A], \quad G_1 = [\Gamma_1 \triangleright V : B], \quad G_2 = [\Gamma_2 \triangleright W : C].\]

By definition, \([\Gamma_1, \Gamma_2 \triangleright (V, W) : B \otimes C]\) is the map \(G_1 \otimes G_2\). By definition still, the map \([\Delta, \Gamma_1, \Gamma_2 \triangleright M : A]\) is \(((id \otimes G_1 \otimes G_2); F)\). By Lemma 7.3, this is the denotation of the latter. Thus, \([\models P' : A] = 1 \cdot [\models P : A].\)

\((-1)\). In this case, \(M \equiv (let * = * in N)\), and then \(P' = [Q, L, N]\). Since \(P\) is of type \(A\) we have

\[x_1: \text{qbit}, \ldots, x_n: \text{qbit} \triangleright M : A, \quad x_1: \text{qbit}, \ldots, x_n: \text{qbit} \triangleright N : A.\]

Since \([\triangleright * : \top] = id_1\), the denotation of the former is equal to the denotation of the latter: we have as requested \([\models P' : A] = 1 \cdot [\models P : A].\)

\((-0)\) and \((-1)\). In this case, \(M \equiv (if 0 then N else N')\) (respectively \(M \equiv (if 1 then N else N')\), and then \(P' = [Q, L, N']\). Since \(P\) is of type \(A\) we have

\[x_1: \text{qbit}, \ldots, x_n: \text{qbit} \triangleright if 0 then N else N' : A,\]
\[x_1: \text{qbit}, \ldots, x_n: \text{qbit} \triangleright if 1 then N else N' : A,\]
\[x_1: \text{qbit}, \ldots, x_n: \text{qbit} \triangleright N, N' : A,\]

and \(\triangleright 0, 1 : \text{bit}\). Since \([\triangleright 0 : \text{bit}][(a) = (a, 0)]\) and \([\triangleright 1 : \text{bit}][(a) = (0, a)]\), the denotation of \(M\) is then equal to the denotation of \(N'\) (respectively, of \(N\)). Therefore \([\models P' : A] = 1 \cdot [\models P : A].\)

\((-1)\). Since \(P = P'\), they have the same denotation.

\((-0)\) and \((-1)\). We prove the case \((-0)\), the other one is similar. The term \(M\) is of the form \(new 0, A = \text{qbit}\). The denotation of \(\triangleright M : \text{qbit}\) is the map \(f\) such that \(f(1) = [0, 0]\). The denotation of \(P\) is

\[G = 1 \rightarrow \mathbb{2} \otimes \mathbb{2} \rightarrow \mathbb{2} \otimes \mathbb{2} \rightarrow \mathbb{2},\]

where \(g\) is the map \(g(1) = QQ'\). Since \(Q\) is a normalized vector, \(G(1) = [0, 0]\). Now, \(P' = [Q \otimes [0, |x_1 \ldots x_n w|], w : \text{qbit}]\) and its denotation is

\[G' = 1 \rightarrow \mathbb{2} \otimes \mathbb{2} \rightarrow \mathbb{2} \otimes \mathbb{2} \rightarrow \mathbb{2},\]

where \(g'(1) = [0, 0] \otimes QQ'\). The map \(G'\) is therefore equal to \(G\).

\((-1)\). This case is similar: the denotation of \(P\) is of the form

\[G = 1 \rightarrow \mathbb{2} \otimes \mathbb{2} \rightarrow \mathbb{2} \otimes \mathbb{2} \rightarrow \mathbb{2} \rightarrow \mathbb{2},\]

where \(F = \Phi^{-1}(U)\), and \(g\) is \(QQ'\). The denotation of \(P'\) is

\[G' = 1 \rightarrow \mathbb{2} \otimes \mathbb{2} \rightarrow \mathbb{2} \otimes \mathbb{2} \rightarrow \mathbb{2} \rightarrow \mathbb{2},\]

where \(g' = g; (\Phi^{-1}(U) \otimes id)\). Therefore they are the same map.
The induction cases are trivial.

Finally, suppose that \( \kappa = m_0 \) or \( m_1 \). Then \( \alpha \to^{m_0} P_0 \) and \( \alpha \to^{m_1} P_0 \) for some \( P_0 \) and some \( P_1 \). we prove the result again by induction on the derivation of one of the reduction.

**Base case.** We use the notation in Definition 7.2.2. In both cases, \( M \) is of the form \( \text{meas }x_i \), and \( A = \text{bit} \). By \( \alpha \)-equivalence one can assume that \( i = 1 \): in this case \( Q \) is of the form

\[
\sum_j \alpha_j |0 \rangle \otimes |\bar{\psi}_j^{(0)} \rangle + \sum_j \beta_j |1 \rangle \otimes |\bar{\psi}_j^{(1)} \rangle = |0 \rangle \otimes \sum_j \alpha_j |\bar{\psi}_j^{(0)} \rangle + |1 \rangle \otimes \sum_j \beta_j |\bar{\psi}_j^{(1)} \rangle.
\]

Since the denotation \( [x_1: \text{qbit } \triangleright \text{meas }x_1: \text{bit}] \) is the map \( p \) of Definition 7.2.2, the denotation \( \models [Q, L, M]: \text{bit} \) is the map

\[
G = 1 \longrightarrow 2 \otimes 2^{\otimes(n-1)} \xrightarrow{p \otimes \text{tr}} 1 \otimes 1.
\]

The value \( g(1) \) is \( QQ^* \), that is

\[
|0\rangle \langle 0| \otimes \sum_{j,k} \alpha_j \alpha_k^* |\bar{\psi}_j^{(0)} \rangle \langle \bar{\psi}_k^{(0)}| + |1\rangle \langle 1| \otimes \sum_{j,k} \beta_j \beta_k^* |\bar{\psi}_j^{(1)} \rangle \langle \bar{\psi}_k^{(1)}|
\]

\[
+ |0\rangle \langle 1| \otimes \sum_{j,k} \alpha_j \beta_k^* |\bar{\psi}_j^{(0)} \rangle \langle \bar{\psi}_k^{(1)}| + |1\rangle \langle 0| \otimes \sum_{j,k} \beta_j \alpha_k^* |\bar{\psi}_j^{(1)} \rangle \langle \bar{\psi}_k^{(0)}|.
\]

Since \( |\psi_j^{(0)} \rangle, |\psi_j^{(1)} \rangle, |\bar{\psi}_j^{(0)} \rangle \) and \( |\bar{\psi}_j^{(1)} \rangle \) are basis vectors, applying \( \text{id} \otimes \text{tr} \) on \( g(1) \) yields

\[
\alpha |0\rangle \langle 0| + \beta |1\rangle \langle 1| + \delta |0\rangle \langle 1| + \gamma |1\rangle \langle 0|,
\]

for some values \( \delta, \gamma \), and where \( \alpha \) and \( \beta \) are as in Definition 7.2.2. Thus, \( G(1) \) is precisely \( (\alpha, \beta) = [\text{prob } P : A] \).

The induction cases are trivial. \( \square \)

**Lemma 7.3.7.** Suppose that \( P : A \) is a fixed point. Then \( [P] \) is the zero map.

**Proof.** Write \( P \) as \( [Q, L, M] \). The proof is done by structural induction on \( M \). \( \square \)

**Theorem 7.3.8** (Soundness). Given a program \( P : A \),

\[
[P : A] = [\text{prob}_I P : A].
\]

**Proof.** By induction on \( n \), using Lemma 7.3.9 one can prove that \( [\text{prob}^n P] = [\text{prob } P] \). From Theorem 7.2.2 there exists an integer \( n \) such that \( \text{prob}^n P = \text{prob}_I P + \sum_i P_i \) with \( P_i \) being fixed points. Therefore, from Lemma 7.3.7 \( [P : A] = [\text{prob}^n P] = [\text{prob}_I P : A] \). \( \square \)

### 7.3.2 Fullness of the First-Order Fragment

In this section we will show a result analog as Theorem 4.3.16 namely that any superoperator is the image of a term. For proving this result, we use the same techniques as in (Selinger 2004).

**Lemma 7.3.9.** Suppose that \( n = 2^s \) and \( m = 2^t \), and let \( F : C^{n \times n} \to C^{m \times m} \) be a contraction. Then there exists a valid typing judgement \( x_1 : \text{qbit}, \ldots, x_s : \text{qbit } \triangleright M : \text{qbit } \otimes t \) whose denotation is the map \( F \).
Proof. By definition, the map \( F \) can be written in the form \( F(A) = UAU^* \), where \( U \in \mathbb{C}^{m \times n} \) is a contraction. There exists matrices \( U_1, U_2 \) and \( U_3 \) such that

\[
U' = \begin{pmatrix}
U_1 \\
U_2 \\
U_3
\end{pmatrix}
\]

is unitary of size \( \mathbb{C}^{2L \times 1} \). Without loss of generality, one can assume that \( L = 2^p \): one can always extend \( U' \) to

\[
\begin{pmatrix}
U' \\
0 \\
I_{2^p - I}
\end{pmatrix}
\]

where \( I_{2^p - I} \) is the identity matrix. The requested program performs the following:

- Allocation of the variables \( y_1 : \text{qbit}, \ldots, y_{l-a} : \text{qbit} \), and let the list of variables \((z_1, \ldots, z_t)\) be \((x_1, \ldots, x_a, y_1, \ldots, y_{l-a})\);
- application of the unitary \( U' \) to \((z_1, \ldots, z_t)\);
- measurement of the variables \( z_t, \ldots, z_l \): if the outcome is \((0, \ldots, 0)\), the program returns the term \((z_1, \ldots, z_t)\). Otherwise it outputs the term \( \Omega^{qbit}_{x_1} \cdots qbit_{x_z} \). \( \square \)

Lemma 7.3.10. Let \( F : \mathbb{C}^{2^t \times 2^t} \to \mathbb{C}^{2 \times 2} \) be a superoperator and \( E \circ G \) is decomposition from Theorem 3.1.32. One can construct another decomposition \( E' \circ G' \), where \( G' : \mathbb{C}^{2^t \times 2^t} \to \mathbb{C}^{2^t+k \times 2^t+k} \) is a contraction and \( E' : \mathbb{C}^{2^t+k \times 2^t+k} \to \mathbb{C}^{2^t \times 2^t} \) is a partial trace operator, for some integer \( k \).

Proof. The proof uses Lemma 3.1.32 to adjust the size of the output space of the sub-unitary \( E' \) to a power of 2. \( \square \)

Lemma 7.3.11. Let \( E : \mathbb{C}^{2^t+k \times 2^t+k} \to \mathbb{C}^{2 \times 2} \) be a partial trace operator. Then there exists a valid typing judgement \( x_1 : \text{qbit}, \ldots, x_t+k : \text{qbit} \Rightarrow M : \text{qbit}^{\otimes t} \)'s whose denotation is \( E \).

Proof. The requested term \( M \) measures the variables \( x_{t+1}, \ldots, x_{t+k} \), perform a test on the result and in all cases returns \((x_1, \ldots, x_t)\). \( \square \)

Lemma 7.3.12. Let \( \sigma = (1,1)^{\otimes n} \otimes 2^{\otimes m} \), and \( \sigma' = 2^{\otimes (m+n)} \). Then the measurement operator \( \mu_\sigma : V_\sigma \to V_{\sigma'} \) is the image of some typing judgement \( x : \text{qbit}^{\otimes (m+n)} \Rightarrow M : \text{bit}^{\otimes n} \otimes \text{qbit}^{\otimes m} \).

Proof. The requested term \( M \) measures the variables \( x_{t+1}, \ldots, x_{t+k} \) and stores the results in \((z_1 : \text{bit}, \ldots, z_k : \text{bit})\). It outputs the product \((z_1, \ldots, z_k, x_1, \ldots, x_t)\). \( \square \)

Theorem 7.3.13. For any types \( A = U_1 \otimes \cdots \otimes U_n \) and \( B = V_1 \otimes \cdots \otimes V_m \), where each \( U_i \) and \( V_j \) is either bit or qbit, if \( F : [A] \to [B] \) is any superoperator, then there exists a valid typing judgement \( x : A \Rightarrow M : B \) of denotation \( F \).

Proof. Without loss of generality, one can assume that \( A = \text{bit}^{\otimes k} \otimes \text{qbit}^{\otimes l} \) and that \( B = \text{bit}^{\otimes x} \otimes \text{qbit}^{\otimes y} \). The map \( F : [A] \otimes [B] \) is of the form \((F_1, \ldots, F_{2^k})\), where each \( F_i : V_{2^i} \to V_{(1,1)^{\otimes i} \otimes 2^i} \) is a superoperator. From Theorem 7.3.12, \( F_i \) splits into \( M_i \circ E_i \circ G_i \), where \( G_i \) is a contraction, \( E_i \) is a partial trace operator, and \( M_i \) is a measurement operator. Using Lemma 7.3.11, one can assume that all of them goes from images of tensors of \( \text{bit} \)'s and \( \text{qbit} \)'s. Therefore, using Lemma 7.3.12, \( F_i \)'s are representable by some terms \( M_i \). The function \( F \) is represented by a term that does a test on its input \( \text{bit} \) and perform the corresponding \( M_i \). \( \square \)

Corollary 7.3.14. For every type \( A = U_1 \otimes \cdots \otimes U_n \), where each \( U_i \) is either bit or qbit, and for every hermitian positive element \( v \in V[A] \) of trace at most 1, \( v = M \Rightarrow A \) for some closed valid term \( M \).
7.3. Denotational Semantics

Proof. Consider the function $F : \mathbb{C} \to V_{\alpha[\alpha]}$ defined by $F(1) = v$. Since $\chi_F = v$ is positive, and since $tr(v) \leq 1$, $F$ is a superoperator. From Theorem 7.3.13, it is the image of some typing judgement $\triangleright M : A$. 

7.3.3 Fullness up to Scalar Multiple

Theorem 7.3.14 does not hold for generic types. However, a weaker statement does hold. We explicate it in this section.

Definition 7.3.15. Given a type $A$, we define the canonical first-order representation $\underline{A}$ of $A$ by the following: $\underline{bit} = bit$, $\underline{qbit} = qbit$, $\underline{\top} = \top$, $\underline{A \otimes B} = \underline{A} \otimes \underline{B}$, $\underline{A \rightarrow B} = \underline{A} \otimes \underline{B}$.

Lemma 7.3.16. For all types $A$, $[A] = [\underline{A}]$.


Definition 7.3.17. We define the $\underline{s}$-size $s(A)$ of a type $A$ as follows. First, $s(bit) = s(qbit) = s(\top) = 1$. Then, $s(A \rightarrow B) = 2^{s(A)} + s(B)$. Finally, $s(A \otimes B) = s(A) + s(B)$.

Lemma 7.3.18. For all types $A$, $s(A) \geq 1$. Also, $s(\underline{A}) \leq s(A)$, with equality if and only if $A = \underline{A}$.


Next, we want to write a correspondence between types $A$ and $\underline{A}$, in the form of typing judgements $x : A \triangleright \Upsilon_{x,\underline{x}} : \underline{A}$ and $x : \underline{A} \triangleright \Upsilon_{x,\underline{x}} : A$ whose denotations are multiples of the identity function. The correspondences are built by induction on the $\underline{s}$-size of $A$:

- knowing the result for $A$ we deduce it for $bit \rightarrow A$, $qbit \rightarrow A$ and $\top \rightarrow A$;
- knowing the result for $A$ and $B$ we deduce it for $A \otimes B$;
- knowing the result for $C \rightarrow (D \rightarrow B)$ we deduce it for $(C \otimes D) \rightarrow B$;
- knowing the result for $C \rightarrow D$ and $(\underline{C} \otimes \underline{D}) \rightarrow B$ we deduce it for $(C \rightarrow D) \rightarrow B$.

The detailed definition goes as follows:

Definition 7.3.19. We define the terms $\Upsilon_{x,\underline{x}}^A$ and $\Upsilon_{x,\underline{x}}^A$ by induction on the $\underline{s}$-size of $A$. First,

\[
\begin{align*}
\Upsilon_{x,\underline{x}}^{bit} &= \Upsilon_{x,\underline{x}}^{bit} = x, \\
\Upsilon_{x,\underline{x}}^{qbit} &= \Upsilon_{x,\underline{x}}^{qbit} = x, \\
\Upsilon_{x,\underline{x}}^{\top} &= \Upsilon_{x,\underline{x}}^{\top} = x
\end{align*}
\]

Then,

\[
\begin{align*}
\Upsilon_{x,\underline{x}}^{A \otimes B} &= \text{let } (y,z) = x \in \langle \Upsilon_{y,\underline{y}}^{A}, \Upsilon_{z,\underline{z}}^{B} \rangle, \\
\Upsilon_{x,\underline{x}}^{A \rightarrow B} &= \text{let } (y,z) = x \in \langle \Upsilon_{y,\underline{y}}^{A}, \Upsilon_{z,\underline{z}}^{B} \rangle.
\end{align*}
\]

For types of the form $A \rightarrow B$, we first consider the case where $A = \top$, $A = bit$ and $A = qbit$:

\[
\begin{align*}
\Upsilon_{x,\underline{x}}^{\top \rightarrow B} &= \langle \ast, \text{let } t^B = x \ast \text{ in } \Upsilon_{t^B}^{B} \rangle \\
\Upsilon_{x,\underline{x}}^{bit \rightarrow B} &= \text{let } (y^\top, z^\bB) = x \in \lambda t. \text{let } * = y \text{ in } \Upsilon_{z,\underline{z}}^{B} \\
\Upsilon_{x,\underline{x}}^{qbit \rightarrow B} &= \text{if } \text{meas}(H(\text{new } 0)) \text{ then } (1, \text{let } t^B = x1 \text{ in } \Upsilon_{t^B}^{B}) \\
&\quad \text{else } (0, \text{let } t^B = x0 \text{ in } \Upsilon_{t^B}^{B}) \\
\Upsilon_{x,\underline{x}}^{bit \rightarrow B} &= \text{let } (y^{bit}, z^B) = x \in \Upsilon_{z,\underline{z}}^{B}
\end{align*}
\]
7.3. Denotational Semantics

\[\lambda^{\text{bit}} \text{ if } x \text{ then } \text{ if } t \text{ then } \Upsilon^B \text{ else } \Omega\]

\[\text{else if } t \text{ then } \Omega \text{ else } \Upsilon^B\]

\[\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}} = \text{let } (u, v) = N_C(H(\text{new } 0), \text{new } 0) \text{ in } (u, \text{let } t^B = xv \text{ in } \Upsilon^B)\]

\[\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}} = \text{let } (g^{\text{bit}}, z^B) = x \text{ in }\]

\[\lambda^{\text{bit}} \text{, let } (y', t') = N_C(y, t) \text{ in }\]

\[\text{let } (y'', t'') = (H_y', t') \text{ in }\]

\[\text{if mean } y'' \text{ then } \Omega \text{ else } \Upsilon^B\]

Then, when \(A\) is of the form \(C \otimes D\), we proceed the following way:

\[\Upsilon^{(C \otimes D) \to B}_{\text{x}_{\text{y}}} = \text{let } f^{(C \to (D \to B)} = \lambda x^C . \lambda u^D . (x(t, u)) \text{ in }\]

\[\text{let } (u^C, v^D \otimes \mathbb{B}) = \Upsilon^C \to (\mathbb{D} \to \mathbb{B}) \text{ in }\]

\[\text{let } (y_x^D, z_x^B) = v \text{ in } (u, y), z\]

\[\Upsilon^{(C \otimes D) \to B}_{\text{x}_{\text{y}}} = \lambda l^{C \otimes D} . \text{let } (y^C, z^D) = t \text{ in } \text{let } (u^C \otimes z^D, v^B) = x \text{ in }\]

\[\text{let } (u^C, v^B) = x \text{ in }\]

\[\text{let } a = \langle w, \langle s, v \rangle \rangle \text{ in } ((\Upsilon^{C \to (D \to B)}_{\text{a}^\mathbb{B}}(y)) \mathbb{Z})\]

Finally, when \(A\) is of the form \(C \to D\), we reduce \(C \to D\) to \(\mathbb{C} \otimes \mathbb{D}\) to fall back on the previous case. The details are as follows:

\[\Upsilon^{(C \to D) \to B}_{\text{x}_{\text{y}}} = \text{let } f^{(\mathbb{C} \otimes \mathbb{D} \to \mathbb{B})} = \lambda x^C . \lambda u^D . (x(t, u)) \text{ in }\]

\[\Upsilon^{(C \otimes D) \to B}_{\text{x}_{\text{y}}} = \lambda l^{C \otimes D} . \text{let } (y^C, z^D) = t \text{ in } \text{let } (u^C \otimes z^D, v^B) = x \text{ in }\]

\[\text{let } (u^C, v^B) = x \text{ in }\]

\[\text{let } a = \langle w, \langle s, v \rangle \rangle \text{ in } ((\Upsilon^{C \to (D \to B)}_{\text{a}^\mathbb{B}}(y)) \mathbb{Z})\]

**Lemma 7.3.20.** For every types \(A\), the typing judgements \(x : A \triangleright \Upsilon^A_{\text{x}_{\text{y}}} : \frac{A}{x} \text{ and } x : \frac{A}{x} \triangleright \Upsilon^{\frac{A}{x}}_{\text{x}_{\text{y}}} : A\) are valid. Moreover, there exist constants \(\lambda, \lambda' > 0\), such that \([\Upsilon^A_{\text{x}_{\text{y}}}] = \lambda \text{id}_{[A]}\) and \([\Upsilon^{\frac{A}{x}}_{\text{x}_{\text{y}}}] = \lambda' \text{id}_{[A]}\).

**Proof.** The proof that the typing judgements are valid is an easy induction on the \(\mathbb{B}\)-size of \(A\). We provide the computation for the difficult cases, namely when the type is \(\text{bit} \to B\) and \(\text{qbit} \to B\).

**Case \(\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}}**. We are considering

\[f = [x : \text{bit} \otimes \mathbb{B} \triangleright \Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}} : \text{bit} \to B] : [B] \oplus [B] \to [B] \oplus [B].\]

An element \((a, b) \in [\mathbb{B}] \oplus [\mathbb{B}]\) corresponds to a probability \(a\) to get the boolean 0 and a probability \(b\) to get the boolean 1 for the bit. This means that \(f(a, b) = ([\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}}](a), [\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}}](b)).\)

By induction hypothesis, \([\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}}]] = \lambda \text{id}\) for some \(\lambda > 0\). Thus we have then \(f = \lambda \text{id}\).

**Case \(\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}}**. We are considering

\[f = [x : \text{bit} \to B \triangleright \Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}} : \text{bit} \otimes \mathbb{B}] : [B] \oplus [B] \to [B] \oplus [B].\]

A function \(g \in V_{[\text{bit} \to B]}\) is sent to \(\frac{1}{2}([\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}}](g(1, 0)), [\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}}](g(0, 1)))\), where we identify the function \(g\) and its representation. By induction hypothesis, \([\Upsilon^{\text{bit} \to B}_{\text{x}_{\text{y}}}]] = \lambda \text{id}\) for some \(\lambda > 0\). Thus \(g \in V_{[\text{bit} \to B]}\), represented by \((g(1, 0), g(0, 1))\), is sent to \(\frac{1}{2} \lambda g\). This means that \(f = \frac{1}{2} \lambda \text{id}\).
Case $\Upsilon_{x \rightarrow y}^{\text{bit} \rightarrow B}$. We are considering

$$f = [x : \text{bit} \otimes \mathbb{B} \triangleright \Upsilon_{x \rightarrow y}^{\text{bit} \rightarrow B} : \text{bit} \rightarrow [B] : 2 \otimes [B] \rightarrow 2 \otimes [B]].$$

We interpret the term as in the definition. Suppose that $x = \langle y, z \rangle$ and $t$ are respectively the matrix of blocks and the quantum bits

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where the blocks $A, B, C$ and $D$ belongs to $V_{[B]}$. Then the products $\langle y, t, z \rangle$ and $\langle y', t', z \rangle$ are respectively

$$\begin{pmatrix} a & b & a & b \\ c & d & a & b \\ c & d & c & d \\ a & b & c & d \end{pmatrix}, \quad \begin{pmatrix} a & b & a & b \\ c & d & a & b \\ c & d & a & b \\ a & b & c & d \end{pmatrix}.$$

Applying $H$ on $y'$ yields a matrix with first entry

$$\frac{1}{2} \lambda (aA + bB + cC + dD),$$

if $[\Upsilon_{x \rightarrow y}^B] = \lambda \text{id}$, corresponding to the probability for $y''$ to be $|0\rangle$. Thus,

$$f \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{2} \lambda (aA + bB + cC + dD),$$

meaning that $x$ maps to a multiple of the function $\text{bit} \rightarrow [B]$ of same denotation. That is, $f = \frac{1}{2} \lambda \text{id}$.

Case $\Upsilon_{x \rightarrow y}^{\text{qbit} \rightarrow B}$. We are considering

$$f = [x : \text{qbit} \otimes \mathbb{B} \triangleright \Upsilon_{x \rightarrow y}^{\text{qbit} \rightarrow B} : \text{bit} \otimes [B] : 2 \otimes [B] \rightarrow 2 \otimes [B]].$$

In this case, the function $f(x)$ creates a pair of two quantum bits in state

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

and applies (a multiple of) the function $x$ on each $2 \times 2$ block: it is precisely (a multiple of) the characteristic function of $x$: the function $f$ is indeed a multiple of the identity. 

**Theorem 7.3.21** (Fullness up to scalar multiple). For any types $A$ and $B$, there exists a constant $\lambda > 0$ such that if $F : [A] \rightarrow [B]$ is any superoperator, then there is a valid typing judgement $x : A \triangleright M : B$ of denotation $\lambda F$.

**Proof.** For the given types $A$ and $B$, consider the terms $\Upsilon_{A \rightarrow y}^A$ and $\Upsilon_{B \rightarrow y}^B$. From Lemma 7.3.20 they have for denotation respectively $\lambda \text{id}$ and $\lambda' \text{id}$, for some $\lambda, \lambda'$. We claim that any superoperator $[A] \rightarrow [B]$ can be interpreted modulo a factor of $\lambda \lambda'$.

Indeed, consider a superoperator $F : [A] \rightarrow [B]$. From Theorem 7.3.20 there exists a valid typing judgement $y : \mathbb{A} \triangleright N : \mathbb{B}$ of denotation $F$. Let $a : A \triangleright M : B$ be the term

$$a : A \triangleright \text{let } y = \Upsilon_{A \rightarrow y}^A \text{ in let } b = N \text{ in } \Upsilon_{B \rightarrow y}^B : B.$$

It has denotation $\lambda \lambda' F$. 

$\square$
7.4. Equivalence Classes of Terms

We call it the axiomatic equivalence relation way: if $\Delta \vDash \text{when}$\n
Table 7.4: Axiomatic equivalence

7.4 Equivalence Classes of Terms

Being able to build terms, we need some tools to compare them. One can compare them through syntactic manipulations, or one can have a finer approach using the two semantics we have built: in the case of the operational semantics, the behavior of the terms is what defines the equivalence, and in the case of the denotational semantics, the equivalence is expressed by the denotation of the terms.

7.4.1 Axiomatic Equivalence

A first notion of equality of terms can be defined by a set of syntactic rules. This is known as the axiomatic equivalence.

Definition 7.4.1. We define an equivalence relation $\approx_{ax}$ on typing judgements. We write the relation as $\Gamma \vdash M \approx_{ax} N : A$, and we define it to be the smallest relation satisfying the rules in Table 7.4, the alpha-equivalence and one congruence rule $(\xi)$ per term constructor. This means for example:

$\Gamma \vdash M \approx_{ax} M' : A \rightarrow B \quad \Delta \vdash N \approx_{ax} N' : A$

$\Gamma, \Delta \vdash MN \approx_{ax} M'N' : B$ \hspace{1cm} \text{(app)}

$\Gamma, x : A \vdash M \approx_{ax} M' : B$

$\Gamma \vdash \lambda x.M \approx_{ax} \lambda x.M' : A \rightarrow B$ \hspace{1cm} \text{(\lambda)}

We call it the axiomatic equivalence relation. We extend it to quantum closures in the following way: if $\Delta \vDash \{ Q, L, M \} : A$ and $\Delta \vDash \{ Q, L, M' \} : A$ are two well-typed quantum closures where $\text{FV}(M) \setminus |\Delta| = \text{FV}(M') \setminus |\Delta| = \{ x_1, \ldots, x_n \}$, then we write $\Delta \vDash \{ Q, L, M \} \approx_{ax} \{ Q, L, M' \} : A$

$\Delta, x_1 : qbit, \ldots, x_n : qbit \vdash M \approx_{ax} M' : A$.

Lemma 7.4.2. The order of the arguments in an application does not matter. Similarly, one can apply the arguments as a pairing or sequentially. More precisely:

$[Q, L, ((\lambda xy.M)N)P] \approx_{ax} [Q, L, ((\lambda yx.M)P)N]$  
$[Q, L, \text{let} (x, y) = (N, P) \text{ in } M] \approx_{ax} [Q, L, ((\lambda xy.M)N)P]$

Proof. By application of rule $(\beta)$ and rule $(\beta_\otimes)$. \hfill \Box
7.4.2 Operational Context

To say that two arbitrary terms have the same behavior, we need a way to observe them. The only observable types at our disposal are the types \( \text{bit} \) and \( \top \). So the fact that two terms \( M \) and \( M' \) have the same behavior can be understood as the fact that in whichever context \( C[-] \) we “use” them, if \( C[-] : \text{bit} \), then \( C[M] \) reduces to 0, respectively, 1, with the same probability as \( C[M'] \). Such a term \( C[-] \) is called an operational context.

**Definition 7.4.3.** We define a formal operational context to be a formula defined by the following BNF:

\[
C[-] ::= [-] \mid (C[-]M) \mid (MC[-]) \mid \lambda x.C[-] \mid \langle C[-], M \rangle \mid \langle M, C[-] \rangle \mid \text{let } (x, y) = C[-] \text{ in } M \mid \text{let } x = M \text{ in } C[-] \mid \text{let } * = C[-] \text{ in } M \mid \text{let } * = M \text{ in } C[-] \mid \text{if } C[-] \text{ then } M \text{ else } N \mid \text{if } M \text{ then } C[-] \text{ else } C'[-].
\]

We call \([-] \) the hole of the context.

The notions of well-typed contexts and free variables in contexts are defined the same ways as for terms. Note that there exists a new notion: the notion of captured variables, which are the variables whose scope includes the hole. We can make this more precise by speaking of typed contexts:

**Definition 7.4.4.** A typed operational context is a typing tree with root \( \Gamma' \ni C[-] : B \), considering the additional axiom \( \Gamma \ni [-] : A \), i.e., a typing tree of the form

\[
\begin{array}{c}
\Gamma \ni [-] : A \\
\vdots \\
\Gamma' \ni C[-] : B.
\end{array}
\]

We say that this context is of type \( B \), with free variables \( \Gamma' \), a hole of type \( A \), and captured variables \( \Gamma \). We also use the notation \( \Gamma' \ni C[\Gamma \ni - : A] : B \) for a typed operational context.

**Lemma 7.4.5.** If

\[
\begin{array}{c}
\Gamma \ni [-] : A \\
\vdots \\
\Gamma' \ni C[-] : B.
\end{array}
\]

is a valid typing derivation, then so is

\[
\begin{array}{c}
\Delta, \Gamma \ni [-] : A \\
\vdots \\
\Delta, \Gamma' \ni C[-] : B,
\end{array}
\]

provided the variables that occur in \( \Delta \) are fresh.

**Proof.** By easy induction on the typing derivation of \( \Gamma' \ni C[-] : B \).

7.4.3 Operational Equivalence

We define a notion of operational equivalence, based on the reduction rules and observations of type \( \text{bit} \), as in Danos and Harmer (2002). (Equivalently, it would suffice to consider observations of type \( \top \).)
7.5. Soundness and Full Abstraction

Definition 7.4.6. Let \( \triangleright C[\Gamma \triangleright - : A] : \text{bit} \) be a closed typed operational context of type \( \text{bit} \), and let \( R = [Q, L, M] \) be a well-typed quantum closure with typing judgement \( \Gamma \vDash [Q, L, C[M]] : A \). In this case we define the substitution \( C[R] \) by \( [Q, L, C[M]] \), where \( M \) is syntactically replacing \( [-] \) in \( C[-] \). We linearly extend this definition to probabilistic distributions of quantum closures of the form \( \Gamma \vDash \sum \rho_i R_i : A \) by setting \( C[\sum \rho_i R_i] = \sum \rho_i C[R_i] \).

Lemma 7.4.7. In Definition 7.4.6, the substitution is well typed and a valid typing judgement for it is \( \Gamma \vDash [Q, L, C[M]] : \text{bit} \).

Proof. This lemma is a direct consequence of Lemma 7.4.5. □

Definition 7.4.8. Given two well-typed quantum closures \( \Gamma \vDash R, R' : A \), we say that \( R \) is operationally equivalent to \( R' \) with respect to \( \Gamma \) if for all closed typed operational contexts \( \triangleright C[\Gamma \triangleright - : A] : \text{bit} \), \( C[R] \Downarrow 0 = C[R'] \Downarrow 0 \) and \( C[R] \Downarrow 1 = C[R'] \Downarrow 1 \). In this case, we write \( \Gamma \vDash R \approx_{\text{op}} R' : A \). If \( M, M' \) are terms, we say that \( \Gamma \triangleright M \approx_{\text{op}} M' : A \) if \( \Gamma \vDash [Q, L, C[M]] \approx_{\text{op}} [Q, L, C[M']] : A \).

7.4.4 Denotational Equivalence

The last equivalence we can define is the denotational equivalence. This equivalence relation is simply stated:

Definition 7.4.9. We say that two typing judgements \( \Gamma \triangleright M, M' : A \) are denotationally equivalent if \([\Gamma \triangleright M : A]\) and \([\Gamma \triangleright M' : A]\) are the same map in \( \text{CPM} \). In that case we write \( \Gamma \triangleright M \approx_{\text{den}} M' : A \). We extend this definition to quantum closures: \( \Gamma \vDash R \approx_{\text{den}} R' : A \) is true if \([\Gamma \vDash R : A]\) = \([\Gamma \vDash R' : A]\).

7.5 Soundness and Full Abstraction

The three defined equivalence relations we have built have the expected behavior: The axiomatic equivalence is sound with respect to the operational equivalence and the denotational semantic is fully abstract with respect to the operational semantics:

Theorem 7.5.1 (Soundness). If \( \Gamma \triangleright M \approx_{\text{ax}} M' : A \) then \( \Gamma \triangleright M \approx_{\text{op}} M' : A \).

Remark 7.5.2. An immediate consequence of soundness and Lemma 7.4.5 is that the order of evaluation does not affect the outcome:

\[ \Gamma \triangleright (\lambda xy.R)M \approx_{\text{op}} (\lambda xy.R)N.M. \]

Theorem 7.5.3 (Full abstraction). The denotational semantics is fully abstract with respect to the operational equivalence of typing judgements, i.e.

\[ [\Gamma \triangleright M : A] = [\Gamma \triangleright M' : A] \text{ if and only if } \Gamma \triangleright M \approx_{\text{op}} M' : A. \]

Remark 7.5.4. The presence of the non-terminating term \( \Omega \) is necessary for full abstraction to hold. Without it, every program terminates with probability 1, and there is only one definable map \( \text{bit} \to \top \). Thus, although \( \lambda f.(f0) \) and \( \lambda f.(f1) \) of type \( (\text{bit} \to \top) \to \top \) have different denotations, no context will distinguish them.
7.5. Soundness and Full Abstraction

7.5.1 Proof of the Soundness Theorem

Assume Theorem 7.5.1. We detail the remaining cases

(η). If \([\Gamma \vdash M : A \rightarrow B] = \Phi(g) : [\Delta] \rightarrow [A] \otimes [B]\), then the denotation \([\Gamma, x : A \triangleright M x : B]\) is a map \(f : [\Gamma] \otimes [A] \rightarrow [B]\), with

\[ f(x \otimes y) = g(x \otimes id_A(y)) = g(x \otimes y). \]

(η0). If \(f = [\Gamma \triangleright M : A \otimes B]\), if \(g = [\Gamma \triangleright let (x, y) = M in (x, y) : A \otimes B]\) and if \(a \in [\Gamma]\), we have

\[ g(a) = (id_A \otimes id_B)(f(a)) = f(a). \]

(ηi). If \(f = [\Gamma \triangleright M : \top]\), if \(g = [\Gamma \triangleright let * = M in * : \top]\), and if \(a \in [\Gamma]\), then \(g(a)\) is equal to \(id_\top(1) \cdot f(a)\), that is, \(f(a)\).

(ηf). In this case, the context \(\Gamma\) splits into \((\Gamma_1, \Gamma_2)\), where \(\Gamma_1 \triangleright B : \text{bit}\) and \(\Gamma_2, x : \text{bit} \triangleright M : A\). If \((p, q)\) is the denotation of the former and \(f\) the denotation of the latter, if \(a \in [\Gamma_1]\) and \(b \in [\Gamma_2]\), \(p(a)f(0, b) + q(a)f(0, 0) = f(0, b \cdot p(a)) + f(b \cdot q(a), 0) = f((p(a), q(a)) \otimes b)\).

(id). This last case is done by noticing that \([x : \text{bit} \triangleright \text{meas}(\text{new} x) : \text{bit}]\) is the identity.

7.5.2 Full Abstraction: Preliminary Lemmas

Lemma 7.5.5. For any two programs \(P, P'\) of type \(\text{bit}\), they have the same denotation if and only if for all \(b \in \{0, 1\}\), \(P \Downarrow b = P' \Downarrow b\).

Proof. Consider two well-typed programs \(P, P' : \text{bit}\). Suppose they have the same denotation \(f\). Then from Lemma 7.5.20, \(f\) is also the denotation of \(\text{prob}_1 P\) and of \(\text{prob}_1 P'\). But by definition, \([\text{prob}_1 P] = (p, q)\), where \(p = (\text{prob}_1 P) \Downarrow 1 = P \Downarrow 1\) and \(q = (\text{prob}_1 P) \Downarrow 0 = P \Downarrow 0\), and similarly for \(P'\). Thus \(P \Downarrow 1 = P' \Downarrow 1\) and \(P \Downarrow 0 = P' \Downarrow 0\). The argument being reversible, we get the other implication.

Lemma 7.5.6. If \([\Gamma \triangleright M : A] = [\Gamma \triangleright M' : A]\) and \(C[\Gamma \triangleright - : A] : \text{bit}\) is a valid context, then \([C[M] : \text{bit}] = [C[M'] : \text{bit}]\).

Proof. The proof uses Lemma 7.5.5.

Lemma 7.5.7. Let \(A\) be a type and let \(v \neq v'\) be hermitian positive elements in \(V[A]\). Then there exists a valid typing judgement \(x : A \triangleright M : \text{bit}\) such that \([M](v) \neq [M](v')\).

Proof. By Lemma 7.5.20, it suffices, without loss of generality, to consider the case where \(A = \text{bit}^\otimes n \otimes q\text{bit}^\otimes m\). Then \([A] = (2^m, \ldots, 2^m), v = (v_1, \ldots, v_2n)\) and \(v' = (v'_1, \ldots, v'_2n)\). If \(v\) and \(v'\) differ, there exists some \(i\) for which \(v_i \neq v'_i\). By Theorem 5.1.13, there exists orthonormal bases of eigenvectors corresponding to \(v_i\) and \(v'_i\). Since they differ, there exists a vector \(w\) such that \(w^*v_iw \neq w^*v'_iw\) (otherwise, \(v_i\) and \(v'_i\) would have the same eigenvectors and eigenvalues, making them equal).

Consider the map

\[ f : (2^m, \ldots, 2^m) \rightarrow (1, 1) \]
\[ (w_1, \ldots, w_n) \rightarrow (w^*w, 0) \]

From Theorem 7.5.14, this is a superoperator. By definition, \(f(v) \neq f(v')\) and by Theorem 7.5.3, it is representable by some valid typing judgement \(x : A \triangleright M : \text{bit}\).
Lemma 7.5.8. Given any type $A$ and any hermitian positive $v \in V_{\Gamma}[A]$, there exists a closed term $M : A$ and $\lambda > 0$ such that $\llbracket M \rrbracket(1) = \lambda v$.

Proof. If $v = 0$, let $M = \Omega$. Else, from Corollary 7.3.14 there exists a valid typing judgement $\triangleright N : \mathbb{A}$ such that $v/\text{Tr}(v) = [\triangleright N : A](1)$. Then let $M = \text{let } x = N \text{ in } \Upsilon A$. From Lemma 7.3.20 $[\triangleright M : A](1)$ and $v$ are collinear. \qed

7.5.3 Proof of the Full Abstraction Theorem

If $[\Gamma \triangleright M : A] = [\Gamma \triangleright M' : A]$, take any valid context $C[\Gamma \triangleright \cdots : A]$ for those two terms. Then from Lemma 7.5.6 $[\triangleright C[M] : \text{bit}] = [\triangleright C[M'] : \text{bit}]$. From Lemma 7.5.5 $C[M] \downarrow b = C[M'] \downarrow b$, for $b \in \{0, 1\}$. Since this holds for arbitrary contexts, $M$ and $M'$ are operationally equivalent.

The opposite implication follows from Lemma 7.5.7 and Lemma 7.5.8. Consider two typing judgements $\Gamma \triangleright M, M' : A$ with denotations

$$F = [\Gamma \triangleright M : A] \quad \text{and} \quad G = [\Gamma \triangleright M' : A],$$

such that $F \neq G$. Since the vector space $V_{\Gamma}[A]$ is spanned by hermitian positive elements, there exists a hermitian positive $v \in V_{\Gamma}[\Gamma]$ such that $F(v) \neq G(v)$.

If $\Gamma = x_1 : A_1, \ldots, x_n : A_n$, let $B = A_1 \otimes \cdots \otimes A_n$. By Lemma 7.5.8 there exists a closed term $R : B$ such that $\llbracket R : B \rrbracket(1) = \lambda v$, for some $\lambda > 0$. By Lemma 7.5.7 there exists a term $x : A \triangleright S : \text{bit}$ such that $[x : A \triangleright S : \text{bit}] (Fv) \neq [x : A \triangleright S : \text{bit}] (Gv)$. Now consider $C[\Gamma \triangleright \cdots : A]$ defined by

$$\text{let } (x_1, \ldots, x_n) = R \text{ in } x = [-] \text{ in } S.$$

Then $[C[M]](1) \neq [C[M']] (1)$, hence by Lemma 7.5.9 $C[M] \downarrow b \neq C[M'] \downarrow b$, for some $b \in \{0, 1\}$. It follows that $M \not\approx_{op} M'$, which completes the proof of full abstraction. \qed
Chapter 8

Structure of the Linear-Non-Linear Fragment

In the previous chapter, we described a semantics for the linear fragment of the quantum lambda calculus of Chapter 6. Doing so, we omitted the issue of duplicability. This chapter and the following ones are concerned with the study of the linear-non-linear fragment of the lambda calculus described in Chapter 6. An extended abstract of the work presented here has been published in [Selinger and Valiron, 2008].

8.1 Computations and Values

In Chapter 7, we developed an interpretation of computations as completely positive linear maps between specific vector spaces. Due to the strict linearity, there was no need to distinguish between values and computations within the denotation. In the case of the general quantum lambda calculus, the computations are not the whole story. Due to the probabilistic behavior of the measurement, in order to give a categorical description of the quantum lambda calculus, the analysis of the values has to be separated from the analysis of the computations. For this purpose we will use the semantics described in Section 5.4.3 and describe a computational model to handle the probabilistic side effect.

8.2 Duplicability Versus Non-Duplicability

While the strong monad handles the probabilistic nature of the computation, it does not deal with the question of the non-duplicability. [Coecke and Pavlovic, 2007] offer a solution for duplication at first order using the notion of classical objects. The idea is that the boolean structure \((1,1)\) admits a “copy” operator such as

\[
\delta_{\text{bit}} : \begin{array}{ccc}
1,1 & \rightarrow & 1,1,1,1 \\
(a,b) & \mapsto & (a,0,0,b),
\end{array}
\]

sending the Boolean 0 to the pair \((0,0)\) and the Boolean 1 to the pair \((1,1)\). This approach does not generalize well at higher-order. Indeed, consider the set of functions \((\top \rightarrow \text{bit})\) and the set of pairs of functions \((\top \rightarrow \text{bit}) \otimes (\top \rightarrow \text{bit})\). Using the denotation in Chapter 4, a function \(f : \top \rightarrow \text{bit}\) is represented by a pair \((a,b)\) where \(a\) is the probability of outputting the Boolean 0 and \(b\) the probability of getting the Boolean 1. Thus, in the denotation, it is the same entity as a boolean. If we define \(\delta_{\top \rightarrow \text{bit}}\) as the same “copy” operator, \(\delta_{\top \rightarrow \text{bit}}(f)\) becomes the pair of functions that outputs
8.3. Structure of the Exponential “!”

The model of linear logic offered by Bierman (1993) and described in Section 5.6.2 is almost a perfect fit. However, it is slightly too general for our purpose. In this section we describe the modifications that are needed.

8.3.1 Idempotency

Indeed, the “!” operator of the type system of the quantum lambda calculus is idempotent, in the sense that $x : A ! \Rightarrow x : ! A$ and $! ! A \Rightarrow x : ! ! A$ are inverse one of each other. This is not reflected in the definition of a generic comonad, where the map

$$LLA \xrightarrow{\delta_A} LA \xrightarrow{\epsilon_A} LL$$

is not equal to the identity.

**Definition 8.3.1** (Taylor (1999)). A comonad $(L, \epsilon, \delta)$ on some category is said to be **idempotent** if $\delta : L \Rightarrow LL$ is an isomorphism.

**Example 8.3.2.** Consider any category $\mathcal{C}$. The functor $id_{\mathcal{C}}$ is an idempotent comonad, with the comultiplication and the counit being the identity natural transformation.

Based on the idea of classical objects of Coecke and Pavlovic (2007), a non-trivial example can be constructed. The setting is the category of finite Hilbert spaces. There is no canonical “copy” operation $E \to E \otimes E$ on a given space $E$ unless a basis has been arbitrarily chosen. We define the category $\text{ClasObj}$ based on the category $\text{fdHilb}$ of finite Hilbert spaces.

**Example 8.3.3.** Let $\text{ClasObj}$ be the category with

- Objects: pairs $(E, B_E)$ where $E$ is a finite dimensional Hilbert space and $B_E$ is a set of orthonormal vectors of $E$. We write $\langle B_E \rangle$ for the subspace of $E$ generated by $B_E$, and $E^{\perp B_E}$ for the subspace of $E$ orthogonal to $\langle B_E \rangle$. 

In summary, the structure of the exponential “!” is a reflection of the idempotent property of the “!” operator in the type system of the quantum lambda calculus.
• Arrows from \((E, B_E) \to (F, B_F)\): linear maps from \(E\) to \(F\) such that for all \(b \in B_E\), \(f(b) \in B_F \cup \{0\}\).

We define a functor \(L\) from \(\text{ClasObj}\) to \(\text{ClasObj}\) as follows: For any object \((E, B_E)\), \(L(E, B_E)\) is the object \((\langle B_E \rangle, B_E)\) and for any morphism \(f : (E, B_E) \to (F, B_F)\), \(Lf\) is the restriction of the linear map \(f : E \to F\) to the subspace generated by \(B_E\).

If \(\epsilon_{(E, B_E)} : L(E, B_E) \to (E, B_E)\) is the canonical linear injection and if \(\delta_{(E, B_E)} : L(E, B_E) \to LL(E, B_E)\) is the linear identity, \((L, \epsilon, \delta)\) is an idempotent comonad.

**Lemma 8.3.4.** If \((L, \epsilon, \delta)\) is an idempotent comonad, then \(\delta L = L \delta\), \(L \epsilon = \epsilon L\) and \(\delta^{-1} = L \epsilon\).

**Proof.** Equation \((2.6.1)\) states that \(\delta; L \delta = \delta; \delta L\). Multiplying on the left by \(\delta^{-1}\), we get \(L \delta = \delta L\). Equation \((2.6.2)\) says \(\delta; \epsilon L = \delta; L \epsilon\). Multiplying on the left by \(\delta^{-1}\), we get \(\epsilon L = L \epsilon\). Finally, since \(\delta; L \epsilon = \epsilon d\), again multiplying on the left by \(\delta^{-1}\) we get the last required equation: \(L \epsilon = \delta^{-1}\).

**Lemma 8.3.5.** Suppose that \((L, \epsilon, \delta, d^L, d^L)\) is an idempotent monoidal comonad. Then \(\epsilon_T; d^L_T = id_{L_T}\).

**Proof.** Consider the following diagram:

![Diagram](image)

The equality is obtained from Lemma \(8.3.2\), the lower triangle by naturality of \(\epsilon\) and the upper triangle by functoriality of \(L\) on the monoidality of \(\epsilon\) (Equation \((2.8.8)\)).

**Example 8.3.6.** The category \(\text{ClasObj}\) from Example \(8.3.2\) inherits a symmetric monoidal structure from \(\text{fdHilb}\) in the following manner:

\[(E, B_E) \otimes (F, B_F) = (E \otimes F, \{\epsilon \otimes f \mid \epsilon \in B_E, f \in B_F\}),\]

\(\top = (\mathbb{C}, \{1\})\),

and the tensor product of two morphisms \(f\) and \(g\) is the morphism of Hilbert spaces \(f \otimes g\). If we define the maps

\[d^L_T : \top \to L_T, \quad d^L_{(E, B_E), (F, B_F)} : L(E, B_E) \otimes L(F, B_F) \to L((E, B_E) \otimes (F, B_F)),\]

as the identities of the respective Hilbert spaces \(\mathbb{C}\) and \(E \otimes F\), then the comonad \((L, \epsilon, \delta, d^L, d^L)\) is monoidal.

### 8.3.2 Coherence Property for Idempotent Comonads

We want to be able to define a map \([A] \to [B]\), image of the relation \(A <: B\). Since by Lemma \(8.3.3\) \((::<)\) is an ordering relation, we would like to have a similar notion on the images. The category \(\mathbb{C}\) has an idempotent comonad. In the following we will show a coherence property for the comonad, and use it to define the image of \(A <: B\).
8.3. Structure of the Exponential

**Definition 8.3.7.** Consider a category $\mathcal{C}$ with an idempotent comonad $(L, \delta, \epsilon)$. Let $(F_1, \ldots, F_n)$ be a list of functors $F_i : \mathcal{C}^{m_i} \times (\mathcal{C}^{op})^l_i \to \mathcal{C}$. Suppose $A$ is the set of elements of the form

$$A, B ::= a | F_i(A_1, \ldots, A_{m_i}, B_1, \ldots, B_{l_i}) | LA,$$

where $a$ spans over a given alphabet $A$. Given a map $G : A \to |\mathcal{C}|$, we build the $A$-$G$-category $\mathcal{C}^G$ a follows:

- The set of objects is $A$.
- Arrows are arrows of $\mathcal{D}$, defined by induction as follows:
  - for all objects $A$ in $\mathcal{C}^G$, the arrows $id_{G(A)}$, $\epsilon_{G(A)}$ and $\delta_{G(A)}$ are arrows of $\mathcal{C}^G$.
  - If $f : A \to B$ is an arrow in $\mathcal{C}^G$ then so are $Lf : LA \xrightarrow{L(f)} LB$,
    $$F_i(X_1, \ldots, f, \ldots, X_l, Y_1, \ldots, Y_{m_i}) = F_i(G(X_1), \ldots, f, \ldots, G(X_l), G(Y_1), \ldots, G(Y_{m_i})),
    F_i(X_1, \ldots, f, \ldots, X_l, Y_1, \ldots, f, \ldots, Y_{m_i}) = F_i(G(X_1), \ldots, G(X_l), G(Y_1), \ldots, f, \ldots, G(Y_{m_i})).$$

Finally, if $f : A \to B$ and $g : B \to C$ are arrows of $\mathcal{C}^G$, $(f; g) : A \to C$ is also an arrow of $\mathcal{C}^G$.

**Theorem 8.3.8.** Consider a category $\mathcal{C}$, an alphabet $A$ and a list of functors $(F_1, \ldots, F_n)$ as in definition 8.3.4. If $f : A \to B$ and $g : A \to B$ are two maps of $\mathcal{C}^G$, they are equal.

Following Kelly’s methodology [Kelly and Laplaza, 1980], we define the free category verifying the conditions, and show that this free category is in fact a poset. Without loss of generality, we consider only one $F_i$, that we name $\times : \mathcal{C}^{op} \times \mathcal{C} \to \mathcal{C}$.

**Definition 8.3.9.** Given an alphabet $A$, we define the graph $G$ as follows: the vertices of $G$ are

$$Vertices \ A, B ::= a | (A \times B) | LA,$$

where $a$ ranges over $A$, and the arrows are two-fold. First, for each vertex $A$ there exists arrows $\delta_A : LA \to LL A$ and $\epsilon_A : LA \to A$. Then for each arrow $f : A \to B$ all expansions of $f$ with respect to $(L, \times)$ are arrows in the graph.

Then we define $K$ to be the free category generated by $G$. We write $id_A$ for the identity on $A$. We call the arrows $id_A$, $\epsilon_A$ and $\delta_A$ elementary arrows.

We define a set of relations $\mathcal{R}$. This set contains first $\mathcal{A}(\mathcal{D})$ and $\mathcal{A}(\mathcal{D})$, the equations of functoriality of $L$ and of naturality of $\epsilon$ and $\delta$, so that $(L, \delta, \epsilon)$ is a comonad. It contains the equations for the bifunctoriality of $\times$. We also request equations $L\epsilon_A ; \delta_A = id_{L^2A}$ and $\epsilon_LA = L\epsilon_A$. Furthermore, we request all expansions of the above relations with respect to $(L, \times)$ to belong to $\mathcal{R}$.

Finally, we define the category $\mathcal{D}$ to be $\mathcal{K}/\mathcal{R}$.

**Lemma 8.3.10.** In $\mathcal{D}$, $\times$ is a bifunctor and $(L, \delta, \epsilon)$ is an idempotent comonad.

**Proof.** All the requested equations are there.

**Definition 8.3.11.** We define a map $K : |\mathcal{D}| \to |\mathcal{D}|$ by induction

$$K(a) = a \quad K(L^2A) = K(LA)
K(\epsilon_A) = \epsilon_A K(A \times B) = (KA) \times (KB)$$
and a set of maps $\zeta_A : A \to KA$, one for each object $A$:

$$\zeta_a = \text{id}_a : a \to a, \quad \zeta_{La} = \text{id}_{La} : La \to La,$$

(8.3.1)

$$\zeta_{L^2 A} = L^2 A \xrightarrow{\delta^{-1}} LA \xrightarrow{\zeta_{La}} K(LA),$$

(8.3.2)

We define subsets $LSubVert$ and $SubVert$ of vertices:

$LSubVert \ U ::= a | A \ltimes B,$

$SubVert \ A,B ::= U | LU.$

An element in $SubVert$ is called a subvertex, and an element of $LSubVert$ a linear subvertex. We define a partial ordering relation $\leq$ on subvertices (where $A,B \in SubVert$ and $U,V \in LSubVert$):

$$a \leq a \quad U \leq V \quad U \leq V \quad A \leq A' \quad B \leq B'$$

and a map $m_{A,B}$ for each $A \leq B$:

$$U \xrightarrow{m_{U,V}} V \quad U \xrightarrow{m_{LU,LV}} LV$$

$$m_{LU} = LU \xrightarrow{\epsilon_U,m_{U,V}} V \quad m_{LU,LV} = LU \xrightarrow{Lm_{LU,V}} LV$$

$$m_a = a \xrightarrow{\text{id}_a} a \quad m_{A,A'} = A' \quad B \xrightarrow{m_{B,B'}} B'$$

Lemma 8.3.12. For all $A$, $\zeta_A$ is an isomorphism.

Proof. Proof by induction on $A$, knowing that $\delta_A$ is an isomorphism.

Lemma 8.3.13. For any vertex $A$, $KA$ is a subvertex.

Proof. Proof by induction on $A$.

Lemma 8.3.14. For any vertex $A$, there exists a unique linear subvertex $U$ and a unique $n \geq 0$ such that $A = L^n U$. In that case, $KA = U$ if $n = 0$, $KA = LU$ otherwise.

Proof. Proof by induction on $A$.

Lemma 8.3.15. If $U$ is a subvertex, then $K(LU) = L(KU)$.

Proof. Proof by case distinction.

Lemma 8.3.16. If $U$ is a subvertex, then

$$LU \xrightarrow{\zeta_{LU}} K(LU) = LU \xrightarrow{\zeta_U} L(KU)$$

Proof. Proof using Lemma 8.3.12 and by case distinction on the possible $\zeta_{LU}$.

Lemma 8.3.17. $\leq$ is an partial ordering relation on subvertices.

Proof. For $A,B$ and $C$ subvertices.
• Reflexivity: \( A \leq A \): proved by structural induction on \( A \).

• Antisymmetry: \( A \leq B \) and \( B \leq A \) implies \( A = B \): proved by structural induction on \( A \).

• Transitivity: \( A \leq B \) and \( B \leq C \) implies \( A \leq C \): proved by structural induction on \( A \).

Lemma 8.3.18. If \( A \leq B \) and \( B \leq C \) are in \( \text{SubVert} \),

\[
A \xrightarrow{m_{A,B}} B \xrightarrow{m_{B,C}} C = A \xrightarrow{m_{A,C}} C. \tag{8.3.3}
\]

Proof. We prove by induction on the derivation of \( A \leq C \) that for all \( B \) such that \( A \leq B \) and \( B \leq C \), Equation (8.3.3) is valid.

- If it is an axiom, then \( A = C \) are \( a \) or \( \top \) and the only for \( B \) is to be the same as \( A \) and \( B \): we are done.

- Suppose it is true for sub-derivations of \( LU \leq LW \), \( U \) and \( W \) being linear subvertices. By case distinction the only \( B \) such that \( LU \leq B \) and \( B \leq LW \) is \( B = LV \), where \( V \) is a linear subvertex. Then by functoriality of \( L \) and and by induction hypothesis, the result is true.

- Suppose it is true for sub-derivations of \( LU \leq W \), \( U \) and \( W \) being linear subvertices. By case distinction the only possible \( B \) such that \( LU \leq B \) and \( B \leq W \) are \( B = V \) or \( LV \), \( V \) a linear subvertex.

  - If \( B = V \): then \( m_{LU,V} = LU \xrightarrow{\epsilon_U} U \xrightarrow{m_{U,V}} V \), and \( m_{LU,V}; m_{V,W} \) is

    \[
    \begin{array}{c}
    LU \\
    \xrightarrow{m_{LU,V}} \\
    \downarrow m_{LU,W} \\
    \end{array}
    \xrightarrow{(a)}
    \begin{array}{c}
    V \\
    \xrightarrow{\epsilon_U} \\
    \downarrow m_{U,V} \\
    \end{array}
    \xrightarrow{(b)}
    \begin{array}{c}
    U \\
    \xrightarrow{m_{U,W}} \\
    \downarrow m_{V,W} \\
    \end{array}
    \xrightarrow{(c)}
    \begin{array}{c}
    W \\
    \xrightarrow{(d)}
    \end{array}
    \]

    where the \( (a) \) and \( (c) \) commute by definition, and \( (b) \) commutes by induction hypothesis.

  - If \( B = LV \): then \( m_{LU,LV} = LU \xrightarrow{Lm_{U,V}} LV \), \( m_{LV,W} = LV \xrightarrow{\epsilon_V} V \xrightarrow{m_{V,W}} W \), and \( m_{LU,LV}; m_{LV,W} \) is

    \[
    \begin{array}{c}
    LU \\
    \xrightarrow{Lm_{U,V}} \\
    \downarrow m_{LU,W} \\
    \end{array}
    \xrightarrow{(a)}
    \begin{array}{c}
    LV \\
    \xrightarrow{\epsilon_V} \\
    \downarrow m_{U,V} \\
    \end{array}
    \xrightarrow{(b)}
    \begin{array}{c}
    U \\
    \xrightarrow{m_{U,W}} \\
    \downarrow m_{V,W} \\
    \end{array}
    \xrightarrow{(c)}
    \begin{array}{c}
    W \\
    \xrightarrow{(d)}
    \end{array}
    \]

    where \( (a) \) commutes by naturality of \( \epsilon \), \( (b) \) and \( (d) \) by definition and \( (c) \) by induction hypothesis.
8.3. Structure of the Exponential

- If it is true for sub-derivations of \((D'' \ltimes E) \leq (D \ltimes E'')\), then by case distinction the only possible \(B\) such that \((D'' \ltimes E) \leq B\) and \(B \leq (D \ltimes E'')\) is \(B = (D' \ltimes E')\) for some vertices \(D'\) and \(E'\). Then \(D \leq D' \leq D''\) and \(E \leq E' \leq E''\), and by induction hypothesis we get the result.

Lemma 8.3.19. For any subvertex \(A\), \(m_{A,A} = id_A\).

Proof. Proof by induction on \(A\).

Lemma 8.3.20. Given any arrow \(f : A \to B\), \(KA \leq KB\).

Proof. We prove it by induction on the construction of \(f\): first the result is true for any elementary arrow and for the identity ion objects. Then it is true by induction on any expansion of such arrows, using the definition. Finally, from Lemma 8.3.17 \(\leq\) is transitive and thus it is true for any composition of expansions.

Lemma 8.3.21. For any map \(g : A \to B\), the following diagram commutes:

\[
\begin{array}{ccc}
A & \xrightarrow{g} & B \\
\downarrow \zeta_A & & \downarrow \zeta_B \\
KA & \xrightarrow{m_{A,B}} & KB.
\end{array}
\]

Proof. First note that \(m_{A,B}\) is well-defined using Lemma 8.3.20. Then we proceed by case distinctions.

- First, \(g\) can be the identity, then it’s done.
- It can be an elementary arrow. In the case \(\delta_A\), the following diagram has to commute:

\[
\begin{array}{ccc}
LA & \xrightarrow{\delta_A} & L^2A \\
\downarrow \zeta_{LA} & & \downarrow \zeta_{L^2A} \\
K(LA) & \xrightarrow{m_{K(LA),K(L^2A)}} & K(L^2A).
\end{array}
\]

By definition \(K(L^2A) = K(LA)\), and from Lemma 8.3.18 \(m_{K(LA),K(LA)} = id_{K(LA)}\). Thus diagram becomes:

\[
\begin{array}{ccc}
LA & \xrightarrow{\delta_A} & L^2A \\
\downarrow \zeta_{LA} & & \downarrow \zeta_{L^2A} \quad (a) \\
K(LA) & \xrightarrow{id} & K(LA) \\
\downarrow \zeta_{LA} & & \downarrow \zeta_{L^2A} \quad (b) \\
K(LA) & \xrightarrow{id} & K(LA),
\end{array}
\]

where (a) commutes by property of comonads, (b) commutes by definition, (c) by vacuity.
• In the case \( \epsilon_A \), from Lemma 8.3.14, \( A \) can be either a subvertex \( U \) or of the form \( LB \). In the case \( A = LB \), using the same equality as above, the following diagram has to commute:

\[
\begin{array}{ccc}
L^2B & \xrightarrow{\epsilon_{LB}} & LB \\
\downarrow \zeta_{L^2B} & & \downarrow \zeta_{LB} \\
K(LA) & \xrightarrow{\text{id}} & K(LA),
\end{array}
\]

and (a) commutes by definition, and (b) by vacuity. In the case \( A = LU \), the diagram that needs to commute, using Lemma 8.3.14 and Lemma 8.3.15 is:

\[
\begin{array}{ccc}
LU & \xrightarrow{\epsilon_U} & U \\
\downarrow \zeta_{LU} & & \downarrow \zeta_U \\
L(KU) & \xrightarrow{\text{id}} & L(KU),
\end{array}
\]

which commutes by definition of \( \zeta_{LU} \).

• Then it can be the expansion \( f \) of an elementary arrow: we prove this case by induction on such an expansion. The base case has been done, it remains to show the general case. Suppose then that the result is true for some expansion \( f : A \rightarrow B \). Then we need to show that the diagram commute for \( LF \), for \( f \times X \) and for \( X \times f \).

• Finally, it can be a composition \( f \) of such expansions. By induction on the number of expansions composed, we show that the diagram commutes for \( f \). What remains to be shown is the iterative case: Suppose \( f : A \rightarrow B \) is such a composition, and \( g : B \rightarrow C \) is an expansion, we want the following diagram to commute:

\[
\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow \zeta_A & & \downarrow \zeta_B \\
KA & \xrightarrow{m_{K,A,KB}} & KB \\
\downarrow \zeta_{KA,KKC} & & \downarrow \zeta_{KB,KKC} & \xrightarrow{m_{K,A,KKC}} & C.
\end{array}
\]

The upper triangle commutes by definition, the lower one using Lemma 8.3.15, the left square by induction hypothesis and the right square because we just proved the result for expansions.

\[\square\]

**Corollary 8.3.22.** In \( D \), any two arrows \( f, g : A \rightarrow B \) are equal.

\[\square\]

**Proof.** From Lemma 8.3.21 they are both equal to \( \zeta_A ; m_{K,A,KB} ; \zeta_B^{-1} \).

\[\square\]

**Proof of Theorem 8.3.8.** We prove the theorem when \( (F_1, \ldots, F_N) \) consists only of one functor \( \times : C^{op} \times C \rightarrow C \).

Consider the free category \( D \) with an idempotent comonad described in Definition 8.3.14. There is an inclusion \( I : D \rightarrow C^{G} \), and any arrow in \( C^{G} \) is the image of an arrow in \( D \). Let \( f, g : A \rightarrow B \) be arrows of \( C^{G} \). There exists \( f' \) and \( g' \) in \( D \) such that \( I(f') = f \) and \( I(g') = g \). From Corollary 8.3.22 \( f' = g' \). Thus \( f = g \).
8.3.3 Duplicable Pairs and Pairs of Duplicable Elements

Unlike the work of Benton et al. (1993); Bierman (1993), we want to think of the type \( ! (A \otimes B) \) as a type of pairs of elements of type \( A \) and \( B \): we want to use the same operation to access the components as one would use for a pair of type \( A \otimes B \), without having to use a dereliction operation.

This immediately raises a concern: consider a pair of elements \( \langle x, y \rangle \) of type \( ! (A \otimes B) \). Are \( x \) and \( y \) duplicable? In the usual linear logic interpretation, they are not. Having an infinite supply of pair of shoes does not mean one has an infinite supply of right shoes: we cannot discard the left shoes. On the other hand, in our interpretation of “classical” data as residing in “classical” memory and therefore being duplicable, if the string \( \langle x, y \rangle \) is duplicable, then so should be the elements \( x \) and \( y \). In other words, we want the duplication to “permeate” the pairing.

The choice of such a “permeable” pairing is more or less forced on us by our desire to have no explicit term syntax for structural rules. Consider the following untyped terms, which can be typed if \( t \) is of type \( ! (A \otimes (B \otimes C)) \):

\[
\text{let } \langle x, u \rangle = t \text{ in let } \langle y, z \rangle = u \text{ in } \langle \langle z, y \rangle, x \rangle, \quad \text{(8.3.4)}
\]

\[
\text{let } \langle x, u \rangle = t \text{ in } \langle \text{let } \langle y, z \rangle = u \text{ in } \langle z, y \rangle, x \rangle. \quad \text{(8.3.5)}
\]

First, we expect these two terms to be axiomatically equal. Term \( \text{(8.3.5)} \) should be of type \( ! (C \otimes B) \otimes A \), regardless of the permeability of the pairing: if \( \langle y, z \rangle \) is duplicable, so should be \( \langle z, y \rangle \). Now, consider the term \( \text{(8.3.4)} \) with a non-permeable pairing. In the naive type system, \( u \) ends up being of type \( B \otimes C \), and the variables \( y \) and \( z \) in the final recombination end up being respectively of type \( B \) and \( C \). It is not possible to make \( \langle z, y \rangle \) of the duplicable type \( ! (C \otimes B) \).

We therefore choose a permeable pairing. Is will be reflected, albeit subtly, in the typing rules \((\otimes J)\) and \((\otimes E)\) of Table 9.1. To enforce it in the semantics, we will pick a strong monoidal comonad to model the operator \("!\)".

8.4 Linear Category for Duplication

We now have enough background to define a candidate for the categorical model of the quantum lambda-calculus. As it was advertised, the structure of the categorical semantics will closely follow the one proposed by Bierman (1993), but with the added twist of a computational monad à la Moggi (1991).

**Definition 8.4.1.** A linear category for duplication is a category \( C \) with the following structure:

- a symmetric monoidal structure \((\otimes, \top, \alpha, \lambda, \rho, \sigma)\);
- an idempotent, strongly monoidal, linear exponential comonad \((L, \delta, \epsilon, d^L, d^L, \diamond, \triangle)\);
- a strong monad \((T, \mu, \eta, t)\);
- a Kleisli exponential \(\rightarrow\), that is, a natural bijective map of arrows
  \[ \Phi : C(A \otimes B, TC) \rightarrow C(A, B \rightarrow C) \]
  and a bifunctor \(\rightarrow : C^{op} \times C \rightarrow C\).

The computational linear category is defined as the Kleisli category \(C_T\).

Categories with a combination of a monad and a comonad have been studied by many authors (Barr, 1990; Hyland and Schalk, 2003; Power and Watanabe, 2002). However, none of them are equivalent to linear categories for duplication: either the monad and the comonad commute or the comonad is not idempotent.
Example 8.4.2. Consider the category $\text{ClasObj}$ of Examples 8.3.3 and 8.3.6. It is symmetric monoidal closed, and it has an idempotent, monoidal comonad $(L, \epsilon, \delta, d^L, d^L)$. Note that the coherence maps $d^L$ and $d^L_{A,B}$ are isomorphisms: the comonad $L$ is strongly monoidal. We can make $\text{ClasObj}$ into a non-trivial linear category for duplication, as follows:

- For every object $(E, B_E)$, define the arrows
  \[ \diamondsuit_{(E,B_E)} : L(E, B_E) \rightarrow T \]
  \[ \bigtriangleup_{(E,B_E)} : L(E, B_E) \rightarrow L(E, B_E) \otimes L(E, B_E) \]
  \[ v \mapsto \sum_{e \in B_E} \langle v|e \rangle, \quad v \mapsto \sum_{e \in B_E} \langle v|e \rangle (e \otimes e). \]

Equipped with these two maps, the comonad $L$ becomes an idempotent, strongly monoidal, linear exponential comonad.

- Consider the functor $T : \text{ClasObj} \rightarrow \text{ClasObj}$ sending the object $(E, B_E)$ to $(0, \emptyset)$ and the morphism $f : (E, B_E) \rightarrow (F, B_F)$ to $Tf = \text{id}_{(0, \emptyset)}$. Together with the maps
  \[ \eta_{(E,B_E)} : (E, B_E) \rightarrow T(E, B_E) \]
  \[ \mu_{(E,B_E)} : TT(E, B_E) \rightarrow T(E, B_E) \]
  \[ t_{(E,B_E),(F,B_F)} : (E, B_E) \otimes T(F, B_F) \rightarrow T((E, B_E) \otimes (F, B_F)) \]
  \[ \eta_{(E,B_E)} = x \mapsto 0, \]
  \[ \mu_{(E,B_E)} = \text{id}_{(0, \emptyset)}, \]
  \[ t_{(E,B_E),(F,B_F)} = \text{id}_{(0, \emptyset)}, \]
the functor $T$ is a strong monad.

- Remember that $\text{ClasObj}$ is a symmetric monoidal category. At first sight, the functor $(-) \otimes (F, B_F)$ does not have a right adjoint. However, if one defines the object
  \[ (E, B_E) \rightarrow (F, B_F) = (0, \emptyset), \]
there is a natural isomorphism
  \[ \text{ClasObj}((E, B_E) \otimes (F, B_F), T(G, B_G)) \cong \text{ClasObj}((E, B_E), (F, B_F) \rightarrow (G, B_G)), \]
making $\rightarrow$ into a Kleisli exponential.

With the structure defined above, $\text{ClasObj}$ is a linear category for duplication.

Remark 8.4.3. A linear category for duplication gives rise to a double adjunction

\[ \mathcal{C}_L \xrightarrow{U_L} \mathcal{C} \xleftarrow{F^T} \mathcal{C}_T. \]

Here the left adjunction arises from the co-Kleisli category $\mathcal{C}_L$ of the comonad $L$. It is as in the linear-non-linear models of [Benton 1994], and $\mathcal{C}_L$ is a category of classical (non-quantum) values. The right adjunction arises from the Kleisli category $\mathcal{C}_T$ of the computational monad $T$, as in [Moggi 1991]. Here $\mathcal{C}_T$ is a category of (effectful) quantum computations.

Example 8.4.4. In Example 8.4.2, the category quantum values is the category $\text{ClasObj}$ and the category of classical values $\text{ClasObj}_L$ is equivalent to the category $\text{FinSet}$. Since the image of any object by $T$ is $(0, \emptyset)$, one can say that the category of computations $\text{ClasObj}_T$ contains only one element: the diverging computation.
Chapter 9

A Computational Lambda Calculus for Duplication

In this chapter, we describe a subset of the lambda calculus for quantum computation of Chapter 6. We focus primarily on the type system and language, and not on the structure of the actual “built-in” quantum operations (such as unitary operators and measurements). The language will be a generic call-by-value linear lambda calculus, which is parametric on some primitive operations that are not further explained. It should be understood, however, that the need to support primitive quantum operations motivates particular features of the type system.

9.1 An Indexed Lambda Calculus

We describe a linear typed lambda calculus with higher-order functions and pairs. The language is designed to manipulate both classical data, which is duplicable, and quantum data, which is non-duplicable. For simplicity, we assume the language is strictly linear, and not affine linear as in Chapter 6. This means duplicable values are both copyable and discardable, whereas non-duplicable values must be used once, and only once.

9.1.1 Type System

We define a type system together with a subtyping relation similar as in Section 6.3. The only difference is that type constants are parametrized.

Definition 9.1.1. The set of types is

\[
\text{Type } A, B ::= \alpha \mid (A \rightarrow B) \mid (A \otimes B) \mid \top \mid !A,
\]

where \( \alpha \) ranges over type constants. While the remainder of this thesis does not depend on the choice of type constants, in our main application this is intended to include a type \text{qbit} of quantum bits, and a type \text{bit} of classical bits. The meaning of the types is the same as in Section 6.3. The type system comes also with the subtyping relation of Definition 6.3.3.

Remark 9.1.2. The type system satisfies Lemmas 6.3.4 and 6.3.5.
9.1.2 Terms

The language is a computational language: it is divided into values on the one hand, and general terms, or computations, on the other.

As in Chapter 7, our goal is to find a semantics for the language. The semantics has to be compositional, that is, the semantics of a given term has to be derived from the semantics of its subterm. We are focusing on a language close to the one of Chapter 6. In this language, consider the following two typing judgements, where \( V \) and \( W \) are values:

\[
x : A \triangleright V : !B, \quad y : B \triangleright W : C.
\]

The typing judgement \( x : A \triangleright \text{let } y = V \text{ in } W : C \) has two valid typing derivations:

\[
x : A \triangleright V : !B, \quad y : B \triangleright W : C \quad \text{and} \quad x : A \triangleright B \quad \text{let } y = V \text{ in } W : C.
\]

In order to be able to define a semantics for judgements like \( x : A \triangleright \text{let } y = V \text{ in } W : C \), we will use indexed terms. The purpose of the indexing will be to make sure that each valid typing judgement has a reasonably unique typing tree.

**Definition 9.1.3.** We define the notion of core values, extended values and terms as follows:

\[
\text{CoreValue } \quad U, U' ::= x^A \mid c^A \mid s^n \mid \lambda^n x^A.M \mid \langle U, U' \rangle^n,
\]

\[
\text{ExtValue } \quad V, W ::= U \mid \langle V, W \rangle^n \mid \text{let } x^A = V \text{ in } W \mid \langle x^A, y^B \rangle^n = V \text{ in } W
\]

\[
\text{let } * = V \text{ in } W,
\]

\[
\text{Term } \quad M, N ::= U \mid \langle M, N \rangle^n \mid (MN) \mid \langle x^A, y^B \rangle^n = M \text{ in } N \mid \text{let } * = M \text{ in } N,
\]

where \( n \) is an integer, \( c \) ranges over a set of constant terms, \( x \) over a set of term variables and \( \alpha \) over a set of constant types. We abbreviate \( \langle \lambda^n x^A.M \rangle N \) by \( x^A = N \text{ in } M, \lambda^n x^m.\) let \( * = x^\top \text{ in } M \) by \( \lambda^n x^m.\) and we omit numerical indexes when they are null.

Core values and extended values are often simply called values when the context is clear. General terms are also called computations.

**Remark 9.1.4.** A technicality we introduced is the distinction between core values and extended values. The core values have the same structure as the values of Section 7.2.4. The need for extended values comes from the fact that we wish to have a destructor for the unit type \( \top \) in the category of values, so that we are allowed to write the judgement

\[
x : A, y : \top \triangleright \text{let } * = y^\top \text{ in } x^A : A.
\]

However, as it will be further developed in Remark 9.1.20, this term will cause problem with substitution in certain situations. We are forced to restrict the substitution to core values.

**Convention 9.1.5.** We use the notations \( \Box, \square \) and \( \blacksquare \) as place holders for \( x^A, * \) and \( \langle x^A, y^B \rangle^n \) (not respectively). We use typed version of them when we want to enforce the underlying type. For example, \( \Box^A \) can stand for \( x^A, * \) if \( A = \top \), or \( \langle x^B, y^C \rangle^n \) if \( A = !^n(B \otimes C) \).

We also define a notion of untyped terms as terms with no index:

\[
\text{PureTerm } \quad M, N ::= x \mid c \mid s \mid \lambda x.M \mid \langle MN \rangle \mid \langle M, N \rangle \mid \text{let } \langle x, y \rangle = M \text{ in } N \mid \text{let } *= M \text{ in } N.
\]

The erasure operation \( \text{Erase} : \text{Term} \rightarrow \text{PureTerm} \) is defined as the operation of removing the types and integers attached to a given indexed term. If \( M = \text{Erase}(M) \), we say that \( M \) is an indexation of \( M \). We define notions of free variables and \( \alpha \)-equivalence on terms, denoted by \( =_\alpha \), in the usual way (see for example Section 6.1).
We use the notation $\{\cdot\}$.

We define a special derived rule called $(\text{let})$:

$$
\frac{\Delta, \Gamma_1, x : A \triangleright M : B \quad \Delta_1, \Gamma_2 \triangleright N : A}{\Delta, \Gamma_1, \Gamma_2 \triangleright \text{let } x^A = N \text{ in } M : B} \quad \text{(let)}
$$

It is derived using Definition $\text{[6.3.6]}$ stating that let $x^A = N$ in $M$ is the term $(\lambda^0x^A.M)N$:

$$
\frac{\Delta, \Gamma_1, x : A \triangleright M : B \quad \Delta_1, \Gamma_2 \triangleright \lambda^0x^A.M : B}{\Delta, \Gamma_1 \triangleright \lambda^0x^A.M : B} \quad \text{(\lambda)}
$$

$$
\frac{\Delta, \Gamma_1 \triangleright \lambda^0x^A.M : B \quad \Delta_1, \Gamma_2 \triangleright N : A}{\Delta, \Gamma_1, \Gamma_2 \triangleright (\lambda^0x^A.M)N : B} \quad \text{(app)}
$$

Table 9.1: Typing rules for the linear-non-linear quantum lambda calculus

Lemma 9.1.6. Suppose that $V$ is a core value (respectively an extended value). Then if $M$ is a term such that $\text{Erase}(M) = \text{Erase}(V)$ then $M$ is a core value (respectively an extended value). □

Lemma 9.1.7. Suppose that $M$ and $M'$ are two terms such that $\text{Erase}(M) = \text{Erase}(M')$. Then $\text{FV}(M) = \text{FV}(M') = \text{FV}(\text{Erase}(M'))$.

Definition 9.1.8. The indexation of terms induces a partial map from terms to types, called the raw type of $M$. We write $M : A$ to say that $A$ is the raw type of $M$, or that $M$ is raw-typed, and we define it inductively as follows:

- $x^A : A$,
- $c^B : B$,
- $*^n : !^n\top$,
- $\lambda^n x^A : \{M : A \rightarrow B\}N : B$,
- $\langle x^A, y^B \rangle^n = M \text{ in } \{N : C\} : C$,
- $let \ s = M \text{ in } \{N : C\} : C$.

We use the notation $\{M : A\}$ to say “the term $M$ when it is of type $A$”.

9.1.3 Typing Judgements

Definition 9.1.9. We define the notion of typing context of Definition $\text{[6.3.6]}$. A typing judgement is a tuple $\Delta \triangleright M : A$, where $M$ is an indexed term, $A$ is a type, and $\Delta$ is a typing context. As before, to each constant term $c$ we assign a type $\!A_c$. A valid typing judgement is a typing judgement that can be derived from the typing rules in Table 9.1.
Lemma 9.1.11. Consider a valid typing judgement $\Delta \triangleright M : A$. Then $FV(M) \subseteq |\Delta|$.

Proof. Proof by induction on the size of $M$.

Case $M \equiv x^B$. The only applicable rule is $(ax_1)$. Then the typing judgement is of the form $!\Delta, x : A \triangleright x^B : B$. We thus have $FV(M) = \{x\} \subseteq |\Delta| \cup \{x\} = |\Delta, x : A|$.

Cases $M \equiv c^B$ and $M \equiv \ast^n$. In both cases $FV(M) = \emptyset$. The result is true by vacuity.

Case $M \equiv \lambda^n x^A. N$. The only applicable rule is $(\lambda_i)$, with $i = 1$ if $n = 0$, $i = 2$ otherwise. Thus there exists some $B$ such that the typing judgement is of the form $!\Delta, x : A \triangleright x^nA. N$ with $\Delta, x : A \triangleright N : B$. By induction hypothesis, we have $FV(N) \subseteq |\Delta, x : A| = |\Delta| \cup \{x\}$. By definition of free variables, $FV(\lambda^n x^A. N) = FV(N) \setminus \{x\} \subseteq |\Delta|$.

Case $M \equiv NP, (N, P)^n$ and let $* = M$ in $N$. The applicable rules are respectively (app), $(\otimes, I)$ and $(\top, E)$. The context $\Delta$ splits into $!\Delta', \Gamma_1, \Gamma_2$ such that $!\Delta', \Gamma_1 \triangleright N : B$ and $!\Delta', \Gamma_2 \triangleright P : C$ for some types $B$ and $C$. By induction hypothesis, $FV(N) \subseteq |!\Delta', \Gamma_1|$ and $FV(P) \subseteq |!\Delta', \Gamma_2|$. Since $FV(M) = FV(N) \cup FV(P)$, we have $FV(M) \subseteq |!\Delta'| \cup |\Gamma_1| \cup |\Gamma_2| = |\Delta|$.

Case $M \equiv let (x^A_1, y^A_2)^n = N in P$. The only applicable rule is $(\otimes, E)$. There exists some type $B$ for which the typing judgement $\Delta \triangleright let (x^A_1, y^A_2)^n = N in P : B$ is valid. Moreover, $\Delta$ splits into $!\Delta', \Gamma_1, \Gamma_2$ such that $!\Delta', \Gamma_1 \triangleright N : !^n(A_1 \otimes A_n)$ and such that $!\Delta', \Gamma_2, x : !^nA_1, y : !^nA_2 \triangleright P : B$. By induction hypothesis, $FV(N) \subseteq |!\Delta', \Gamma_1| = |!\Delta'| \cup |\Gamma_1|$ and $FV(P) \subseteq |!\Delta', \Gamma_2, x : !^nA_1, y : !^nA_2| = |!\Delta' \cup |\Gamma_2| \cup \{x, y\}|$. By definition of free variables, $FV(M) = FV(N) \cup (FV(P) \setminus \{x, y\})$. Thus $FV(M) \subseteq |\Delta|$.

And this closes the proof of Lemma 9.1.11.

Lemma 9.1.12. Consider a term $M$ and any valid typing judgement $\Delta \triangleright M : B$. Then the raw type $A$ of $M$ exists, and the type $B$ is equal to $A$.

Proof. Proof by structural induction on $M$, looking at a typical typing judgement $\Delta \triangleright M : A$.

Case $M \equiv x^B$. The only applicable rule is $(ax_1)$. Then the typing judgement is of the form $!\Delta, x : A \triangleright x^B : B$. We thus have $M : B$.

Case $M \equiv c^B$. The only applicable rule is $(ax_2)$. Thus the typing judgement is of the form $!\Delta \triangleright c^B : B$. We thus have $M : B$.

Case $M \equiv \ast^n$. The only applicable rule is $(\top, I)$. The type $B$ is of the form $!^n\top$ and the typing judgement is of the form $!\Delta \triangleright \ast^n : !^n\top$. Thus we have $M : B$.

Case $M \equiv \lambda^0x^A. N$. The only applicable rule is $(\lambda_1)$. Thus there exists some $B$ such that the typing judgement is of the form $!\Delta \triangleright \lambda^0x^A. N : A \rightarrow B$ with $\Delta, x : A \triangleright N : B$. By induction hypothesis, we have $N : B$. Thus $\lambda^0x^A. N : A \rightarrow B$.

Case $M \equiv \lambda^n+1x^A. N$. The only applicable rule is $(\lambda_2)$. Then $\Delta = !\Delta'$, and there exists some $B$ such that the typing judgement is of the form $!\Delta' \triangleright \lambda^n+1x^A. N : !^n+1(A \rightarrow B)$. The judgement is inferred from $!\Delta', x : A \triangleright N : B$. By induction hypothesis, we have $N : B$. This makes $\lambda^n+1x^A. N : !^n+1(A \rightarrow B)$.

Case $M \equiv NP$. The only applicable rule is (app). The context $\Delta$ splits into $!\Delta', \Gamma_1, \Gamma_2$ such that $!\Delta', \Gamma_1 \triangleright N : A \rightarrow B$ and $!\Delta', \Gamma_2 \triangleright P : A$. By induction hypothesis, $N : A \rightarrow B$ and $M : A$. Thus $NP : B$. 


9.1. An Indexed Lambda Calculus

Case \( M \equiv \langle N, P \rangle^n \). The only applicable rule is \((\odot, I)\). This means \( \Delta \triangleright \langle N, P \rangle^n : !^n(A \odot B) \), and the context \( \Delta \) splits into \( !^n(\Delta', \Gamma_1, \Gamma_2) \) such that \( !^n(\Delta', \Gamma_1) \triangleright N : !^nA \) and such that \( !^n(\Delta', \Gamma_2) \triangleright P : !^nB \). By induction hypothesis, \( N : !^nA \) and \( P : !^nB \). Thus \( \beta\eta \langle N, P \rangle^n : !^n(A \odot B) \).

Case \( M \equiv \text{let } * = N \text{ in } P \). The only applicable rule is \((\top, E)\). For some type \( A \), the typing judgement \( \Delta \triangleright \text{let } * = N \text{ in } P : A \) is valid and \( \Delta \) splits into \( !^n(\Delta', \Gamma_1, \Gamma_2) \) such that \( !^n(\Delta', \Gamma_1) \triangleright N : \top \) and such that \( !^n(\Delta', \Gamma_2) \triangleright P : A \). By induction hypothesis, \( P : A \). This means \( \text{let } * = N \text{ in } P : A \).

Case \( M \equiv \text{let } (x^n, y^n)^n = N \text{ in } P \). The only applicable rule is \((\odot, E)\). We have the valid typing judgement \( \Delta \triangleright \text{let } (x^n, y^n)^n = N \text{ in } P : B \) for some type \( B \) and \( \Delta \) splits into \( !^n(\Delta', \Gamma_1, \Gamma_2) \) such that \( !^n(\Delta', \Gamma_1) \triangleright N : !^n(A_1 \odot A_2) \) and such that \( !^n(\Delta', \Gamma_2) \triangleright x : !^nA_1, y : !^nA_2 \triangleright P : B \). By induction hypothesis, \( P : B \). We deduce that \( M : B \).

Therefore, regardless of the chosen typing judgement \( \Delta \triangleright M : A \), \( A \) is always equal to the raw type of \( M \).

\[ \text{Remark 9.1.13.} \quad \text{Although the type } A \text{ in a valid typing judgement } \Delta \triangleright M : A \text{ is only dictated by } M, \text{ the context } \Delta \text{ cannot be chosen arbitrarily for the judgement to be valid. Consider the term } f^{A\rightarrow A}(f^{A\rightarrow A}x^A) : A. \text{ The context } (f : !^n(A \rightarrow A), x : A) \text{ makes a valid typing judgement, but } (f : A \rightarrow A, x : A) \text{ does not.} \]

\[ \text{Lemma 9.1.14.} \quad \text{Consider a valid typing judgement } \Delta \triangleright M : B \text{ and the subtyping relation } \Delta' <: \Delta. \text{ Then } \Delta' \triangleright M : B \text{ is valid.} \]

Proof. Let \( \pi \) be a derivation of \( \Delta \triangleright M : B \) The proof is done by induction on the size of \( \pi \).

Case \((ax_1)\). The typing judgement is of the form \( !\Delta, x : A \triangleright x^B : B \) with \( A <: B \). We have then \( \Delta = (\Delta, x : A) \). Since \( \Delta' <: \Delta \), the context \( \Delta' \) is of the form \( (\Delta', x : A') \), where \( !\Delta' <: !\Delta \) and \( A' <: A \). Note that \( !\Delta' \) is duplicable from Lemma 8.3.20. Since \( A <: B \), we have \( A' <: B \). Applying rule \((ax_1)\), we have that \( !\Delta', x : A' \triangleright x^B : B \) is valid.

Cases \((ax_2)\) and \( (\top, I)\). The typing judgements are respectively of the form \( !\Delta \triangleright c^B : B \) and \( !\Delta \triangleright *^n : !^n\top \), where \( \Delta = !\Delta \). Since \( \Delta' <: \Delta \), from Lemma 8.3.20 we can therefore apply \((ax_2)\) (respectively \((\top, I)\)) and get that \( !\Delta' \triangleright M : B \) is valid.

Case \((\lambda x)\). There exists some \( B \) such that the typing judgement is of the form \( \Delta \triangleright \lambda x^A.N : A \rightarrow B \) with \( \Delta, x : A \triangleright N : B \). Since \( (\Delta', x : A) <: (\Delta, x : A) \), by induction hypothesis, we have \( \Delta', x : A \triangleright N : B \). Applying \((\lambda x)\), we get that \( \Delta \triangleright \lambda x^A.N : A \rightarrow B \) is valid.

Case \((\lambda y)\). We have \( \Delta = !\Delta \), and there exists some \( B \) such that the typing judgement is of the form \( \Delta \triangleright \lambda y^A.N : !^{n+1}(A \rightarrow B) \). The judgement is inferred from \( !\Delta, x : A \triangleright N : B \). Since \( \Delta' <: !\Delta \), from Lemma 8.3.20 we have \( !\Delta', x : A \triangleright N : B \). We have therefore \( !\Delta', x : A < : !\Delta, x : A \). By induction hypothesis, we have \( !\Delta', x : A \triangleright N : B \). Finally, we can apply the typing rule \((\lambda y)\) in order to get that \( !\Delta' \triangleright \lambda y^A.N : !^{n+1}(A \rightarrow B) \) is valid.

Cases \((\text{app}), (\odot I), (\top E) \) and \((\odot E)\). The term \( M \) is respectively of the form

\[ M \equiv NP, \quad M \equiv \langle N, P \rangle^n, \quad M \equiv \text{let } * = N \text{ in } P, \quad M \equiv \text{let } (x^{D_1}, y^{D_2})^n = N \text{ in } P. \]

The typing context \( \Delta \) splits into \( (\Delta', \Gamma_1, \Gamma_2) \) such that \( !\Delta', \Gamma_1 \triangleright N : B_1 \) and such that \( !\Delta', \Gamma_2, \Delta \triangleright P : B_2 \), for some types \( B_1, B_2 \) and a context \( \Lambda \) that is empty for the first three cases and equal to \( (x : D_1, y : D_2) \) in the last case.
Let $9.1. An Indexed Lambda Calculus 114$

Proof. The proof is done by induction on the structure of some context $\Delta$. Cases

Case The only inductive case is the following.

Proof by induction on the size of the derivation of $\Delta$.

Case $V$. The typing judgement is then of the form $!\Delta, x : A \vdash x^B : !B'$, with $A <: !B$. By Lemma \ref{lem:typing-dual}, the type $A$ is of the form $!A'$, and the context $\Gamma$ is of the requested form.

Case $V = c^B$. Here, the only typing rule available for it is $(ax_2)$. The typing judgement is therefore of the form $!\Delta \vdash c^B : B$: the lemma is true in this case.

Case $V = *^m$. The only typing rule available for it is $(\top, I)$. The typing judgement is therefore of the form $!\Delta \vdash *^{n+1} : !^n+1 \top$: as in the previous case, the lemma is true.

Case $V = \lambda^m x^B. M$. There are two available typing rules for validating $\Gamma \vdash \lambda^m x^B. M : !A$, but only one, that is $(\lambda_2)$, for a duplicable lambda abstraction. This means $m = n + 1$, and $!A = !^{n+1}(B \rightarrow C)$. The fact that $\Gamma$ is of the form $!\Delta$ is one of the requirement of this typing rule.

The only inductive case is the following.

Case $V = (V_1, V_2)^m$. The only available typing rule is $(\otimes, I)$, stating that the type $!A$ is of the form $!^{n+1}(B \otimes C)$, that $m = n + 1$ and that $\Gamma = !\Delta, \Gamma_1, \Gamma_2$, with $!\Delta \vdash V_1 : !^{n+1}B$ and $!\Delta, \Gamma_2 \vdash V_2 : !^{n+1}C$ being valid typing judgements. Since $V_1$ and $V_2$ are core values, the induction hypothesis applies, and $\Gamma_1$ is of the form $!\Delta'$ and $\Gamma_2$ is of the form $!\Gamma'$. This makes $\Gamma$ of the requested form.

Hence, by structural induction on $V$, Lemma \ref{lem:typing-indices} is valid.

Lemma 9.1.16. Consider the following valid typing judgement: $\Delta, x : A \vdash M : B$. Then for every free instance $x^{A'}$ in $M$, $A <: A'$.

Proof. Proof by induction on the size of the derivation of $\Delta, x : A \vdash M : B$.

Case $(ax_1)$. The typing judgement is of the form $!\Delta, y : A \vdash y^B : B$, with $A <: !B$. If $y = x$, then the result is true since $x^B$ is the only free variable. If $y \neq x$, there is no instance of $x$, so the result is true by vacuity.

Case $(ax_2)$. The typing judgement is of the form $!\Delta \vdash c^B : B$: there is no free variable, the result is true by vacuity.

Cases $(\lambda_1)$ and $(\lambda_2)$. The typing judgement is of the form $\Delta, x : A \vdash \lambda^m y^B. M : !^n(B \rightarrow C)$, with $\Delta, x : A, y : B \vdash M : !C$ and $y \neq x$. By induction hypothesis, for every free instance $x^{A'}$ of $M$ one has $A <: A'$. Thus it is also true for every free instance $x^{A'}$ of $\lambda^m y^B. M$.

Cases $(app)$, $(\otimes, I)$, $(\top, E)$ and $(\otimes, E)$. The term $M$ is respectively of the form

$$M \equiv NP, \quad M \equiv (NP)^n, \quad M \equiv \text{let } * = N \text{ in } P, \quad M \equiv \text{let } (y^{D_1}, z^{D_2})^n = N \text{ in } P.$$
The typing context $\Delta : x : A$ splits into $!\hat{\Delta}, \Gamma_1, \Gamma_2$ such that $!\hat{\Delta}, \Gamma_1 \triangleright N : B_1$ and such that $!\hat{\Delta}, \Gamma_2, \lambda \triangleright P : B_2$, for some types $B_1, B_2$ that depend on the rule used and for some context $\Lambda$, empty in the three first cases and equal to $(y : D_1, z : D_2)$ in the last case. Using $\alpha$-equivalence one can assume that $x$ is different from $y$ and $z$. There are three cases, depending on where $x : A$ is to be found.

*Found in $\Gamma_1$. Then there is no free instance of $x$ in $P$, and by induction hypothesis every free instance $x^{A'}$ in $N$ are such that $A <: A'$. Then for all free instances $x^{A'}$ in $M$, $A <: A'$.*

*Found in $\Gamma_2$. Then there is no free instance of $x$ in $N$, and by induction hypothesis every free instance $x^{A'}$ in $P$ are such that $A <: A'$. Then for all free instances $x^{A'}$ in $M$, $A <: A'$.*

*Found in $!\Delta$. Applying induction hypothesis on both typing judgements, we get that or all free instances $x^{A'}$ in $N$ and in $P$, thus in $M$, $A <: A'$.*

Thus by induction, the lemma is valid.

**Lemma 9.1.17.** Consider a valid typing judgement $\Delta \triangleright M : A$, where $M$ is of the form $(N, P)^n$, $NP$, let $x = N$ in $P$ or let $(y^C, z^D)^n = N$ in $P$. If $x : B$ if $x \neq y, z$ is in $\Delta$ such that $B$ is not of the form $!A'$ then $x$ cannot be free both in $N$ and in $P$.

**Proof.** The proof is done by case distinction on the first typing rule used in the derivation of $\Delta \triangleright M$.

**Definition 9.1.18.** In a typing judgement $\Delta \triangleright M : A$, a term variable $x \in |\Delta|$ is called dummy if $x \notin \text{FV}(M)$.

**Lemma 9.1.19.** Let $\Delta, x : A \triangleright M : B$ be a valid typing judgement where $x$ is a dummy variable for $M$. Then

- 1. the type $A$ is of the form $!A'$;
- 2. the typing judgement $\Delta \triangleright M : B$ is valid;
- 3. for any fresh variable $y$ and any type $C$, the typing judgement $\Delta, x : A, y : !C \triangleright M : B$ is valid.

**Proof.** We prove the result by induction on the size of the derivation of $\Delta, x : A \triangleright M : B$.

*Case (ax1).* The typing judgement is of the form $!A', z : D \triangleright z^E : E$, with $D <: E$. If there is a dummy variable $x$, it is in $|\Delta'|$ and is therefore duplicable. If we write $!A' = (!A''), x : A$, by rule (ax1) the typing judgement $!A''$, $z : D \triangleright z^E : E$ is valid. Now, if for some fresh variable $y$ if we consider the typing judgement $!A', z : D, y : !C \triangleright z^E : E$, it is valid by the same rule (ax1).

*Case (ax2) and case ($\top.$I).* The typing judgement has a context of the form $!A'$. If there is a dummy variable $x$, it is in $|\Delta'|$ and is therefore duplicable. Removing this variable from the context does not change the validity of the judgement. Now, if we extend the context to $!A', y : !C$, the typing judgement is again valid by the same rule (ax2) or ($\top.$I).

*Case ($\lambda_1$) and case ($\lambda_2$).* The typing judgement is $\Delta, x : A \triangleright \lambda^n z^D, N : !n (D \rightarrow E)$, such that $\Delta, x : A, z : D \triangleright N : E$ is valid. If $x \notin \text{FV}(\lambda^n z^D, N)$, then $x$ is not in $\text{FV}(N)$ (since $x \neq z$), and by induction hypothesis its type is of the form $!A'$.

Now, consider some fresh $y$ and some type $C$. By induction hypothesis, $\Delta, y : !C, x : A, z : D \triangleright N : E$ and $\Delta, z : D \triangleright N : E$ are valid. If the rule applied was ($\lambda_1$), then the integer $n$ is 0, and one can again apply ($\lambda_1$) to get $\Delta, x : A, y : !C \triangleright \lambda^n z^D, N : !n (D \rightarrow E)$ and $\Delta \triangleright \lambda^n z^D, N : !n (D \rightarrow E)$. If the rule applied was ($\lambda_2$), then the integer $n$ is greater than 0 and the context $\Delta$ is of the form $!A'$. Then rule ($\lambda_2$) can again be applied to get $!A', x : A, y : !C \triangleright \lambda^n z^D, N : !n (D \rightarrow E)$ and $!A' \triangleright \lambda^n z^D, N : !n (D \rightarrow E)$.
9.1. An Indexed Lambda Calculus

Cases \( (\text{app}), (\otimes I), (\top E) \) and \( (\otimes E) \). The term \( M \) is respectively of the form

\[
M \equiv NP, \quad M \equiv (N, P)^n, \quad M \equiv \text{let } * = N \text{ in } P, \quad M \equiv \text{let } \langle x^{D_1}, y^{D_2} \rangle^n = N \text{ in } P.
\]

The typing context \( (\Delta, x : A) \) splits into \( !\Delta', \Gamma_1, \Gamma_2 \) such that \( !\Delta', \Gamma_1 \triangleright N : B_1 \) and such that \( !\Delta', \Gamma_2 \triangleright P : B_2 \), for some types \( B_1, B_2 \) that depend on the rule used.

First let us prove that \( \Delta, x : A, y : !C \triangleright M : B \) is valid when \( y \) is a fresh variable and \( C \) is any type. By induction hypothesis, \( !\Delta', \Gamma_1, y : !C \triangleright N : B_1 \) is valid. So applying back the rule that was used, we get that \( \Delta, x : A, y : !C \triangleright M : B \) is valid.

Second, let us show that if \( x \notin FV(M) \), then its type is of the form \( !A' \) and \( \Delta \triangleright M : B \) is valid. There are three cases, depending on where \( x \) is to be found.

**Found in \( \Gamma_1 \).** Then since \( x \in !|\Delta', \Gamma_1| \) but \( x \notin FV(N) \), by induction hypothesis the type of \( x \) in the context is of the form \( !A \), and if \( \Gamma_1 = (\Gamma'_1, x : A) \), we have \( !\Delta, \Gamma'_1 \triangleright N : B_1 \) valid. Applying back the typing rule used, we get \( \Delta \triangleright M : B \) valid.

**Found in \( \Gamma_2 \).** Then since \( x \in !|\Delta', \Gamma_2| \) but \( x \notin FV(P) \), by induction hypothesis the type of \( x \) in the context is of the form \( !A \), and if \( \Gamma_2 = (\Gamma'_2, x : A) \), we have \( !\Delta, \Gamma'_2 \triangleright P : B_2 \) valid. Applying back the typing rule used, we get \( \Delta \triangleright M : B \) valid.

**Found in \( !\Delta' \).** Then the type of \( x \) is automatically of the form \( !A \). By induction hypothesis, if \( !\Delta' = (!\Delta'', x : A) \), both \( !\Delta'', \Gamma_1 \triangleright N : B_1 \) and \( !\Delta'', \Gamma_2 \triangleright P : B_2 \) are valid. Applying back the typing rule used, we get \( \Delta \triangleright M : B \) valid.

And this ends the proof. \( \square \)

### 9.1.4 Type Casting and Substitution Lemma

We now wish to define a set of call-by-value equations on typed terms. To be able to define a well-typed \( \beta \)-reduction rule, we first need a substitution lemma. Given a value \( x : A \triangleright V : B \) and a term \( y : B \triangleright M : C \), one expects \( x : A \triangleright M[V / y] : C \) to be well typed. Unfortunately, in the presence of Church-style type indices and subtyping, the naive notion of substitution is not technically well-typed. For example, consider the following valid typing derivations:

\[
\frac{A \rightarrow A \leftarrow !A \rightarrow A}{x : A \rightarrow A \triangleright x^{!A\rightarrow A} : !A \rightarrow A}, \quad \frac{A \leftarrow A}{y : A \triangleright y^A : A \triangleright \lambda^0 y^A \cdot y^A : A \rightarrow A}.
\]

Having two valid typing judgements of the form \( x : B \triangleright M : C \) and \( !V : B \), it is reasonable to expect to be able to substitute \( V \) for \( x \) in \( M \). Doing so yields the following typing judgement:

\[
\triangleright \lambda^0 y^A \cdot y^A : !A \rightarrow A,
\]

which is not technically valid due to the superscript on the bound variable. The standard trick to resolve this issue (see e.g. [Pierce 2002]) is to use implicit typecasting, or coercion. In this section we give a precise definition of substitution using typecasting.

**Definition 9.1.20.** Given \( M : A \) and \( A \leftarrow B \), we define the map \( \text{TypeCast}(M, B) \), written \( \{M : A \leftarrow B\} \), or simply \( \{M : B\} \), by induction on \( M \) as follows:

- **Base cases:**
  \[
  \{x^A : B\} = x^B, \quad \{c^A : B\} = c^B, \quad \{s^n : !^m \top\} = s^m.
  \]
9.1. An Indexed Lambda Calculus

• Induction cases:

\[
\lambda^n x A . M : !^k (A' \rightarrow B') = \lambda^n x A'. \{M : B',\},
\]

\[
\{M \{N : A \} : B\} = \{M : A \rightarrow B\} N,
\]

\[
\{(M, N) : !^m (A \otimes B)\} = \{\{M : !^m A\}, \{N : !^m B\}\}^m,
\]

\[
\{\text{let } (x^A, y^B)^n = M \text{ in } N : C\} = \{\text{let } x^A, y^B)^n = M \text{ in } \{N : C\},
\]

\[
\{\text{let } * = M \text{ in } N : C\} = \{\text{let } * = M \text{ in } \{N : C\}\}.
\]

Lemma 9.1.21. Suppose \(N : A\) and \(A : A'.\) Then

\[
\{\text{let } x^B = M \text{ in } N : A'\} = (\text{let } x^B = M \text{ in } \{N : A'\}).
\]

Proof. Using Definition 9.1.20:

\[
\{\text{let } x^B = M \text{ in } N : A'\} = \{(\lambda^0 x^B . N) M : A'\}
\]

\[
= \{\lambda^0 x^B . N : B \rightarrow A'\} M
\]

\[
= (\lambda^0 x^B . \{N : A'\}) M
\]

\[
= (\text{let } x^B = M \text{ in } \{N : A'\}).
\]

And this ends the proof.

Lemma 9.1.22. Suppose that \(M : A\) and that \(A : A' : A''.\) Then \(\{\{M : A'\} : A''\} = \{M : A''\}.
\]

Proof. Proof by induction on the size of \(M\).

Lemma 9.1.23. Suppose that \(M : A.\) then \(\{M : A\} = M.\)

Proof. Proof by structural induction on \(M.\)

Lemma 9.1.24. If the raw type \(A\) of \(M\) exists and if \(A : A',\) then \(\{M : A'\}\) is well-defined and of raw type \(A'.\)

Proof. Proof by structural induction on \(M.\)

Lemma 9.1.25. Suppose \(M : A\) and \(A : A'.\) Then \(\text{Erase}(M) = \text{Erase}\{M : A'\}.\)

Proof. Proof by structural induction on \(M.\)

Lemma 9.1.26. Consider a valid typing judgement \(\Delta \triangleright M : A\) and the subtyping relation \(A : A'.\) Then \(\Delta \triangleright \{M : A'\} : A'\) is valid.

Proof. Proof by induction on the size of \(M.\)

Lemma 9.1.27. Suppose \(M : A\) and \(A : A'.\) If \(M\) is a core value (respectively an extended value), so is \(M' = \{M : A'\}.\)

Proof. Lemma 9.1.25 states that \(\text{Erase}(M) = \text{Erase}(M')\) and Lemma 9.1.6 that since \(M\) is a (core, extended) value, so is \(M'.\)
Definition 9.1.28. Given two valid typing judgements $!\Delta, \Gamma_1 \triangleright V : A$ and $!\Delta, \Gamma_2, x : A \triangleright M : B$ where $V$ is a core value, where $M$ is any term, and where $|\Gamma_1| \cap |\Gamma_2| = \emptyset$, we define the substitution $M[V/x]$ (capture avoiding) of $x$ by $V$ in $M$ as follows: we replace each free instance $x^A$ (where $A \ll A'$ from Lemma 9.1.16) in $M$ by $[V \ll A']$. This is formally defined as follows:

$$(x^A)[V/x] = \{V \ll A\},$$

$$(c^B)[V/x] = c^B,$$

$$(s^n)[V/x] = s^n,$$

$$(MN)[V/x] = (M[N/x])(N[V/x]),$$

$$( (M,N)^n )[V/x] = (M[N/x],N[V/x])^n,$$

$$(\text{let } * = M \text{ in } N)[V/x] = \text{let } * = (M[V/x]) \text{ in } (N[V/x]),$$

$$(\lambda^n x^C.M)[V/x] = \lambda^n x^C.M,$$

$$(\lambda^n y^C.M)[V/x] = \lambda^n y^C.(M[V/x]) \quad (\text{if } y \neq x \text{ and } y \not\in \text{FV}(V)).$$

If $y = x$ or $z = x$:

$$(\text{let } (y^C,z^D)^n = M \text{ in } N)[V/x] = (\text{let } (y^C,z^D)^n = (M[V/x]) \text{ in } N).$$

If $y \neq x$ and $z \neq x$ (and $y,z \not\in \text{FV}(V)$):

$$(\text{let } (y^C,z^D)^n = M \text{ in } N)[V/x] = (\text{let } (y^C,z^D)^n = (M[V/x]) \text{ in } (N[V/x])).$$

Definition 9.1.29. Suppose that $!\Delta, \Gamma_i \triangleright V_i : A_i$ are valid typing judgements, for $i = 1 \ldots n$, where $V_i$ is a core value. Suppose that $!\Delta, \Gamma, x_1 : A_1, \ldots, x_n : A_n \triangleright M : B$ is valid. By $\alpha$-equivalence one can assume that the $x_i$'s are not free in any $V_j$'s. Assuming this, we define the multiple substitution $M[V_1/x_1, \ldots, V_n/x_n]$ by induction on $n$:

- If $n = 0$, we define $M[]$ to be $M$.
- If $n \neq 0$, we define $M[V_1/x_1, \ldots, V_n/x_n]$ to be $M[V_1/x_1, \ldots, V_{n-1}/x_{n-1}][V_n/x_n]$, using Definition 9.1.28.

Remark 9.1.30. Note that we only allowed substitution by core values, and not by extended values nor by general terms. This is due to the strict linearity of the type system. Suppose that we are given the valid typing judgements

$$x : \top \triangleright \text{let } * = x^\top \text{ in } k : \top, \quad y : !\top \triangleright c : A_c.$$  

If we were allowed to substitute term variables by extended values, then one could substitute the former term in place of $y$ in the latter term. However, doing so would yield the non-valid typing judgement

$$x : \top \triangleright c : A_c.$$  

The problem comes from the fact that an object of type $\top$ can be weakened, although it is not explicitly duplicable.

Lemma 9.1.31. In Definition 9.1.28, if $x \not\in \text{FV}(M)$, $M[V/x] = M$.

Proof. One proves by structural induction on $M$ that if $x \not\in \text{FV}(M)$ then $M[V/x] = M$.

Case $M \equiv y^C$. Since $x \not\in \text{FV}(M)$, $y \leq x$. Then by definition $M[V/x] = M$.
9.1. An Indexed Lambda Calculus

Cases $M \equiv s^n$ and $M \equiv e^B$. Again, by definition $M[V/x] = M$.

Case $M \equiv \lambda^n y^C. N$. If $y = x$ then by definition $(\lambda^n y^C. N)[V/x] = \lambda^n y^C. N$ and we are done. If $y \neq x$, the substitution $(\lambda^n y^C. N)[V/x]$ is equal to $\lambda^n y^C. (N[V/x])$. Then by induction hypothesis, $N[V/x] = N$, and thus $M[V/x] = M$.

Cases $M \equiv NP$, $M \equiv \langle N, P \rangle^n$ and $M \equiv \langle \text{let } s = N \text{ in } P \rangle$. By induction hypothesis, $N[V/x] = N$ and $P[V/x] = P$. Using the definition of substitution, $M[V/x] = M$.

Case $M \equiv \langle \text{let } y^C, z^D \rangle^n = N \text{ in } P$. Using $\alpha$-equivalence one can suppose that $y$ and $z$ are not free variables of $V$. Then, if $y = x$ or $z = x$, $M[V/x] = \langle \text{let } y^C, z^D \rangle^n = N[V/x]$ in $P$). By induction hypothesis $N[V/x] = N$ and thus $M[V/x] = M$. If $x \neq y$ and $x \neq z$, $M[V/x] = \langle \text{let } y^C, z^D \rangle^n = N[V/x] \text{ in } P[V/x])$. By induction hypothesis $N[V/x] = N$ and $P[V/x] = P$, thus making $M[V/x] = M$.

Then Lemma 9.1.31 is valid.

Lemma 9.1.32. In Definition [13], if $M$ is a core value, so is $M[V/x]$, and if $M$ is an extended value, so is $M[V/x]$.

Proof. By induction on the structure of $M$ we prove that if $M$ is a core value, so is $M[V/x]$. Base cases:

Cases $M \equiv y^B$. If $y \neq x$, then $M[V/x] = M$, and it is a core value. If $y = x$, then $M[V/x] = \{V <: B\}$, which is a core value from Lemma 9.1.24.

Cases $M \equiv s^n$ and $M \equiv e^B$. In both cases $M[V/x] = M$, already in the form of a core value.

Case $M \equiv \lambda^n y^C. N$. In this situation $M[V/x]$ is of the form $\lambda \ldots$, which is a core value.

Induction case:

Case $M \equiv \langle V_1, V_2 \rangle^n$, with $V_1, V_2$ core values. We have $M[V/x] = \langle V_1[V/x], V_2[V/x] \rangle^n$. By induction hypothesis, $V_1[V/x]$ and $V_2[V/x]$ are core values, making the term $\langle V_1[V/x], V_2[V/x] \rangle^n = M[V/x]$ into a core value.

This exhausts the possibilities. Thus, by structural induction, $M[V/x]$ is a core value is $M$ is. We do the same for extended values, and prove that $M[V/x]$ is an extended value if $M$ is, by structural induction on $M$. The base cases are the same as the base cases for core values, replacing the word “core” by the word “extended”, and remembering that any core value is an extended value. The induction cases go as follows.

Cases $M \equiv \langle V_1, V_2 \rangle^n$ and (let $s = V_1$ in $V_2$). In this case, $V_1$ and $V_2$ are extended values. Write $f(V_1, V_2)$ for $M$. Then we have $M[V/x] = f(V_1[V/x], V_2[V/x])$. By induction hypothesis, $V_1[V/x]$ and $V_2[V/x]$ are extended values, making the term $M[V/x]$ into an extended value.

Case $M \equiv \langle \text{let } y^C = V_1 \text{ in } V_2 \rangle$ (respectively $M \equiv \langle \text{let } y^C, z^D \rangle^n = N \text{ in } P$). We write $f(V_1, V_2)$ in place of $M$. Modulo $\alpha$-equivalence one can assume that $y$ (resp. $y$ and $z$) is not a free variable of $V$. If $y = x$ (resp. $y = x$ or $z = x$) then $M[V/x] = f(V_1[V/x], V_2)$. If $y \neq x$ (resp. $y \neq x$ and $z \neq x$), $M[V/x] = f(V_1[V/x], V_2[V/x])$. By induction hypothesis, $V_1[V/x]$ (and $V_2[V/x]$ in the second case) are extended values. This means that in both cases, $M[V/x]$ is an extended value.

This exhausts the possible cases, and the proof by induction is done: if $M$ is an extended value, so is $M[V/x]$.
9.1. An Indexed Lambda Calculus

Lemma 9.1.33 (Substitution Lemma). Given two valid typing judgements \( \Delta, \Gamma_1 \triangleright V : A \) and \( \Delta, \Gamma_2, x : A \triangleright M : B \) such that \( V \) is a core value and such that \( |\Gamma_1| \cap |\Gamma_2| = \emptyset \), the typing judgement \( \Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] : A \) is valid.

Proof. The proof is done by induction on the size of \( M \).

Case \( M \equiv y^B \). Then the derivation of the typing judgement of \( M \) starts with the rule (ax₁). This implies that \( \Gamma_2 = \Gamma'_2 \) and the typing judgement of \( M \) is \( \Delta, \Gamma'_2, x : A \triangleright y^B : B \).

If \( y = x \), then \( A : B \) and \( M[V/x] = \Delta, \Gamma_1 \triangleright \{V : B\} \) is well-defined. From Lemma 9.1.26 \( \Delta, \Gamma_1 \triangleright M[V/x] : B \) is well-typed. Using Lemma 9.1.19 \( \Delta, \Gamma_1, \Gamma'_2 \triangleright M[V/x] : B \) is valid.

If \( y \neq x \), then \( M[V/x] = y^B \). Since \( \Delta, \Gamma_2, x : A \triangleright y^B : B \) is valid, \( A \) has to be of the form \( !A' \). Then by Lemma 9.1.15 \( \Gamma_1 \) is of the form \( !\Gamma'_1 \). From Lemma 9.1.10 \( \Delta, \Gamma'_1, \Gamma'_2 \triangleright y^B : B \) is valid.

Case \( M \equiv c^B \) (resp. \( M \equiv *^n \)). A derivation of \( M \) starts with rule (ax₂) (resp. rule (T.I)). In both cases the context \( \Gamma_2, x : A \) is duplicable: \( \Gamma_2 = \Gamma'_2 \) and \( A = !A' \). The core value \( V \) is then in fact of type \( !A' \). By Lemma 9.1.15 \( \Gamma_1 \) is of the form \( !\Gamma'_1 \) for some context \( \Gamma'_1 \).

In both cases, the substitution \( M[V/x] \) yields back \( M \). Thus, \( \Delta, \Gamma'_1, \Gamma'_2 \triangleright M[V/x] : B \) is valid by applying the typing rule (ax₂) (resp. (T.I)).

Case \( M \equiv \lambda^n y^C.N \). The typing judgement for the term \( M \) is of the form \( \Delta, \Gamma_1, x : A \triangleright \lambda^n y^C.N : !^n(C \rightarrow D) \), and any typing derivation starts with either \( (\lambda_1) \) or \( (\lambda_2) \) depending on the value \( n \).

In both cases, the judgement \( \Delta, \Gamma_2, x : A, y : C \triangleright N : D \) is valid.

Note that \( x \) cannot be equal to \( y \) in this situation. Using \( \alpha \)-equivalence, one can furthermore choose \( y \) such that it does not belong to \( \Gamma_1 \).

The induction hypothesis can be applied on the judgements \( \Delta, \Gamma_1 \triangleright V : B \) and \( \Delta, \Gamma_2, y : C, x : A \triangleright N : D \), and we get the valid typing judgement

\[
\Delta, \Gamma_1, \Gamma_2, y : C \triangleright N[V/x] : D. \tag{9.1.1}
\]

Note that since \( x \neq y \), the substitution \( (\lambda^n y^C.N)[V/x] = \lambda^n y^C.(N[V/x]) \). There are two cases, depending on \( n \).

If \( n = 0 \), applying \( (\lambda_1) \) on Equation 9.1.1 gives that \( \Delta, \Gamma_1, \Gamma_2 \triangleright (\lambda^0 y^C.N)[V/x] : C \rightarrow D \) is valid.

If \( n \neq 0 \), then \( (\lambda_2) \) is the first rule for the derivation of \( M \), and \( \Gamma_2, x : A \) is of the form \( (\Gamma_3, x : A') \). Since \( A = !A' \) is duplicable and since \( V \) is a core value, by Lemma 9.1.15 the context \( \Gamma_1 \) is of the form \( !\Gamma'_1 \). The rule \( (\lambda_2) \) can then be applied on Equation 9.1.1 to get the valid typing judgement \( \Delta, \Gamma_1, \Gamma_2 \triangleright (\lambda^0 y^C.N)[V/x] : !^n(C \rightarrow D) \).

Cases \( M \equiv N_1 N_2, (N_1, N_2)^n \), (let \( * = N_1 \) in \( N_2 \)) and (let \( (y^C, z^D)^n = N_1 \) in \( N_2 \)).

A typing derivation of \( \Delta, \Gamma_2, x : A \triangleright M : B \) starts with

\[
\begin{array}{c}
\vdots \\
\Delta', \Gamma_2 \triangleright N_1 : B_1 \\
\Delta', \Gamma_2, \Lambda \triangleright N_2 : B_2 \\
\Delta, \Gamma_2, x : A \triangleright f(N_1, N_2) : B \\
\end{array}
\]

where \( (\Delta', \Gamma_{21}, \Gamma_{22}) = (\Delta, \Gamma_1, x : A) \), where \( M = f(N_1, N_2) \), where

<table>
<thead>
<tr>
<th>if ( f(N_1, N_2) ) is...</th>
<th>(X) is...</th>
<th>B is...</th>
<th>( B_1 ) is...</th>
<th>( B_2 ) is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N_1 N_2 )</td>
<td>(app)</td>
<td>( D )</td>
<td>( C \rightarrow D )</td>
<td>( C )</td>
</tr>
<tr>
<td>( \langle N_1, N_2 \rangle^n )</td>
<td>(( \odot ).I)</td>
<td>( !^n(C \odot D) )</td>
<td>( !^n D )</td>
<td></td>
</tr>
<tr>
<td>let ( * = N_1 ) in ( N_2 )</td>
<td>(( \odot ).E)</td>
<td>( D )</td>
<td>( \top )</td>
<td>( D )</td>
</tr>
<tr>
<td>let ( (y^C, z^D)^n = N_1 ) in ( N_2 )</td>
<td></td>
<td>( E )</td>
<td>( !^n(C \odot D) )</td>
<td>( E )</td>
</tr>
</tbody>
</table>
for some types \( C, D \) and \( E \), and where \( \Lambda \) is empty in the three first cases and equal to \( (y : !^m C, z : !^n D) \) in the last case.

By \( \alpha \)-equivalence one can assume that in the last case, the variables \( y \) and \( z \) in \( \Lambda \) does not occur anywhere in the other contexts.

From Lemma 9.1.19 one can assume that \( \Gamma_21 \) and \( \Gamma_22 \) do not contain any duplicable variables, implying that \( |\Delta| \subseteq |\Delta'| \). Thus there exists some context \( !\Psi \) such that \( !\Delta' = (!\Psi, !\Delta) \). In particular, this means that

\[
(\Psi, \Gamma_21, \Gamma_22) = (\Gamma_2, x : A).
\]

This equation is the main result that will allow us to apply the induction hypothesis, and thus finish the proof.

The variable \( x : A \) belongs to either \( !\Psi, \Gamma_21 \) or \( \Gamma_22 \). We study each one of these three possibilities.

\( x \in |!\Psi| \). In this case, \( A = !A' \) and \( !\Psi = (!\Psi', x : !A') \). The contexts \( (\Delta', \Gamma_21) \) and \( (\Delta', \Gamma_22, \Lambda) \) becomes respectively \( (\Psi', !\Delta, \Gamma_21, x : !A') \) and \( (\Psi', !\Delta, \Gamma_22, \Lambda, x : !A') \), meaning that the typing judgements \( !\Psi', !\Delta, \Gamma_21, x : !A' \triangleright N_1 : B_1 \) and \( !\Psi', !\Delta, \Gamma_22, \Lambda, x : !A' \triangleright N_2 : B_2 \) are valid.

Since \( !\Psi = (!\Psi', x : !A') \), Equation xx implies that \( (\Psi', \Gamma_21, \Gamma_22) = \Gamma_2 \). Since \( |\Gamma_1| \cap |\Gamma_2| = \emptyset \), the set \( |\Gamma_1| \) does not intersect \( |\Psi'|, |\Gamma_2|, \Gamma_1[21] \) nor \( |\Gamma_2| \). This means that the typing context \( (\Psi', !\Delta, \Gamma_21, \Gamma_22, \Gamma_1) \) is valid. Together with the fact that \( \Lambda \) does not intersect anything, the requirements on the contexts in the following are satisfied.

By Lemma x, the typing judgement \( !\Psi', !\Delta, \Gamma_1 \triangleright V : !A' \) is valid.

By Lemma x, the context \( \Gamma_1 \) is of the form \( !\Gamma_1 \).

Using the fact that \( f(N_1[V/x], N_2[V/x]) = f(N_1, N_2)[V/x] \) and applying the typing rule (X), one gets that \( !\Psi', !\Delta, \Gamma_21, \Gamma_22, \Gamma_1 \triangleright f(N_1, N_2)[V/x] : B \) is valid. One can rewrite this typing judgement as \( !\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] : B \).

\textbf{Case } \( x \in |\Gamma_21| \) \textbf{ and case } \( x \in |\Gamma_22| \). The two cases are symmetrical (modulo the use of \( \Lambda \), which does not bring any difficulty), by inverting the role of 1 and 2 in the indices. We provide the proof for 2.

The context \( \Gamma_22 \) is of the form \( (\Gamma_22', x : A) \). This means that \( !\Psi, !\Delta, \Gamma_22, \Lambda, x : A \triangleright N_2 : B_2 \) is valid.

Equation xx implies that \( (\Psi, \Gamma_21, \Gamma_22) = \Gamma_2 \). Since \( |\Gamma_1| \cap |\Gamma_2| = \emptyset \), the set \( |\Gamma_1| \) does not intersect \( |\Psi|, |\Gamma_2| \) nor \( |\Gamma_2| \). This means that the typing context \( (\Psi, !\Delta, \Gamma_21, \Gamma_22, \Gamma_1) \) is valid. Together with the fact that \( \Lambda \) does not intersect anything, the requirements on the contexts in the following are satisfied.

By Lemma xx, the typing judgement \( !\Psi, !\Delta, \Gamma_1 \triangleright V : A \) is valid.

By Lemma xx, the context \( \Gamma_1 \) is of the form \( !\Gamma_1 \).

One can apply the induction hypothesis: the judgement \( !\Psi, !\Delta, \Gamma_22, \Lambda, \Gamma_1 \triangleright N_2[V/x] : B_2 \) is valid.

Since \( (\Psi, !\Delta) = !\Delta' \), the typing judgement \( !\Psi, !\Delta, \Gamma_21 \triangleright N_1 : B_1 \) is valid.

Since \( x \in |\Gamma_22| \), \( x \) is not a free variable of \( N_1 \). From Lemma xx, this means that \( f(N_1, N_2)[V/x] = f(N_1, N_2[V/x]) \). (In the case \( x \in |\Gamma_21| \), the substitution \( f(N_1, N_2)[V/x] \) is equal to \( f(N_1[V/x], N_2) \)).

One can then apply the typing rule (X) and get that \( !\Psi', !\Delta, \Gamma_21, \Gamma_22, \Gamma_1 \triangleright f(N_1, N_2)[V/x] : B \) is valid.

By definition, the context of this typing judgement is \( (\Delta, \Gamma_1, \Gamma_2) \). This makes \( !\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] : B \) a valid typing judgement.
9.1. An Indexed Lambda Calculus

Hence, by structural induction on the typing derivation of $!\Delta, \Gamma_2, x : A \triangleright M : B$, Lemma 9.1.33 is valid.

**Lemma 9.1.34.** Suppose that $!\Delta, \Gamma_1 \triangleright V : A$ and $!\Delta, \Gamma_2, x : A \triangleright M : B$ such that $V$ is a core value and such that $|\Gamma_1| \cap |\Gamma_2| = \emptyset$. Suppose moreover that $B < : B'$. Then $\{M[V/x] < : B'\} = \{M < : B'\}[V/x]$. 

**Proof.** By induction on the size of $M$.

*Case $M \equiv x^B$. In this case, the typing judgement $!\Delta, \Gamma_2, x : A \triangleright M : B$ comes from the rule $(ax_1)$, meaning that $A < : B$.*


*Case $M \equiv c^B$, $y^n$ and $y^B$, with $y \neq x$. In these three cases, $M[V/x] = M$ and $\{M < : B'\}[V/x] = \{M < : B'\}$, making the result true by vacuity.*

*Case $M \equiv \lambda^n y^C.N$. By $\alpha$-equivalence one can assume that $y \neq x$. since $M$ is well-typed of type $B$, there exists a type $D$ such that $B = !^m(C \rightarrow D)$. Therefore, $B' = !^m(C' \rightarrow D')$, with $D < : D'$, $C' < : C$ and $m = 0$ if $n = 0$. One has

\[
\{M[V/x] < : B'\} = \{\lambda^n y^C.N[V/x] < : !^m(C' \rightarrow D')\} = \lambda^m y^C'.\{N[V/x] < : D'\}
\]

which is by induction hypothesis $\lambda^m y^C'.\{N < : D'\}[V/x]$. Therefore

\[
\{M[V/x] < : B'\} = \lambda^m y^C'.\{N < : D'\}[V/x] = (\lambda^m y^C'.\{N < : D'\})[V/x] = \{\lambda^m y^C'.N < : !^m(C' \rightarrow D')\}[V/x] = \{M < : B'\}[V/x].
\]

*Case $M \equiv NP$. Since $M$ is of type $B$, there exists a type $C$ such that $N : C \rightarrow B$ and such that $P : C$. We have therefore:

\[
\{M[V/x] < : B'\} = \{(N[V/x])(P[V/x]) < : B'\}
\]

\[
= (N[V/x])\{P[V/x] < : C \rightarrow B'\}
\]

\[
= (N[V/x])\{(P < : C \rightarrow B')\}[V/x]
\]

\[
= (N\{P < : B'\})[V/x]
\]

\[
= \{NP < : B'\}[V/x]
\]

\[
= \{M < : B'\}[V/x].
\]

*Case $M \equiv (let \ (y^C, z^D) = N in P)$. By $\alpha$-equivalence one can assume that $x \neq y, z$. Since $M$ is of type $B$, so in $P$. We have therefore:

\[
\{M[V/x] < : B'\} = \{let \ (y^C, z^D) = N[V/x] in P[V/x] < : B'\}
\]

\[
= let \ (y^C, z^D) = N[V/x] in \{P[V/x] < : B'\}
\]

\[
= let \ (y^C, z^D) = N[V/x] in \{P < : B'\}[V/x]
\]

\[
= \{let \ (y^C, z^D) = N in \{P < : B'\}\}[V/x]
\]

\[
= \{let \ (y^C, z^D) = N in P < : B'\}[V/x]
\]

\[
= \{M < : B'\}[V/x].
\]

The remaining cases are similar.
9.2 Equational Logic of Typed Terms

Definition 9.2.1. We define an equivalence relation on (indexed) typing judgements. We write \( \Delta \vdash M \approx_{ax} M' : A \), or simply \( M \approx_{ax} M' \), to indicate that \( \Delta \vdash M : A \) and \( \Delta \vdash M' : A \) are equivalent. Axiomatic equivalence is defined as the reflexive, symmetric, transitive, and congruence closure of

- the rules from Table 9.2, Table 9.3, so long as both sides of the equivalences are well-typed.
- the following two rules:

  Rule \( \text{app} \). Suppose that \( A <: B \). If \( \Delta = (!\Delta', \Gamma_1, \Gamma_2) \) such that
  \[ !\Delta', \Gamma_1 \triangleright N : B \rightarrow C, \quad !\Delta', \Gamma_2 \triangleright P : A, \]
  then \( \Delta \triangleright N \{P <: B\} \approx_{ax} \{N <: A \rightarrow C\} P : C. \)

  Rule \( \text{let} \). Suppose that \( A <: A', B <: B' \), and \( n' = 0 \) if \( n = 0 \).
  If \( \Delta = (!\Delta', \Gamma_1, \Gamma_2) \) such that
  \[ !\Delta', \Gamma_1 \triangleright N : !n(A \otimes B), \quad !\Delta', \Gamma_2, x : !n'A, y : !n'B' \triangleright P : E, \]
  then
  \[ \Delta \triangleright \left( \text{let} \langle x^{A'}, y^{B'} \rangle^n = \{N <: !n'(A' \otimes B')\} \text{ in } P \right) \approx_{ax} \left( \text{let} \langle x^A = N \text{ in } P \rangle \right) : E. \]

Lemma 9.2.2. Suppose that \( A <: A' \). If \( \Delta = (!\Delta', \Gamma_1, \Gamma_2) \) such that
  \[ !\Delta, \Gamma_1 \triangleright N : A, \quad \Delta', \Gamma_2, x : A' \triangleright P : E, \]
  then
  \[ \Delta \triangleright \left( \text{let} x^{A'} = \{N <: A'\} \text{ in } P \right) \approx_{ax} \left( \text{let} x^A = N \text{ in } P \right) : E. \]

Proof. By definition. \( \square \)

Convention 9.2.3. The rule stated in Lemma 9.2.2 will be referred to using the symbol \( \text{let}_< \).

Lemma 9.2.4. The equivalences of Table 9.4 are derivable.

Proof. By case distinction. \( \square \)

Lemma 9.2.5. Suppose that \( \Delta \vdash M \approx_{ax} M' : A \) and that \( \Delta' <: \Delta \) and \( A <: A' \). Then \( \Delta' \vdash \{M <: A'\} \approx_{ax} \{M' <: A'\} : A' \).

Proof. We have \( \Delta \vdash M : A \) and \( \Delta \vdash M' : A \). From Lemma 9.1.14 \( \Delta' \vdash M : A \) and \( \Delta' \vdash M' : A \) are valid. From Lemma 9.1.26 \( \Delta' \vdash \{M <: A'\} : A' \) and \( \Delta' \vdash \{M' <: A'\} : A' \) are valid. It remains to prove that they are axiomatically equivalent. We prove it by induction on the size of the derivation of \( \Delta \vdash M \approx_{ax} M' : A \).

Base case: \( \beta\eta\)-rules.
(\beta_0) \Delta \triangleright \text{let } x = V \text{ in } M 
\approx_{ax} M[V/x] : A 

(\lambda^{n}x{A}:\{V <: A \rightarrow B\})x^A \n\approx_{ax} V : !^n (A \rightarrow B). 

\Delta' \triangleright \text{let } x^A = N \text{ in } x^A \n\approx_{ax} N : A.

\eta_\lambda \Delta \triangleright \lambda^nx^A,\{V <: A \rightarrow B\}x^A \n\approx_{ax} V : !^n (A \rightarrow B).

\eta_\lambda \Delta \triangleright \text{let } x^A = N \text{ in } \{V<n:T\} \n\approx_{ax} N : !^n T.

Table 9.2: Axiomatic equivalence axioms: beta-eta-rules

(\lambda^{n}x{A}:\{V <: A \rightarrow B\})x^A \n\approx_{ax} V : !^n (A \rightarrow B).

\Delta' \triangleright \text{let } x^A = N \text{ in } x^A \n\approx_{ax} N : A.

\eta_\lambda \Delta \triangleright \lambda^nx^A,\{V <: A \rightarrow B\}x^A \n\approx_{ax} V : !^n (A \rightarrow B).

\eta_\lambda \Delta \triangleright \text{let } x^A = N \text{ in } \{V<n:T\} \n\approx_{ax} N : !^n T.

Table 9.3: Axiomatic equivalence axioms: commutation rules

Case (\beta_0). In this case, M = (let x = V in N) and M' = N[V/x]. From Lemma 9.1.24, \{M <: A'\} = (let x = V in N) \n\approx_{ax} N[V/x] : A'.

Using equivalence rule (\beta_0), \Delta' \triangleright \text{let } x^B = V \text{ in } M \n\approx_{ax} M[V/x] : A'.

Case (\beta_0). We have M = (let x = V in N) and M' = N[V/x, W/y]. From Definition 9.1.24, \{M <: A'\} = (let x = V in N) \n\approx_{ax} N[V/x, W/y] : A'.

Using equivalence rule (\beta_0), \Delta' \triangleright \text{let } x^B = V \text{ in } M \n\approx_{ax} M[V/x, W/y] : A'.

Case (\beta_0). In this case, the term is \text{let } x = V in N and M' = N. From Definition 9.1.20, \{M <: A'\} = (let x = V in N) \n\approx_{ax} N[V/x] : A'.

Using equivalence rule (\beta_0), we obtain the axiomatic equivalence \Delta' \triangleright \text{let } x = V in N \n\approx_{ax} N[V/x] : A'.

Case (\eta_\lambda). In this case, M = \lambda^n x^B \{V <: B \rightarrow C\} x^B, M' = V, A = !^n (B \rightarrow C) and A' = !^n (B' \rightarrow C') with m = 0 if n = 0, C <: C' and B' <: B.

From Definition 9.1.20, \{M <: A'\} = \lambda^n x^B \{\{V <: B \rightarrow C\} x^B <: C\} = \lambda^n x^B \{\{V <: B \rightarrow C\} <: B' \rightarrow C'\} x^B. From Lemma 9.1.22, \{M <: A'\} = \lambda^n x^B \{\{V <: B \rightarrow C\} <: B' \rightarrow C'\} x^B.

We have \Delta' \triangleright !^n (B' \rightarrow C'). Since x \notin \Delta' and since x^B \{x^B <: B\}, by equivalence rule (app_\lambda) and by Definition 9.1.22, we have \Delta', x : B' \rightarrow \{V <: B \rightarrow C'\} x^B \approx_{ax} \{V <: B \rightarrow C'\} x^B : C'.

Thus by congruence \Delta' \triangleright !^n (B' \rightarrow C').

From Lemma 9.1.22, \{V <: B' \rightarrow C'\} = \{V <: !^n (B' \rightarrow C') <: B' \rightarrow C'\}. Using rule (\eta_\lambda), by transitivity we get that \Delta' \triangleright \{M <: !^n (B' \rightarrow C')\} \approx_{ax} \{V <: !^n (B' \rightarrow C')\} : !^n (B' \rightarrow C').

Case (\beta_0). In this case, M = (let x = N in x)x^A and M' = N.

From Definition 9.1.20, \{M <: A'\} = (let x = N in x)x^A. From Lemma 9.1.22, \Delta' \triangleright \{let x^A = N \text{ in } x^A\} \approx_{ax} \{let x^A = N \text{ in } x^A\} : A'. Applying rule (\beta_0), we get that this is equivalent to \Delta' \triangleright \{M <: A'\} \n\approx_{ax} \{M <: A'\} : A'.

Case (\eta_\lambda). In this case, M = (let x = N in x)x^A and M' = N. We also have
(\alpha_{let}) \Delta, y : A \triangleright M : B \approx_{ax} \Delta, x : A \triangleright let \ y^A = x^A \ in M : B

(\lambda x) !\Delta \triangleright let \ x^{\lambda C} = V in \lambda y. M \approx_{ax} \lambda^{n+1} y. let \ x^C = V in M : !n+1(A \rightarrow B)

(\eta_\Pi) \Delta \triangleright \langle V, let \ \Box = M in N \rangle \approx_{ax} let \ \Box = M in (V, N) : !n(A \land B)

(\eta_\iota) \Delta \triangleright \langle let \ \Box = M in N, V \rangle \approx_{ax} let \ \Box = M in (N, V) : !n(A \land B)

(\eta_{app2}) \Delta \triangleright \langle let \ \Box = M in N, V \rangle \approx_{ax} let \ \Box = M in NV : B

(\eta_{app1}) \Delta \triangleright \langle let \ \Box = M in N \rangle \approx_{ax} let \ \Box = M in NV : B

Table 9.4: Axiomatic equivalence: derived rules

\( A = !^m(B \land C), \text{ and since } A <: A', A' = !^m(B' \land C') \text{ with } m = 0 \text{ if } n = 0, \text{ with } B <: B' \text{ and with } C <: C'. \)

From Definition 9.20 \( \{M <: A'\} = \{let \ (x^B, y^C)^m = N in (x^{imB'}, y^{imC'})^m\}. \) From equivalence rule (\( \eta_{\iota} \)),

\[ \Delta' \triangleright let \ (x^B, y^C)^m = N in (x^{imB'}, y^{imC'}) \approx_{ax} let \ (x^B, y^C)^m = \{N <: !^m(B' \land C')\} in (x^{imB'}, y^{imC'})^n : A'. \]

Applying rule (\( \eta_{\eta} \)), we get that this is equivalent to \( \Delta' \triangleright \{N <: A'\} : A' \)

Case (\( \eta_{\eta} \)). In this case, \( M = \{let * = \{N <: \top\} \ in *^m\}, M' = N \ and \ A = !^m \top. \) Since \( A <: A', A' = !^m \top \text{ with } m = 0 \text{ if } n = 0. \)

From Definition 9.20 \( \{N <: \top\} = \{\{N <: !^m \top\} <: \top\}. \)

From Lemma 9.22 \( \{\{N <: !^m \top\} <: \top\} \ in *^m \approx_{ax} \{N <: !^m \top\}. \)

And this prove the lemma for the \( \beta-\eta \)-rules of Table 9.2

Next base cases: commutation rules.

Case (\( \alpha_{let} \)). Here, \( M = \{let \ -1 = (let \ -2 = N_2 in N_1) \ in P\} \) and \( M' = \{let \ -2 = N_2 in let \ -1 = N_1 \ in P\}. \)

Using Definition 9.20 \( \{M <: A'\} = \{let \ -1 = (let \ -2 = N_2 in N_1) \ in \{P <: A'\}\} \) and \( \{M' <: A'\} = \{let \ -2 = N_2 in let \ -1 = N_1 \ in \{P <: A'\}\}. \) Using equivalence rule (\( \alpha_{let} \)), we find that \( \Delta' \triangleright \{M <: A'\} \approx_{ax} \{M' <: A'\} : A'. \)

Case (\( \eta_{\iota} \)). This case is similar to the previous one. Here, \( M = \{let \ -1 = V \ in let \ -2 = W \ in N\} \) and \( M' = \{let \ -2 = W \ in let \ -1 = V \ in N\}. \)

Using Definition 9.20 \( \{M <: A'\} = \{let \ -1 = V \ in let \ -2 = W \ in \{N <: A'\}\} \) and \( \{M' <: A'\} = \{let \ -2 = W \ in let \ -1 = V \ in \{N <: A'\}\}. \) Using equivalence rule (\( \eta_{\iota} \)), we find that \( \Delta' \triangleright \{M <: A'\} \approx_{ax} \{M' <: A'\} : A'. \)

Case (\( \alpha_{app1} \)). Here, \( M = \{let \ x^{B \rightarrow A} = N \ in let \ y^B = P \ in (x^{B \rightarrow A} y^B)\} \) and \( M' = NP. \) Using Definition 9.20 \( \{M <: A'\} = \{let \ x^{B \rightarrow A} = N \ in let \ y^B = P \ in (x^{B \rightarrow A} y^B)\}. \) From Lemma 9.20

\[ \Delta' \triangleright let \ x^{B \rightarrow A} = N \ in let \ y^B = P \ in (x^{B \rightarrow A} y^B) \approx_{ax} let \ x^{B \rightarrow A'} = \{N <: B \rightarrow A'\} \ in let \ y^B = P \ in (x^{B \rightarrow A'} y^B) : A'. \]
9.2. Equational Logic of Typed Terms

Rule (let$^{GP}$) says that this is equivalent to $\Delta \triangleright \{N < ; B \rightarrow A'\} : A$. The result is obtained by using Definition 9.1.20: $\{M' < : A'\} = \{N < ; B \rightarrow A'\}$. 

Case (let$^\Delta$). In this case, $M = (let \; x^D = V \; in \; \lambda^n y^B.N)$, $M' = \lambda^n y^B.(let \; x^D = V \; in \; N)$, $A = V^n(B \rightarrow C)$ and $A' = \lambda^n(B' \rightarrow C')$ with $m = 0$ if $n = 0$, $C < : C'$ and $B' < : B$.

Using Definition 9.1.20: $\{M < : A'\} = (let \; x^D = V \; in \; \lambda^m y^B.N \langle N < ; C'\rangle)$ and $\{M' < : A'\} = \lambda^m y^B.(let \; x^D = V \; in \; \{N < ; C'\})$.

Using equivalence rule (let$^\Delta$), we have as required that $\Delta' \triangleright \{M < : A'\} \approx_{ax} \{M' < : A'\} : A'$.

Case (let$^{\ominus}$). In this situation, $M = (let \; x^m B = N \; let \; y^n C = P \ominus(x^m B, y^n C)^m)$, $M' = (N, P)^m$, $A = N^m(B \otimes C)$ and $A' = !^m(B' \otimes C')$ with $m = 0$ if $n = 0$, $C < : C'$ and $B < : B'$.

Using Definition 9.1.20: $\{M < : A'\} = (let \; x^m B = N \; in \; \lambda^m y^n C = P \ominus(x^m B', y^n C')^m)$ and $\{M' < : A'\} = \{N < ; !^m C\}, \{P < ; !^m D\})^m$.

Using twice Lemma 9.1.22 we get that $\Delta' \triangleright \{M < : A'\} \approx_{ax} (let \; x^m B' = N < ; !^m B')$ in $\{M' < : A'\} : C'$.

Applying (let$^{\ominus}$) and transitivity gives the required result.

Rules concerning typecasting. For these two rules, we use in each case the notation of Definition 9.1.23.

In both cases, we have $\Delta \triangleright M \approx_{ax} M' : C$. We want to show that if $\Delta' \triangleright \Delta$ and $C < : C'$ then $\Delta' \triangleright \{M < : C'\} \approx_{ax} \{M' < : C'\} : C'$.

The fact that $\Delta' \triangleright \{M < : C'\} : C'$ and that $\Delta' \triangleright \{M' < : C'\} : C'$ is proved using Lemma 9.1.13 and 9.1.24.

The fact that they are axiomerically equivalent is proved as follows.

Case (app$_{\ominus}$). We have $M = N(P < ; B)$ and $M' = (N < ; A \rightarrow C)P$.

Consider $\{M < : C'\}$. From Definition 9.1.20, it is equal to $\{N < ; B \rightarrow C'\}(P < ; B)$.

Using rule (app$_{\ominus}$), we infer that $\Delta \triangleright \{M < : C'\} \approx_{ax} \{N < ; B \rightarrow C'\} : (A \rightarrow C')P : C'$.

Using Lemma 9.1.22 we deduce that $\Delta' \triangleright \{N < ; A \rightarrow C'\} : C'$. We conclude by noticing that from Definition 9.1.23: $\{M' < : C'\} = \{N < ; A \rightarrow C'\}$.

Case (let$^\ominus$). Here, $M = (let \; (x^A, y^B)^n = (N < ; !^n (A' \otimes B')) \; in \; P)$ and $M' = (let \; (x^A, y^B)^n = (N in \; P))$.

The term $\{M < : C'\}$ is equal to let $(x^A, y^B)^n = \{N < ; !^n (A' \otimes B')\}$ in $\{P < ; C'\}$ by Definition 9.1.24. The term $\{M' < : C'\}$ is equal from the same definition to the term $let \; (x^A, y^B)^n = N in \{P < ; C'\}$.

They are axiomerically equivalent because of the equivalence rule (let$^\ominus$).

And this ends the base cases.

Rules specific to equivalence relations. The reflexivity, the symmetry, the transitivity are trivial.

Reflexivity. In this case, $M = M'$. Therefore $\{M < : A'\} = \{M' < : A'\}$. One has that $\Delta' \triangleright \{M' < : A'\} = \{M < : A'\}$ by reflexivity.

Symmetry. Here, $\Delta \triangleright M \approx_{ax} M' : A'$ was proved by first proving $\Delta \triangleright M' \approx_{ax} M : A'$. By induction hypothesis, we conclude that $\Delta' \triangleright \{M' < : A'\} \approx_{ax} \{M < : A'\} : A'$. We then apply again symmetry.

Transitivity. Here, $\Delta \triangleright M \approx_{ax} M' : A'$ was proved introducing a third term $M''$ such that $\Delta \triangleright M \approx_{ax} M'' : A$ and $\Delta \triangleright M'' \approx_{ax} M' : A$. By induction hypothesis, this means that $\Delta' \triangleright \{M < : A'\} \approx_{ax} \{M'' < : A'\} : A'$ and $\Delta \triangleright \{M'' < : A'\} \approx_{ax} \{M' < : A'\} : A'$. We can then apply transitivity to get the result.
9.2. Equational Logic of Typed Terms

Confluence rules. There is one confluence rule per term constructor. We list the cases in the following.

Case $M \equiv \lambda^n x^C. N$. Then $M' \equiv \lambda^n x^C. N'$, the type $A$ is of the form $!^n (C \rightarrow D)$ and the type $A'$ is of the form $!^n (C \rightarrow D) \equiv 0$. We have $\Delta, x : C \vdash N \approx_{ax} N' : D$, and $\Delta$ is of the form $!^n \Delta$ if $n \neq 0$.

By induction hypothesis, $\Delta', x : C \vdash \{N < A : D'\} \approx_{ax} \{N' < A' : D'\} : D'$. It is then possible to apply the confluence rule for $(\lambda_1)$ to get the result.

Cases $M \equiv N_1 N_2$, $(N_1, N_2)^n$, (let $* = N_1$ in $N_2$) and (let $(y^C, z^D)^n = N_1$ in $N_2$).

In each case we use the shortcut notation $f(N_1, N_2)$ in place of the corresponding construct. Then $M' \equiv f(N_1', N_2')$ for some terms $N_1'$ and $N_2'$, and the typing judgements $\Delta \vdash M, M' : A$ comes from

$!^n \Delta, \Gamma_1 \vdash N_1 : B_1$, $!^n \Delta, \Gamma_1 \vdash N_1' : B_1$,

$!^n \Delta, \Gamma_2 \vdash N_2 : B_2$, $!^n \Delta, \Gamma_2 \vdash N_2' : B_2$, $!^n \Delta, \Gamma_1 \vdash N_1 : B_1$, $!^n \Delta, \Gamma_1 \vdash N_1' : B_1$,

and from the application of a typing rule $(X)$, where $\Delta = (\Delta_1 \Delta_2)$, and where

$\begin{array}{c|c|c|c|c|c}
N_1 N_2 & (\text{app}) & D & C \rightarrow D & C \\
(N_1, N_2)^n & (\otimes.1) & !^n (C \otimes D) & !^n C & !^n D \\
\text{let } * = N_1 \text{ in } N_2 & (\top.E) & D & \top & D \\
\text{let } (y^C, z^D)^n = N_1 \text{ in } N_2 & (\otimes.E) & E & !^n (C \otimes D) & E \\
\end{array}$

for some types $C$, $D$ and $E$, and where $\Lambda$ is empty in the three first cases and equal to $(y : !^n C, z : !^n D)$ in the last case. By $\alpha$-equivalence one can assume that in the last case, the variables $y$ and $z$ in $\Lambda$ does not occur anywhere in the other contexts.

The type $A'$ is such that $A \ll A'$. Its structure is then governed by the one of $A$. Let us construct $B_1'$ and $B_2'$ as follows:

$\begin{array}{c|c|c|c|c}
N_1 N_2 & D' & C \rightarrow D' & C \\
(N_1, N_2)^n & !^m (C' \otimes Dm) & !^m C' & !^m D' \\
\text{let } * = N_1 \text{ in } N_2 & D' & \top & D' \\
\text{let } (y^C, z^D)^n = N_1 \text{ in } N_2 & E' & !^n (C \otimes D) & E' \\
\end{array}$

for some types $C'$, $D'$ and $E'$ such that $C \ll C'$, $D \ll D'$ and $E \ll E'$. Note that in each case, $B_1 < B_1'$ and $B_2 < B_2'$. One can therefore apply the induction hypothesis, and get that

$!^n \Delta', \Gamma_1' \vdash \{N_1 < A' \} : B_1'$,

$!^n \Delta', \Gamma_2' \vdash \{N_2 < A' \} : B_2'$,

$!^n \Delta', \Gamma_1' \vdash \{N_1' < B_1' \} : B_1'$,

$!^n \Delta', \Gamma_2' \vdash \{N_2' < B_2' \} : B_2'$,

are valid, where $\Delta' = (\Delta_1', \Gamma_1')$, where $\{N_1 \} < A$ and $\{N_2 \} < A$ and $\{N_1 \} < A$ and $\{N_2 \} < A$.

One can apply the confluence rule for $(X)$ and get that

$\Delta' \vdash \{N_1 < B_1' \} \approx_{ax} \{N_1' < B_1' \} \approx_{ax} \{N_2 < B_2' \} : A'$.

Using Definition 9.1.20 and Lemma 9.1.28 this means that $\Delta' \vdash \{M < A' \} : A'$.

and this closes the list of possible cases. □
9.3. The Category $C_{\lambda}$

Lemma 9.2.6. If $!\Delta, \Gamma_1, x : A \triangleright M : B$ is a valid typing judgement, and if $!\Delta, \Gamma_2 \triangleright V \approx_{ax} V' : A$ are axiomatically equivalent core values such that $|\Gamma_1| \cap |\Gamma_2| = \emptyset$, then $!\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] \approx_{ax} M[V'/x] : B$ are axiomatically equivalent typing judgements.

Proof. First note that $!\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] : B$ and $!\Delta, \Gamma_1, \Gamma_2 \triangleright M[V'/x] : B$ are axiomatically equivalent typing judgements.

Cases $M \equiv g^C, c^C$ and $*^n$. In these cases, either $M[V/x] = M$ and $M[V'/x] = M$ or $M[V/x] = \{V : A <: C\}$ and $M[V'/x] = \{V' : A <: C\}$. In the former case we have axiomatic equivalence be reflexivity of the relation and in the latter case we have it using Lemma 9.1.33.

Case $M \equiv \lambda^n y^C.N$. Note that since $!\Delta, \Gamma_1, x : A \triangleright M : B$ is well-typed, we have $x \neq y$ and $B = n^n(C \rightarrow D)$ for some type $D$. In particular, $M[V/x] = \lambda^n y^C.(N[V/x])$ and $M[V'/x] = \lambda^n y^C.(N[V'/x]).$

The typing tree of the typing judgement starts with typing rule $(\lambda_i)$ and has for hypothesis $!\Delta, \Gamma_1, x : A, y : C \triangleright N : D$. The integer $i = 1$ if $n = 0$, otherwise $i = 2$. In the latter, $(\Gamma_1, x : A)$ is of the form $(\Gamma_1, x : !A)$.

By induction hypothesis, $!\Delta, \Gamma_1, y : C \triangleright N[V/x] \approx_{ax} N[V'/x] : D$. Applying congruence, we get the result.

The remaining cases are done similarly.

The following result stipulates that all the indexations of a given erasure live in the same axiomatic class. In other words, the axiomatic equivalence class of a term is independent of its indexation.

Theorem 9.2.7. If $\text{Erase}(M) = \text{Erase}(M')$ and if $\Delta \triangleright M, M' : A$ are valid typing judgements, then $M \approx_{ax} M'$.

The proof of Theorem 9.2.7 requires some machinery that we develop in Chapter 10.

9.3 The Category $C_{\lambda}$

The language of Section 9.1 together with its axiomatic equivalence can be made into a syntactic category.

Lemma 9.3.1. We can define a category as follows: Objects are types, and arrows $A \rightarrow B$ are axiomatic classes of valid typing judgements of the form $x : A \triangleright V : B$, where $V$ is an extended value. We define the composition of arrows $x : A \triangleright V : B$ and $y : B \triangleright W : C$ to be $x : A \triangleright let y = V in W : C$. The identity on $A$ is set to be the arrow $x : A \triangleright x : A$.

Proof. The composition of two arrows yields an arrow axiomatically equivalent to a value due to Axiom $(\beta_\lambda)$ and Lemmas 9.1.32 and 9.1.33. Composition is associative due to Axiom $(\text{let}_1)$. The arrow $x : A \triangleright x : A$ is indeed the identity on $A$ due to axioms $(\alpha_{let})$ and $(\beta_\lambda^2)$.

Definition 9.3.2. The category described in Lemma 9.3.1 will be referred as $C_{\lambda}$.
9.3. The Category $C_\lambda$

9.3.1 Monoidal Structure

**Lemma 9.3.3.** If we equip $C_\lambda$ with the arrows

$$
\alpha_{A,B,C} = x : A \otimes (B \otimes C) \triangleright \text{let} \langle y, z \rangle = x \text{ in } \langle t, u \rangle = z \text{ in } \langle y, t, u \rangle : (A \otimes B) \otimes C,
$$

$$
\lambda_A = x : \top \otimes A \triangleright \text{let} \langle y, z \rangle = x \text{ in } \text{let } * = y \text{ in } z : A,
$$

$$
\rho_A = x : A \otimes \top \triangleright \text{let} \langle y, z \rangle = x \text{ in } \text{let } * = z \text{ in } y : A,
$$

$$
\sigma_{A,B} = x : A \otimes B \triangleright \text{let} \langle y, z \rangle = x \text{ in } \langle z, y \rangle : B \otimes A,
$$

and with the arrows $(x : A \triangleright V : B) \otimes (y : C \triangleright W : D) = z : A \otimes B \triangleright \text{let} \langle x, y \rangle = z \text{ in } \langle V, W \rangle : C \otimes D$, then $(C_\lambda, \otimes, \top)$ is a symmetric monoidal category.

Proof. We need to show that $\alpha$, $\lambda$, $\rho$ and $\sigma$ are isomorphic natural transformations, that they satisfy Equations (2.7.1), (2.7.2), (2.7.3), (2.7.4), (2.7.5) and (2.7.6), and that the constructor $\otimes$ is a bifunctor.

Isomorphisms. Let’s show that $\alpha$, $\lambda$, $\rho$ and $\sigma$ are isomorphisms. It is sufficient to exhibit their inverse:

$$
\alpha_{A,B,C}^{-1} = x' : (A \otimes B) \otimes C \triangleright \text{let} \langle y', z' \rangle = x' \text{ in } \text{let} \langle t', u' \rangle = y' \text{ in } \langle t', (u', z') \rangle : A \otimes (B \otimes C),
$$

$$
\lambda_A^{-1} = x' : A \triangleright \langle *, x' \rangle : \top \otimes A,
$$

$$
\rho_A = x' : A \triangleright \langle x', * \rangle : A \otimes \top,
$$

$$
\sigma_{A,B} = x' : B \otimes A \triangleright \text{let} \langle y', z' \rangle = x' \text{ in } \langle z', y' \rangle : A \otimes B,
$$

Naturality of $\alpha$, $\lambda$, $\rho$ and $\sigma$. Let’s consider $\lambda$. Let $f = a : A \triangleright V : A'$ be any arrow $A \rightarrow A'$. We need to show that the diagram

$$
\begin{array}{ccc}
\top \otimes A & \xrightarrow{\lambda_A} & A \\
\downarrow f & & \downarrow f \\
\top \otimes A & \xrightarrow{\lambda_{A'}} & A'
\end{array}
$$

commutes, i.e. $\lambda_A f = (\top \otimes f) \lambda_{A'}$. The arrow $\top \otimes f$ is $b : \top \otimes A \triangleright \text{let} \langle t, a \rangle = b \triangleright \langle t, V \rangle : \top \otimes A'$. So the left hand side of the equation is

$$
b : \top \otimes A \triangleright \text{let } x = (\text{let } \langle t, a \rangle = b \triangleright \langle t, V \rangle ) \text{ in } \langle y, z \rangle = x \text{ in } \text{let } * = y \text{ in } z \\
\approx_{ax} \text{let } \langle t, a \rangle = b \triangleright \langle t, V \rangle \text{ in } \langle y, z \rangle = x \text{ in } \text{let } * = y \text{ in } z \text{ by (let}_1\rangle
$$

$$
\approx_{ax} \text{let } \langle t, a \rangle = b \triangleright \langle t, V \rangle \text{ in } \langle y, z \rangle = \langle t, V \rangle \text{ in } \text{let } * = y \text{ in } z \text{ by (let}_\delta\rangle
$$

The right hand side of the equation is

$$
x : \top \otimes A \triangleright \text{let } a = (\text{let } \langle y, z \rangle = x \text{ in let } * = y \text{ in } z ) \text{ in } V \\
\approx_{ax} \text{let } \langle y, z \rangle = x \text{ in let } * = y \text{ in let } a = z \text{ in } V : A' \text{ by (let}_1\rangle
$$

$$
\approx_{ax} \text{let } \langle y, a \rangle = x \text{ in let } * = y \text{ in } V : A' \text{ by (ax)}
$$
9.3. The Category $C_\lambda$

Both side are then alpha equivalent, which proves that $\lambda$ is a natural transformation.

The proof of naturality of $\rho$ is exactly similar.

For $\sigma_{A,B}$, consider two arrows $f = a : A \triangleright V : A'$ and $g = b : B \triangleright W : B'$. We aim to show that

\[
\begin{array}{ccc}
A \otimes B & \xrightarrow{\sigma_{A,B}} & B \otimes A \\
\downarrow{f \otimes g} & & \downarrow{g \otimes f} \\
A' \otimes B' & \xrightarrow{\sigma'_{A',B'}} & B' \otimes A'
\end{array}
\]

commutes, i.e. $\sigma_{A,B}; (g \otimes f) = (f \otimes g); \sigma'_{A',B'}$. The left hand side is the arrow:

\[
x : A \otimes B \triangleright \text{let } c = (\text{let } (y,z) = x \text{ in } (z,y)) \text{ in } \\
\text{let } (b,a) = c \text{ in } \langle W, V \rangle \\
\approx_{\alpha x} \text{let } (y,z) = x \text{ in } \langle W, V \rangle
\]

which is axiomatically equivalent to the left hand side.

To prove the naturality of $\alpha$, let’s choose three functions $f = a : A \triangleright V : A'$, $g = b : B \triangleright W : B'$ and $h : C \triangleright U : C'$. It is enough to show that

\[
\begin{array}{ccc}
A \otimes (B \otimes C) & \xrightarrow{\alpha_{A,B,C}} & (A \otimes B) \otimes C \\
\downarrow{f \otimes (g \otimes h)} & & \downarrow{(f \otimes g) \otimes h} \\
A' \otimes (B' \otimes C') & \xrightarrow{\alpha'_{A',B',C'}} & (A' \otimes B') \otimes C'
\end{array}
\]

commutes, i.e. that $\alpha_{A,B,C}; ((f \otimes g) \otimes h) = (f \otimes (g \otimes h)) ; \alpha'_{A',B',C'}$.

Let’s write down the components of this equation:

\[
f \otimes g = d : A \otimes B \triangleright \text{let } (a,b) = d \text{ in } \langle V, W \rangle : A' \otimes B' \\
g \otimes h = i : B \otimes C \triangleright \text{let } (b,c) = i \text{ in } \langle W, U \rangle : B' \otimes C'
\]

Then

\[(f \otimes g) \otimes h \quad e : (A \otimes B) \otimes C \triangleright \]
9.3. The Category $C_\lambda$

\[
\text{let } \langle d, c \rangle = e \text{ in } \left\{ \begin{array}{l}
\text{let } \langle a, b \rangle = d \text{ in } \langle V, W \rangle, \quad U \\
\end{array} \right. \\
\approx_{ax} \text{let } \langle d, c \rangle = e \text{ in } \text{let } \langle a, b \rangle = d \text{ in } \langle V, W \rangle, U : (A' \otimes B') \otimes C' \\
\text{by (let}_2^\otimes) \\
\]

\[
f \otimes (g \otimes h) \quad j : A \otimes (B \otimes C) \triangleleft \\
\text{let } \langle a, i \rangle = j \text{ in } \left\{ \begin{array}{l}
V, \text{ let } \langle b, c \rangle = i \text{ in } \\
\end{array} \right. \\
\approx_{ax} \text{let } \langle a, i \rangle = j \text{ in } \text{let } \langle b, c \rangle = i \text{ in } \langle V, (W, U) \rangle : (A' \otimes (B' \otimes C')) \\
\text{by (let}_1^\otimes). \\
\]

Finally,

\[
\alpha_{A, B, C} = \quad x : A \otimes (B \otimes C) \triangleleft \text{let } \langle x_1, x_2 \rangle = x \text{ in } \\
\text{let } \langle x_3, x_4 \rangle = x_2 \text{ in } \\
\langle (x_1, x_3), x_4 \rangle : (A \otimes B) \otimes C \\
\alpha_{A', B', C'} = \quad y : A' \otimes (B' \otimes C') \triangleleft \text{let } \langle y_1, y_2 \rangle = y \text{ in } \\
\text{let } \langle y_3, y_4 \rangle = y_2 \text{ in } \\
\langle (y_1, y_3), y_4 \rangle : (A' \otimes B') \otimes C' \\
\]

Now let’s consider the left hand side of the equation:

\[
x : A \otimes (B \otimes C) \triangleleft \text{let } e = \left( \begin{array}{l}
\text{let } \langle x_1, x_2 \rangle = x \text{ in } \\
\text{let } \langle x_3, x_4 \rangle = x_2 \text{ in } \\
\langle (x_1, x_3), x_4 \rangle \\
\end{array} \right) \text{ in } \\
\text{let } \langle d, c \rangle = e \text{ in } \\
\text{let } \langle a, b \rangle = d \text{ in } \langle (V, W), U \rangle \\
\approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \text{let } (x_3, x_4) = x_2 \text{ in } \\
\text{let } e = (\langle x_1, x_3 \rangle, x_4) \text{ in } \\
\text{let } \langle d, c \rangle = e \text{ in } \\
\text{let } \langle a, b \rangle = d \text{ in } \langle (V, W), U \rangle \\
\approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \text{let } (x_3, x_4) = x_2 \text{ in } \\
\text{let } \langle d, c \rangle = (\langle x_1, x_3 \rangle, x_4) \text{ in } \\
\text{let } \langle a, b \rangle = d \text{ in } \langle (V, W), U \rangle \text{ by (let}_1) \\
\approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \text{let } (x_3, x_4) = x_2 \text{ in } \\
\text{let } \langle d, c \rangle = \langle x_1, x_3 \rangle \text{ in } \langle (V, W), U \rangle \text{ by (\beta_\lambda)} \\
\approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \text{let } (x_3, x_4) = x_2 \text{ in } \\
\text{let } \langle a, b \rangle = \langle x_1, x_3 \rangle \text{ in } \langle (V, W), U \rangle [x_4/c] \text{ by (\beta_\circ)} \\
\approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \text{let } (x_3, x_4) = x_2 \text{ in } \\
\langle (V, W), U \rangle [x_1/a, x_3/b, x_4/c] \text{ by (\beta_\circ)} \\
\approx_{ax} \text{let } \langle a, x_2 \rangle = x \text{ in } \text{let } \langle b, c \rangle = x_2 \text{ in } \\
\langle (V, W), U \rangle : (A' \otimes B') \otimes C' \text{ by (a_{let}).} \\
\]

9.3. The Category $C_\lambda$

The right hand side is

$$j : A \otimes (B \otimes C) \triangleright \text{ let } y = \left( \begin{array}{l} \text{ let } (a, i) = j \text{ in } \\ \langle V, \langle W, U \rangle \rangle \\ \text{ let } (y_1, y_2) = y \text{ in } \\ \text{ let } (y_3, y_4) = y_2 \text{ in } \langle \langle y_1, y_3 \rangle, y_4 \rangle \end{array} \right) \triangleright \text{ let } \langle a, i \rangle = j \text{ in let } \langle b, c \rangle = i \text{ in } \langle \langle y_1, y_3 \rangle, y_4 \rangle$$

which is axiomatically equivalent to the left hand side. Thus $\alpha$ is a natural transformation.

Bifunctoriality of $\otimes$. First we need to show that $\otimes$ is well defined on equivalence classes. Given $x : A \triangleright V \equiv_{ax} V' : B$ and $x : C \triangleright W \equiv_{ax} W' : D$:

$$z : A \otimes C \triangleright \text{ let } \langle x, y \rangle = z \text{ in } \langle V, W \rangle \equiv_{ax} \text{ let } \langle x, y \rangle = z \text{ in } \langle V', W' \rangle : B \otimes D$$

since $\langle V, W \rangle \equiv_{ax} \langle V', W' \rangle$.

Then we need to show that $(- \otimes B)$ and $(A \otimes -)$ are functors, and that they verify

$$(f \otimes B)\langle A' \otimes g \rangle = (A \otimes g)\langle f \otimes B' \rangle$$

for every $f : A \rightarrow A'$ and every $g : B \rightarrow B'$.

$(id_A \otimes id_B)$ is $(x : A \triangleright x : A) \otimes (y : B \triangleright y : B)$, which is by definition $z : A \otimes B \triangleright \text{ let } \langle x, y \rangle = z \text{ in } \langle x, y \rangle : A \otimes B$, which is by Rule (8) the identity $z : A \otimes B \triangleright z : A \otimes B$. So both $(- \otimes B)$ and $(A \otimes -)$ preserves identities.

Let $f$ be $x : A \triangleright V : A'$ and $f'$ be $y : A' \triangleright W : A''$. $((f, f') \otimes B)$ is

$$z : A \otimes B \triangleright \text{ let } \langle x, t \rangle = z \text{ in } \langle y, V \text{ in } W, t \rangle \equiv_{ax} \text{ let } \langle x, t \rangle = z \text{ in let } \langle y, V \text{ in } W, t \rangle \text{ by (let}$2\text{).}$$

On another hand, $(f \otimes B); (f' \otimes B)$ is

$$z : A \otimes B \triangleright \text{ let } \langle x, t \rangle = z \text{ in } \langle V, t \rangle \text{ in }
\text{ let } \langle y, v \rangle = u \text{ in } \langle W, v \rangle \equiv_{ax} \text{ let } \langle x, t \rangle = z \text{ in let } \langle y, v \rangle = \langle V, t \rangle \text{ in } \langle W, v \rangle \text{ by (let}$1\text{).}$$

$$z : A \otimes B \triangleright \text{ let } \langle x, t \rangle = z \text{ in let } y = \langle V, t \rangle \text{ in } \text{ let } \langle y, v \rangle = u \text{ in } \langle W, v \rangle \equiv_{ax} \text{ let } \langle x, t \rangle = z \text{ in let } y = \langle V, t \rangle \text{ in } \langle W, v \rangle \text{ by (let}$1\text{).}$$

$$z : A \otimes B \triangleright \text{ let } \langle x, t \rangle = z \text{ in let } y = \langle V, t \rangle \text{ in } \text{ let } \langle y, v \rangle = u \text{ in } \langle W, v \rangle \equiv_{ax} \text{ let } \langle x, t \rangle = z \text{ in let } y = \langle V, t \rangle \text{ in } \langle W, v \rangle \text{ by (let}$1\text{).}$$
9.3. The Category $C_{\lambda}$

\[
\text{let } v = t \text{ in } (W, v)
\]

\[
\approx_{ax} \text{let } (x, t) = z \text{ in let } y = V \text{ in } (W, t)
\]

by \((\beta_\circ), (\beta_\lambda)\)

and thus the two morphisms are equals.

Using \((\text{let}_1^\circ)\) in place of \((\text{let}_2^\circ)\), we can show that \((A \otimes (g' \circ g)) = (A \otimes g); (A \otimes g')\), for \(g : B \to B'\) and \(g' : B' \to B''\).

Finally, we must show that if \(f = A \triangleright V : A'\) and \(g = B \triangleright U : B'\), then \((f \otimes B); (A' \otimes g) = (A \otimes g); (f \otimes B')\).

The left hand side is

\[
z: A \otimes B \triangleright \text{let } z' = (\text{let}(x, t) = z \text{ in } V, t) \text{in}
\]

\[
\approx_{ax} \text{let } (x, t) = z \text{ in let } z' = (V, t) \text{ in}
\]

\[
\approx_{ax} \text{let } (x, t) = z \text{ in let } u = V \text{ in}
\]

\[
\approx_{ax} \text{let } (x, y) = z \text{ in } (V, W)
\]

by \((\text{let}_1), (\beta_\circ), (\beta_\lambda)\), \((\beta_\lambda)\) and \((\alpha_{let})\), this is axiomatically equivalent to \(\text{let}(x, y) = z \text{ in } (V, W)\). Thus the required equality hold, and \(\otimes\) is bifunctorial.

**Commutative diagrams.** We need to verify Equations 2.7.1, 2.7.2, 2.7.3, 2.7.4, 2.7.5, and Equation 2.7.6.

**Equations 2.7.1.** We want to prove that

\[
\alpha_{A,B,C,D}; \alpha_{A \otimes B,C,D} = (id_A \otimes \alpha_{B,C,D}); \alpha_{A,B \otimes C} \otimes id_D.
\]

For the left hand side, the components are as follows:

\[
\alpha_{A,B,C,D} = x:\ A \otimes (B \otimes (C \otimes D)) \triangleright \text{let } (x_1, x_2) = x \text{ in}
\]

\[
\text{let } (x_3, x_4) = x_2 \text{ in}
\]

\[
\langle (x_1, x_3), x_4 \rangle : (A \otimes B) \otimes (C \otimes D),
\]

\[
\alpha_{A \otimes B,C,D} = y : (A \otimes B) \otimes (C \otimes D) \triangleright \text{let } (y_1, y_2) = y \text{ in}
\]

\[
\text{let } (y_3, y_4) = y_2 \text{ in}
\]

\[
\langle (y_1, y_3), y_4 \rangle : ((A \otimes B) \otimes C) \otimes D).
\]

Then

\[
\alpha_{A,B,C,D}; \alpha_{A \otimes B,C,D} = x : A \otimes (B \otimes (C \otimes D)) \triangleright
\]

\[
\text{let } y = \begin{pmatrix}
\text{let } (x_1, x_2) = x \text{ in } \\
\text{let } (x_3, x_4) = x_2 \text{ in } \\
\langle (x_1, x_3), x_4 \rangle
\end{pmatrix} \text{ in } \begin{pmatrix}
\text{let } (y_1, y_2) = y \text{ in } \\
\text{let } (y_3, y_4) = y_2 \text{ in } \\
\langle (y_1, y_3), y_4 \rangle
\end{pmatrix}
\]
\( \approx_{ax} \) let \((x_1, x_2) = x \) in \( (x_3, x_4) = x_2 \) in

\[
\text{let } y = \langle \langle x_1, x_3 \rangle, x_4 \rangle \text{ in let } \langle y_1, y_2 \rangle = y \text{ in } (y_3, y_4) \text{ by (let}_1) \]

\( \approx_{ax} \) let \((x_1, x_2) = x \) in \( (x_3, x_4) = x_2 \) in

\[
\text{let } \langle y_1, y_2 \rangle = \langle \langle x_1, x_3 \rangle, x_4 \rangle \text{ in let } \langle y_3, y_4 \rangle = y_2 \text{ in } (y_3, y_4) \text{ by (let}_1) \]

\( \approx_{ax} \) let \((x_1, x_2) = x \) in \( (x_3, x_4) = x_2 \) in

\[
\text{let } \langle y_3, y_4 \rangle = x_4 \text{ in } \langle \langle x_1, x_3 \rangle, y_3 \rangle, y_4 \rangle \text{ by (\(\beta_\odot\))} \]

For the right hand side, the components are as follows:

\[
\alpha_{B,C \odot D} = \quad x : B \otimes (C \otimes D) \triangleright \text{let } \langle x_1, x_2 \rangle = x \text{ in}
\]

\[
\text{let } \langle x_3, x_4 \rangle = x_2 \text{ in } \langle \langle x_1, x_3 \rangle, x_4 \rangle : (B \otimes C) \otimes D, \]

\[
\alpha_{A,B \otimes C} = \quad y : A \otimes (B \otimes C) \triangleright \text{let } \langle y_1, y_2 \rangle = y \text{ in}
\]

\[
\text{let } \langle y_3, y_4 \rangle = y_2 \text{ in } \langle \langle y_1, y_3 \rangle, y_4 \rangle : (A \otimes B) \otimes C, \]

\[
\alpha_{A,B \otimes C,D} = \quad z : A \otimes ((B \otimes C) \otimes D) \triangleright \text{let } \langle z_1, z_2 \rangle = z \text{ in}
\]

\[
\text{let } \langle z_3, z_4 \rangle = z_2 \text{ in } \langle \langle z_1, z_3 \rangle, z_4 \rangle : (A \otimes (B \otimes C)) \otimes D, \]

and \( id_A = t : A \triangleright t : A, \ id_D = u : D \triangleright u : D \). Then we compute \( id_A \otimes \alpha_{B,C \otimes D} \) and \( \alpha_{A,B \otimes C} \otimes id_D \):

\[
id_A \otimes \alpha_{B,C \otimes D} = a : A \otimes (B \otimes (C \otimes D)) \triangleright \text{let } \langle x_1, x_2 \rangle = x \text{ in}
\]

\[
\text{let } \langle x_3, x_4 \rangle = x_2 \text{ in } \langle \langle x_1, x_3 \rangle, x_4 \rangle \text{ by (let}_1) \]

\[
\approx_{ax} \text{let } \langle t, x \rangle = a \text{ in let } \langle x_1, x_2 \rangle = x \text{ in}
\]

\[
\text{let } \langle x_3, x_4 \rangle = x_2 \text{ in } \langle \langle t, \langle x_1, x_3 \rangle \rangle, x_4 \rangle \text{ by (let}_1 \rangle \]

\[
\alpha_{A,B \otimes C} \otimes id_D = b : (A \otimes (B \otimes C)) \otimes D \triangleright \text{let } \langle y_1, y_2 \rangle = y \text{ in}
\]

\[
\text{let } \langle y_3, y_4 \rangle = y_2 \text{ in } \langle \langle y_1, y_3 \rangle, y_4 \rangle, u \rangle \text{ by (let}_2 \rangle \]

\[
\approx_{ax} \text{let } \langle y, u \rangle = b \text{ in let } \langle y_1, y_2 \rangle = y \text{ in}
\]

\[
\text{let } \langle y_3, y_4 \rangle = y_2 \text{ in } \langle \langle y_1, y_3 \rangle, y_4 \rangle , u \rangle \text{ by (let}_2 \rangle \]

Let’s compose \( id_A \otimes \alpha_{B,C \otimes D} \) and \( \alpha_{A,B \otimes C,D} \):

\[
(id_A \otimes \alpha_{B,C \otimes D}) : \alpha_{A,B \otimes C,D} = \quad a : A \otimes (B \otimes (C \otimes D)) \triangleright \text{let } z = \left( \text{let } \langle t, x \rangle = a \text{ in let } \langle x_1, x_2 \rangle = x \text{ in} \right)
\]

\[
\text{let } \langle x_3, x_4 \rangle = x_2 \text{ in } \langle \langle t, \langle x_1, x_3 \rangle \rangle, x_4 \rangle \text{ in let } \langle z_1, z_2 \rangle = z \text{ in let } \langle z_3, z_4 \rangle = z_2 \text{ in } \langle \langle z_1, z_3 \rangle, z_4 \rangle \]
9.3. The Category $C_\lambda$

\[ \approx_{ax} \text{let } (t, x) = a \text{ in let } \langle x_1, x_2 \rangle = x \text{ in } \langle x_3, x_4 \rangle = x_2 \text{ in let } z = \langle t, \langle x_1, x_3 \rangle, x_4 \rangle \text{ in } \langle z_1, z_2 \rangle = z \text{ in let } \langle z_3, z_4 \rangle = z_2 \text{ in } \langle \langle z_1, z_3 \rangle, z_4 \rangle \text{ by (let1)} \]

\[ \approx_{ax} \text{let } (t, x) = a \text{ in let } \langle x_1, x_2 \rangle = x \text{ in let } \langle x_3, x_4 \rangle = x_2 \text{ in } \langle z_1, z_2 \rangle = \langle t, \langle x_1, x_3 \rangle, x_4 \rangle \text{ in } \langle z_3, z_4 \rangle = \langle \langle z_1, z_3 \rangle, z_4 \rangle \text{ by (let1)} \]

\[ \approx_{ax} \text{let } (t, x) = a \text{ in let } \langle x_1, x_2 \rangle = x \text{ in let } \langle x_3, x_4 \rangle = x_2 \text{ in let } \langle z_1, z_2 \rangle = \langle t, \langle x_1, x_3 \rangle, x_4 \rangle \text{ in } \langle z_3, z_4 \rangle = \langle \langle z_1, z_3 \rangle, z_4 \rangle \text{ by (let1)} \]

Now we can compute the right hand of the equation:

\[
\begin{align*}
(a \otimes (B \otimes (C \otimes D))) &\triangleright \text{let } b = \left( \begin{aligned}
\text{let } (t, x) &= a \text{ in let } \langle x_1, x_2 \rangle = x \text{ in let } \langle x_3, x_4 \rangle = x_2 \text{ in let } (t, \langle x_1, x_3 \rangle, x_4) = (a, a_4) \text{ in let } a_3 = a_2 \text{ in } \langle a_1, a_3 \rangle, a_4 \rangle : (A \otimes (B \otimes C)) \otimes D \\
\text{let } (y, u) &= b \text{ in let } \langle y_1, y_2 \rangle = y \text{ in let } \langle y_3, y_4 \rangle = y_2 \text{ in } \langle\langle y_1, y_3 \rangle, y_4, u \rangle
\end{aligned}\right) \text{ in } \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle = \langle t, x, t, x \rangle \text{ by (let1)}
\end{align*}
\]

and this is alpha-equivalent to $\alpha_{A,B,C,D} \triangleright A \otimes B \otimes C, D$ Thus Equation \ref{9.11} is verified.

**Equation \ref{9.2}.** We want to show that $\alpha_{A, \top, C}, (\rho_A \otimes \text{id}_C) = \text{id}_A \otimes \lambda_C$. We first write down the components of the equation:

\[
\begin{align*}
a &\triangleright a : A \otimes (\top \otimes C) \triangleright \text{let } \langle a_1, a_2 \rangle = a \text{ in let } \langle a_3, a_4 \rangle = a_2 \text{ in } \langle a_1, a_3 \rangle, a_4 \rangle : (A \otimes \top) \otimes C, \\
\lambda_C &= b : \top \otimes C \triangleright \text{let } \langle b_1, b_2 \rangle = b \text{ in let } * = b_1 \text{ in } b_2 : C, \\
\rho_A &= c : A \otimes \top \triangleright \text{let } \langle c_1, c_2 \rangle = c \text{ in let } * = c_2 \text{ in } c_1 : A,
\end{align*}
\]

and $\text{id}_A = u : A \triangleright u : A$ and $\text{id}_C = v : C \triangleright v : C$. Then we construct $\rho_A \otimes \text{id}_C$ and $\text{id}_A \otimes \lambda_C$:

\[
\begin{align*}
\rho_A \otimes \text{id}_C &= \text{x} : (A \otimes \top) \otimes C \triangleright \text{let } \langle c, v \rangle = x \text{ in let } \langle c_1, c_2 \rangle = c \text{ in let } * = c_2 \text{ in } c_1, v \rangle
\end{align*}
\]
9.3. The Category $C_\lambda$

\[ \approx_{ax} \text{let } (c, v) = x \text{ in let } (c_1, c_2) = c \text{ in} \]
\[ \text{let } * = c_2 \text{ in } (c_1, v) : A \otimes C \text{ by } (let_2^\Sigma), \]

\[ id_A \otimes \lambda_C = \quad \beta \]
\[ y : A \otimes (T \otimes C) \triangleright \text{let } (u, b) = y \text{ in } \begin{cases} \text{let } (b_1, b_2) = b \text{ in } & \text{by } (let_2^\Sigma) \end{cases} \]
\[ \approx_{ax} \text{let } (u, b) = y \text{ in let } (b_1, b_2) = b \text{ in} \]
\[ \text{let } * = b_1 \text{ in } (u, b_2) : A \otimes C \text{ by } (let_2^\Sigma). \]

We then compose $\alpha_{A,T,C}$ and $\rho_A \otimes id_C$:

\[ a : A \otimes (T \otimes C) \triangleright \text{let } x = \left( \begin{array}{l}
\text{let } (a_1, a_2) = a \text{ in } \\
\text{let } (a_3, a_4) = a_2 \text{ in } (a_1, a_3), a_4 \end{array} \right) \text{ in} \]
\[ \approx_{ax} \text{let } (a_1, a_2) = a \text{ in let } (a_3, a_4) = a_2 \text{ in} \]
\[ \text{let } x = (a_1, a_3), a_4 \text{ in } \text{let } (c_1, c_2) = c \text{ in} \]
\[ \text{let } * = c_2 \text{ in } (c_1, v) : A \otimes C \text{ by } (let_1) \]
\[ \text{by } (\beta_\lambda) \]
\[ \approx_{ax} \text{let } (a_1, a_2) = a \text{ in let } (a_3, a_4) = a_2 \text{ in} \]
\[ \text{let } (c_1, c_2) = (a_1, a_3) \text{ in let } * = c_2 \text{ in } (c_1, a_4) : A \otimes C \text{ by } (\beta_\otimes) \]

which is alpha-equivalent to $id_A \otimes \lambda_C$: Diagram [2.7.2] commutes.

**Equation [2.14].** We want to show $\lambda_T = \rho_T$.

\[ \lambda_T = \quad x : T \otimes T \triangleright \text{let } (y, z) = x \text{ in let } * = y \text{ in } z \]
\[ \approx_{ax} \text{let } (y, z) = x \text{ in} \]
\[ \text{let } * = y \text{ in let } * = z \text{ in } * : T \text{ by } (\eta_\Sigma) \]

\[ \rho_T = \quad x : T \otimes T \triangleright \text{let } (y, z) = x \text{ in let } * = z \text{ in } y \]
\[ \approx_{ax} \text{let } (y, z) = x \text{ in} \]
\[ \text{let } * = z \text{ in let } * = y \text{ in } * \text{ by } (\eta_\Sigma) \]
\[ \approx_{ax} \text{let } (y, z) = x \text{ in} \]
\[ \text{let } * = y \text{ in let } * = z \text{ in } * : T \text{ by } (let_2). \]

Thus the equation holds.

**Equation [2.15].** We want $\sigma_{A,B} ; \sigma_{B,A} = id_{A \otimes B}$.

\[ \sigma_{A,B} = x : A \otimes B \triangleright \text{let } (x_1, x_2) = x \text{ in } (x_2, x_1) : B \otimes A \]
\[ \sigma_{B,A} = y : B \otimes A \triangleright \text{let } (y_1, y_2) = y \text{ in } (y_2, y_1) : A \otimes B \]
\[ \sigma_{A,B} ; \sigma_{B,A} = x : A \otimes B \triangleright \text{let } y = (\text{let } (x_1, x_2) = x \text{ in } (x_2, x_1)) \text{ in} \]
\[ \text{let } (y_1, y_2) = y \text{ in } (y_2, y_1). \]
9.3. The Category $C_\lambda$

\[ \approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \]
\[ \text{let } y = \langle x_2, x_1 \rangle \text{ in } \]
\[ \text{let } \langle y_1, y_2 \rangle = y \text{ in } \langle y_2, y_1 \rangle \]

\[ \approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \]
\[ \text{let } \langle y_1, y_2 \rangle = \langle x_2, x_1 \rangle \text{ in } \langle y_2, y_1 \rangle \]

\[ \approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \langle x_1, x_2 \rangle \]

\[ \approx_{ax} x : A \otimes B \]

and thus $2.7.3$ holds.

Equation $2.7.6$: We want $\sigma_{B,\top} ; \lambda_B = \rho_B$. The components are:

\[ \sigma_{B,\top} = x : B \otimes \top \triangleright \text{let } \langle x_1, x_2 \rangle = x \text{ in } \langle x_2, x_1 \rangle : B \otimes \top, \]
\[ \lambda_B = y : \top \otimes B \triangleright \text{let } \langle y_1, y_2 \rangle = y \text{ in let } * = y_1 \text{ in } y_2 : B, \]
\[ \rho_B = x : B \otimes \top \triangleright \text{let } \langle x_1, x_2 \rangle = x \text{ in let } * = x_2 \text{ in } x_1 : B. \]

Let’s compute the left hand side:

\[ \sigma_{B,\top} ; \lambda_B = x : B \otimes \top \triangleright \text{let } y = \langle \text{let } \langle x_1, x_2 \rangle = x \text{ in } \langle x_2, x_1 \rangle \rangle \text{ in } \]
\[ \text{let } \langle y_1, y_2 \rangle = y \text{ in let } * = y_1 \text{ in } y_2 \]
\[ \approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in let } y = \langle x_1, x_2 \rangle \text{ in } \]
\[ \text{let } \langle y_1, y_2 \rangle = y \text{ in let } * = y_1 \text{ in } y_2 \]
\[ \approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in } \]
\[ \text{let } \langle y_1, y_2 \rangle = \langle x_1, x_2 \rangle \text{ in let } * = y_1 \text{ in } y_2 \]
\[ \approx_{ax} \text{let } \langle x_1, x_2 \rangle = x \text{ in let } * = x_2 \text{ in } x_1 : B \]

which is exactly $\rho_B$.

Equation $2.7.6$. We want

\[ \alpha_{A,B,C} ; \sigma_{A \otimes B,C} ; \alpha_{C,A,B} = (\text{id}_A \otimes \sigma_{B,C}) ; \alpha_{A,C,B} ; (\sigma_{A,C} \otimes \text{id}_B). \]

Left hand side. Let’s write down the components:

\[ \alpha_{A,B,C} = x : A \otimes (B \otimes C) \triangleright \text{let } \langle x_1, x_2 \rangle = x \text{ in } \]
\[ \text{let } \langle x_3, x_4 \rangle = x_2 \text{ in } \langle \langle x_1, x_3 \rangle, x_4 \rangle : (A \otimes B) \otimes C, \]
\[ \sigma_{A \otimes B,C} = y : (A \otimes B) \otimes C \triangleright \text{let } \langle y_1, y_2 \rangle = y \text{ in } \langle y_2, y_1 \rangle : C \otimes (A \otimes B), \]
\[ \alpha_{C,A,B} = z : C \otimes (A \otimes B) \triangleright \text{let } \langle z_1, z_2 \rangle = z \text{ in } \]
\[ \text{let } \langle z_3, z_4 \rangle = z_2 \text{ in } \langle \langle z_1, z_3 \rangle, z_4 \rangle : (C \otimes A) \otimes B. \]

Let’s compose $\alpha_{A,B,C}$ and $\sigma_{A \otimes B,C}$:

\[ \alpha_{A,B,C} ; \sigma_{A \otimes B,C} = x : A \otimes (B \otimes C) \triangleright \]
9.3. The Category $\mathcal{C}_A$

Let $y = \begin{pmatrix} \text{let } (x_1, x_2) = x \text{ in} \\
\text{let } (x_3, x_4) = x_2 \text{ in } \langle (x_1, x_3), x_4 \rangle \end{pmatrix}$ in

\[\begin{align*}
\text{let } (y_1, y_2) &= y \text{ in } (y_2, y_1) \\
\approx_{\beta} \text{let } (x_1, x_2) &= x \text{ in } \langle (x_3, x_4) \rangle \text{ in} \\
\text{let } (y_1, y_2) &= y \text{ in } (y_2, y_1) \\
\approx_{\beta} \text{let } (x_1, x_2) &= x \text{ in } \langle (x_3, x_4) \rangle \text{ in} \\
\text{let } (y_1, y_2) &= y \text{ in } (y_2, y_1)
\end{align*}\]

Let’s compute the complete left hand side:

\[\begin{align*}
\alpha_{A,B,C} \cdot \sigma_{A \otimes B, C} \cdot \alpha_{C,A,B} &= x : A \otimes (B \otimes C) \triangleright \\
\text{let } z &= \begin{pmatrix} \text{let } (x_1, x_2) = x \text{ in} \\
\text{let } (x_3, x_4) = x_2 \text{ in } \langle (x_1, x_3), x_4 \rangle \end{pmatrix} \text{ in} \\
\text{let } (z_1, z_2) &= z \text{ in } \langle (z_3, z_4) \rangle = z_2 \text{ in } \langle (z_1, z_3), z_4 \rangle \\
\approx_{\beta} \text{let } (x_1, x_2) &= x \text{ in } \langle (x_3, x_4) \rangle \text{ in} \\
\text{let } (z_1, z_2) &= (x_4, (x_1, x_3)) \text{ in} \\
\text{let } (z_3, z_4) &= z_2 \text{ in } \langle (z_1, z_3), z_4 \rangle \\
\approx_{\beta} \text{let } (x_1, x_2) &= x \text{ in } \langle (x_3, x_4) \rangle \text{ in} \\
\text{let } (z_3, z_4) &= (x_3, x_1) \text{ in } \langle (x_4, z_3), z_4 \rangle \\
\approx_{\beta} \text{let } (x_1, x_2) &= x \text{ in } \langle (x_3, x_4) \rangle \text{ in} \\
\text{let } (x_3, x_4) &= x_2 \text{ in } \langle (x_4, x_1), x_3 \rangle : (C \otimes A) \otimes B \text{ by (}\beta_{\otimes}\text{)}
\end{align*}\]

Right hand side: let’s right down the components:

\[\begin{align*}
id_A &= a : A \triangleright a : A, \\
\sigma_{B,C} &= b : B \otimes C \triangleright \text{let } \langle b_1, b_2 \rangle = b \text{ in } \langle b_2, b_1 \rangle : C \otimes B,
\end{align*}\]

thus

\[\begin{align*}
id_A \otimes \sigma_{B,C} &= x : A \otimes (B \otimes C) \triangleright \text{let } \langle a, b \rangle = x \text{ in} \\
\langle a, \text{let } (b_1, b_2) = b \text{ in } \langle b_2, b_1 \rangle \rangle \\
\approx_{\beta} \text{let } \langle a, b \rangle &= x \text{ in} \\
\text{let } (b_1, b_2) &= b \text{ in } \langle a, \langle b_2, b_1 \rangle \rangle \text{ by (}\beta_{\otimes}^\triangleright\text{)}
\end{align*}\]

\[\begin{align*}
id_B &= c : B \triangleright c : B, \\
\sigma_{A,C} &= d : A \otimes C \triangleright \text{let } \langle d_1, d_2 \rangle = d \text{ in } \langle d_2, d_1 \rangle : C \otimes A,
\end{align*}\]

thus

\[\begin{align*}
\sigma_{A,C} \otimes id_B &= y : (A \otimes C) \otimes B \triangleright \text{let } \langle d, c \rangle = y \text{ in}
\end{align*}\]
Definition 9.3.4. We define the term $\lambda y. (\text{let } * = y \text{ in } M)$, for $M$ a fresh variable.
Lemma 9.3.5. The following axiomatic relations are satisfied:

\[ \Delta \triangleright (\lambda_*, M)^* \cong_{ax} M : A \]

\[ \Delta \triangleright (\lambda_*, V)^* \cong_{ax} V : \top \rightarrow A \]

Proof. Proof by simple calculation.

Lemma 9.3.6. Let \( \eta_A \) be the arrow \( x : A \triangleright \lambda_* x : \top \rightarrow A \) and \( (x : A \triangleright V : \top \rightarrow B)^* \). We want to check Equations (2.5.3), (2.5.4) and (2.5.5).

**Proof.**

We need to check Equations (2.5.3), (2.5.4) and (2.5.5).

Equation (2.5.3). We want \( \eta_A^* = \text{id}_{\top \rightarrow A} : \)

\[ \eta_A = x : A \triangleright \lambda_* x : \top \rightarrow A \]

\[ \eta_A^* = y : \top \rightarrow A \triangleright \lambda_* \text{. let } x = (y^* \text{ in } (\lambda_* x)^*) : \top \rightarrow A \]

Thus

\[ f^* = z : \top \rightarrow A \triangleright \lambda_* \text{. let } y = (z^* \text{ in } (V^*) : \top \rightarrow B, \]

and

\[ \eta_A^* : f^* = x : A \triangleright \lambda_* \text{. let } z = (\lambda_* x)^* \text{ in } \lambda_* \text{. let } y = (z^* \text{ in } (V^*) : \top \rightarrow B \]

\[ = x : A \triangleright \lambda_* \text{. let } y = ((\lambda_* x)^* \text{ in } (V^*) : \top \rightarrow B \]

\[ = x : A \triangleright \lambda_* \text{. let } y = x \text{ in } (V^*) : \top \rightarrow B \]

\[ = y : A \triangleright \lambda_* V^* : \top \rightarrow B \]

\[ = y : A \triangleright V : \top \rightarrow B \]

\[ = f \]

Equation (2.5.4). We want \( f^* ; g^* = (f ; g^*)^* \). If

\[ f = x : A \triangleright V : \top \rightarrow B, \]

\[ g = y : B \triangleright W : \top \rightarrow C, \]

then

\[ f^* = z : \top \rightarrow A \triangleright \lambda_* \text{. let } x = (z^* \text{ in } (V^*) : \top \rightarrow B, \]

\[ g^* = t : \top \rightarrow B \triangleright \lambda_* \text{. let } y = (t^* \text{ in } (W^*) : \top \rightarrow C. \]

Let's compute

\[ f^* ; g^* = z : \top \rightarrow A \triangleright \text{ let } t = (\lambda_* \text{. let } x = (z^* \text{ in } (V^*))) \]
Proof. The fact that \((\lambda\ast, \eta, \mu, t)\) is a monad is a corollary of Lemmas \(\text{9.3.6}\) and \(\text{2.5.3}\). It remains to show that \(t_{A,B}\) is natural in \(A\) and \(B\), and that it satisfies Equations \(\text{9.3.11}\), \(\text{9.3.14}\) and \(\text{9.3.15}\).

### Naturality of \(t_{A,B}\) in \(A\)

We must show that given a map \(f : A \to A'\), the diagram

\[
\begin{array}{ccc}
A \otimes (\top \to B) & \xrightarrow{t_{A,B}} & \top \to (A \otimes B) \\
| & \downarrow{f \otimes (\top \to B)} & \downarrow{\top \to (f \otimes B)} \\
A' \otimes (\top \to B) & \xrightarrow{t_{A',B}} & \top \to (A' \otimes B)
\end{array}
\]

is commutative.
commutes. If \( f \) is the value \( t : A \triangleright V : A' \), then

\[
\begin{align*}
f \otimes (\top \rightarrow B) : u : A \otimes (\top \rightarrow B) \triangleright & \; \langle t, u' \rangle = u \text{ in } \langle V, u' \rangle : A' \otimes (\top \rightarrow B), \\
\top \rightarrow o(f \otimes B) : v : \top \rightarrow o(A \otimes B) \triangleright & \; \lambda \ast. \left( \begin{array}{c}
\text{let } v' = v^* \text{ in } \\
\text{let } t, v'' = v' \text{ in }
\end{array} \right) : \top \rightarrow o(A' \otimes B).
\end{align*}
\]

One needs to show that \( f \otimes (\top \rightarrow B); t_{A',B} = t_{A,B}; \top \rightarrow o(f \otimes B) \). The right hand side is

\[
\begin{align*}
z : A \otimes (\top \rightarrow B) \triangleright & \; \text{let } v = \left( \begin{array}{c}
\text{let } \langle x, y \rangle = z \text{ in } \\
\lambda \ast. \langle x, y \ast \rangle \text{ in } \\
\text{let } v' = v^* \text{ in } \\
\text{let } t, v'' = v' \text{ in } \langle V, v'' \rangle
\end{array} \right) \\
\approx_{ax} & \; \lambda \ast. \left( \begin{array}{c}
\text{let } \langle x, y \rangle = z \text{ in } \\
\text{let } v = \lambda \ast. \langle x, y \ast \rangle \text{ in } \\
\text{let } v' = v^* \text{ in } \\
\text{let } t, v'' = v' \text{ in } \langle V, v'' \rangle
\end{array} \right) \text{ by } (\text{let}^\lambda) \text{ and } (\text{let}_1) \\
\approx_{ax} & \; \lambda \ast. \left( \begin{array}{c}
\text{let } \langle x, y \rangle = z \text{ in } \\
\text{let } v' = \langle x, y \ast \rangle \text{ in } \\
\text{let } t, v'' = v' \text{ in } \langle V, v'' \rangle
\end{array} \right) \text{ by } (\beta_\lambda) \text{ and } (\beta_\ast) \\
\approx_{ax} & \; \lambda \ast. \left( \begin{array}{c}
\text{let } \langle x, y \rangle = z \text{ in } \\
\text{let } v' = \langle x, y \ast \rangle \text{ in } \\
\text{let } t, v'' = v' \text{ in } \langle V, v'' \rangle
\end{array} \right) \text{ by } (\beta_\delta) \text{ and } (\beta_\delta)
\end{align*}
\]

The left hand side is

\[
\begin{align*}
u : A \otimes (\top \rightarrow B) \triangleright & \; \text{let } z = \langle t, u' \rangle = u \text{ in } \langle V, u' \rangle \text{ in } \\
& \; \text{let } \langle x, y \rangle = z \text{ in } \lambda \ast. \langle x, y \ast \rangle \\
\approx_{ax} & \; \text{let } \langle t, u' \rangle = u \text{ in } \\
& \; \text{let } z = \langle V, u' \rangle \text{ in }
\end{align*}
\]
This ends the proof.

\[\text{We define } \Phi^{A,B,C} \text{ and the map } \lambda y \text{ by (let)} \]

\[\begin{align*}
\text{Similarly, if we apply } \Phi^{A,B,C} \circ \Phi^{-1}_{A,B,C} \text{ to } t : A \otimes B \triangleright V : \top \triangleright C, \text{ we get } \\
t : A \otimes B \triangleright \lambda y \cdot \langle x, y \rangle = t \text{ in } (\lambda y \cdot t = \langle x, y \rangle \text{ in } V y)^* y
\end{align*}\]
9.3. The Category $\mathcal{C}_\lambda$

$$\approx_{ax} \lambda^* \text{. let } \langle x, y \rangle = t \text{ in } t = \langle x, y \rangle \text{ in } V^* \quad \text{ by } (\beta_\lambda)$$

$$\approx_{ax} \lambda^* \text{. let } t = \langle x, y \rangle \text{ in } t = \langle x, y \rangle \text{ in } V^* \quad \text{ by } (\text{let}_2)$$

$$\approx_{ax} \lambda^* \text{. let } \langle x, y \rangle = \langle x, y \rangle \text{ in } V^* \quad \text{ by } (\beta_\lambda)$$

$$\approx_{ax} \lambda^* V^* \quad \text{ by } (\beta_\gamma)$$

$$\approx_{ax} \lambda \text{. let } \langle x, y \rangle = \langle x, y \rangle \text{ in } V^* \quad \text{ by } (\beta_\lambda)$$

$$\approx_{ax} \lambda \text{. let } t = \langle x, y \rangle \text{ in } t = \langle x, y \rangle \text{ in } V^* \quad \text{ by } (\text{let}_2)$$

and thus $\Phi_{A,B,C}^{-1}$ is the inverse of $\Phi_{A,B,C}$. To finish the proof it is enough to show that $\leadsto$ is bifunctorial. We need to show that $(- \leadsto -)$ and $(A \leadsto -)$ are functors, and that $(f \leadsto B); (A \leadsto g) = (A' \leadsto g); (f \leadsto B)$, if $f : A \rightarrow A'$ and $g : B \rightarrow B'$.

First consider $id_A \leadsto id_B$: If $id_A = a : A \triangleright a : A$ and $id_B = b : B \triangleright b : B$, it is the arrow

$$x : A \leadsto B \triangleright \lambda a. \text{ let } b = xa \text{ in } b$$

$$\approx_{ax} \lambda a. xa \quad \text{ by } (\beta_\lambda^2)$$

$$\approx_{ax} x \quad \text{ by } (\eta_\lambda)$$

Then consider $f = x : A \triangleright V : A' \triangleright f' = y : A' \triangleright W : A''$. We compute $(f \leadsto B)$ and $(f' \leadsto B)$:

$$t : A'' \leadsto B \triangleright \lambda y. \text{ let } b = tW \text{ in } b$$

$$\approx_{ax} \lambda y. tW : A' \leadsto B \quad \text{ by } (\beta_\lambda^2),$$

$$z : A' \leadsto B \triangleright \lambda x. \text{ let } b = zV \text{ in } b$$

$$\approx_{ax} \lambda x. zV : A \leadsto B \quad \text{ by } (\beta_\lambda^2).$$

The composition of these two functions is

$$t : A'' \leadsto B \triangleright \text{ let } z = \lambda y. tW \text{ in } \lambda x. zV$$

$$\approx_{ax} \lambda x. (\lambda y. tW) V$$

$$\approx_{ax} \lambda x. \text{ let } y = V \text{ in } tW : A \leadsto B \quad \text{ by definition.}$$

Let’s compute $(f; f') \leadsto B$:

$$t : A'' \leadsto B \triangleright \text{ let } b = t(\text{let } y = V \text{ in } W) \text{ in } b$$

$$\approx_{ax} \lambda x. t(\text{let } y = V \text{ in } W)$$

$$\approx_{ax} \lambda x. \text{ let } y = V \text{ in } tW : A \leadsto B \quad \text{ by } (\text{let}^{\text{opp}}),$$

which is precisely $(f' \leadsto B); (f \leadsto B)$.

Now consider $g = x : B \triangleright V : B' \triangleright g' = y : B' \triangleright W : B''$. We compute $(A \triangleright g)$ and $(A \triangleright g')$:

$$t : A \triangleright B \triangleright \lambda a. \text{ let } x = ta \text{ in } V : A \triangleright B',$$

$$z : A \triangleright B' \triangleright \lambda a'. \text{ let } y = za' \text{ in } W : A \triangleright B''.$$
We call ∨V computing (Definition 9.3.9). It means there should be another indexation of the original value, well-typed of duplicable.

However, in the context of indexed terms, the correct statement of this property is slightly more technical. It means there should be another indexation of the original value, well-typed of duplicable.

Let us write down the components of the equations:

\[ A' \rightarrow g = x_1 : A' \rightarrow B \triangleright \lambda x_2. \text{let } y = x_1 x_2 \text{ in } V : A' \rightarrow B' \]

\[ A \rightarrow g = y_1 : A \rightarrow B \triangleright \lambda y_2. \text{let } y = y_1 y_2 \text{ in } V : A \rightarrow B' \]

\[ f \rightarrow B' = z : A' \rightarrow B' \triangleright \lambda x. U : A \rightarrow B' \]

\[ f \rightarrow B = t : A' \rightarrow B \triangleright \lambda x. U : A \rightarrow B \]

Computing \( A' \rightarrow g ); (f \rightarrow B'), we get

\[ x_1 : A' \rightarrow B \triangleright \lambda z = (\lambda x_2. \text{let } y = x_1 x_2 \text{ in } V) \lambda x. z U \]

\[ \approx_{ax} \lambda x. (\lambda x_2. \text{let } y = x_1 x_2 \text{ in } V) U \]

\[ \approx_{ax} \lambda x. \text{let } y = x_1 U \text{ in } V : A \rightarrow B' \]

by \((\beta)\)

The other hand of the equation, \((f \rightarrow B); (A \rightarrow g)\), is

\[ t : A' \rightarrow B \triangleright \text{let } y_1 = \lambda x. U \text{ in } \lambda y_2. \text{let } y = y_1 y_2 \text{ in } V \]

\[ \approx_{ax} \lambda y_2. \text{let } y = (\lambda x. U) y_2 \text{ in } V \]

\[ \approx_{ax} \lambda x. \text{let } y = t U \text{ in } V \]

by \((\beta)\)

by \((\alpha_{let})\),

and thus the equation holds.

9.3.3 Comonadic Structure

The goal is to have the type constructor ! to be a comonad. Ideally, we would like the following to be a derived typing rule:

\[
\begin{align*}
!\Delta \triangleright V : A \\
!\Delta \triangleright V : !A.
\end{align*}
\]

However, in the context of indexed terms, the correct statement of this property is slightly more technical. It means there should be another indexation of the original value, well-typed of duplicable.

Definition 9.3.9. We define a map ! on extended values in the following way:

\[ !x^B = x'^B \]

\[ !(V, W)^n) = (V, !W)^{n+1} \]

\[ !(let \ast = V \text{ in } W) = \text{let } \ast = V \text{ in } !W, \]

\[ !(x^n) = x^{n+1} \]

\[ !(let \langle x^A, y^B \rangle^n = V \text{ in } W) = \text{let } \langle x^A, y^B \rangle^{n+1} = !V \text{ in } !W, \]

\[ !(\lambda^n x^A.M) = \lambda^{n+1} x^A.M, \]

\[ !(let \langle x^A = V \text{ in } W) = \text{let } x^A = !V \text{ in } !W. \]

We call !V the promotion of V.

Lemma 9.3.10. Given a valid typing judgement \( !\Delta \triangleright V : A \), the typing judgement \( !\Delta \triangleright !V : !A \) is valid.

Proof. Proof by structural induction on the derivation of \( !\Delta \triangleright V : A \)
Lemma 9.3.11. Consider an extended value $V$. Then $\text{Erase}(! V) = \text{Erase}(V)$.

Proof. Proof by structural induction on $V$. \hfill \square

Lemma 9.3.12. If $\Delta \triangleright V \approx_{ax} W : A$, then $! \Delta \triangleright !(V \approx_{ax} W) : !A$

Proof. By structural induction on the derivation of $\Delta \triangleright V \approx_{ax} W : A$. We fully develop the case $(\beta_3)$.

Suppose that $\Delta \triangleright \text{let } x^A = V \text{ in } W : B$ is valid. Then so is $\Delta \triangleright W[V/x] : B$. We have $!(\text{let } x^A = V \text{ in } W) = (\text{let } x^{!A} = !V \text{ in } !W)$. From Lemma 9.3.11

$$! \Delta \triangleright \text{let } x^{!A} = !V \text{ in } !W : !B$$

is valid. We therefore have $! \Delta \triangleright ![W[V/x]] : !B$, and by rule $(\beta_3)$, they are axiomatically equivalent.

Now, using 9.3.10, Lemma 9.3.11 and Theorem 9.2.7, we have $! \Delta \triangleright ![W[V/x]] \approx_{ax} ![W[V/x]] : !B$. Therefore,

$$! \Delta \triangleright ![\text{let } x^A = V \text{ in } W] \approx_{ax} ![W[V/x]] : !B.$$ The other cases are handled similarly. \hfill \square

Lemma 9.3.13. Given the map $!$ sending $A$ to $!A$ and sending $x : A \triangleright V : B$ to $x : !A \triangleright !V : !B$, and given the arrows

$$\epsilon_A = x : !A \triangleright x^A : A, \quad \delta_A = x : !A \triangleright x^{!A} : !^2A,$$

$(!, \epsilon, \delta)$ is an idempotent comonad in $C_\lambda$.

Proof. We show the functoriality of $!$.

First, from Lemma 9.3.12 $!$ is a well-defined function on equivalence class of arrows.

Then, given $x : A \triangleright V : B$ and $y : B \triangleright W : C$ we need to show that

$$!(x : A \triangleright V : B); !(y : B \triangleright W : C) \approx_{ax} !(x : A \triangleright \text{let } y = V \text{ in } W : C).$$

Both hands ends up being by definition of composition equal to

$$x : !A \triangleright y^{!B} = !V \text{ in } !W : !C.$$

Finally, the image $!\text{id}_A$ of the unit on $A$ is $!(x : A \triangleright x : A)$, which is by definition $x : !A \triangleright x : !A$, namely the unit on $!A$.

Using Lemmas 9.1.20 9.3.11 and Theorem 9.2.7, the equations

$$x : !A \triangleright \{V <: B\} \approx_{ax} V : B,$$

$$x : !A \triangleright \{V <: !!B\} \approx_{ax} \{V >: !!B\} : !!B$$

are valid, making $\epsilon$ and $\delta$ natural transformations.

The facts that $\delta_A$ is an isomorphism and that $\delta$ and $\epsilon$ verify Equation (2.6.1) and (2.6.2) use similar techniques. \hfill \square
9.3. The Category $C_\lambda$

Lemma 9.3.14. Given the maps

\[
\begin{align*}
\alpha_{A,B,C} &= x : A \otimes (B \otimes C) \rightharpoonup \text{let}(y,z) = x \in (y,t) : (A\otimes B)\otimes C \\
\lambda_A &= x : \top \otimes A \rightharpoonup \text{let}(y,z) = x \in \text{let} * = y \in z : A \\
\rho_A &= x : A \otimes \top \rightharpoonup \text{let}(y,z) = x \in \text{let} * = z \in y : A \\
\sigma_{A,B} &= x : A \otimes B \rightharpoonup \text{let}(y,z) = x \in \langle z,y \rangle : B \otimes A \\
\eta_A &= x : A \rightharpoonup \text{let} \ast x : \top \rightarrow A \\
\mu_A &= x : \top \rightarrow (\top \rightarrow A) \rightharpoonup \text{let} \ast \ast x * : \top \rightarrow A \\
\iota_{A,B} &= z : A \otimes (\top \rightarrow B) \rightharpoonup \text{let}(x,y) = z \in \text{let} \ast = z \in \ast : (A \otimes B) \\
\varepsilon_A &= x : !A \rightharpoonup \text{let}(x) : \top \\
d^A_{A,B} &= z : !A \otimes !B \rightharpoonup \text{let}(x,y) = z \in \langle x,y \rangle : !(A \otimes B) \\
d^\top &= z : \top \rightharpoonup \text{let} \ast = z \in \ast : \top \\
\bigtriangleup_A &= x : !A \rightharpoonup \text{let}(x) : !A \oplus !A \\
\lozenge_A &= x : !A \rightharpoonup \text{let} \ast : \top \\
(x : A \triangleright V : B) \otimes (y : C \triangleright W : D) &= z : A \otimes B \rightharpoonup \text{let}(x,y) = z \in \langle V,W \rangle : C \otimes D \\
(x : A \triangleright V : B) \triangleright (y : C \triangleright W : D) &= z : B \triangleright C \rightharpoonup \text{let} \ast \ast = \ast \ast \ast \in \ast : \bot \triangleright A \\
(x : A \triangleright V : \top \rightarrow B) \ast &= y : \top \rightarrow A \rightharpoonup \text{let} \ast \ast = y \ast \in \ast : \top \rightarrow B \\
\Phi_{A,B,C}(x : A \triangleright V : B \triangleright C) &= t : A \otimes B \rightharpoonup \text{let}(x,y) = t \in V y : \top \rightarrow C
\end{align*}
\]

Table 9.5: Definitions of maps and operations on maps in $C_\lambda$

9.3.4 The Category $C_\lambda$ is a Linear Category for Duplication

Lemma 9.3.14. If we define the maps

\[
\begin{align*}
d^A_{A,B} &= z : !A \otimes !B \rightharpoonup \text{let}(x^A,y^B) = z \in \langle x^A,y^B \rangle : !(A \otimes B), \\
d^\top &= z : \top \rightharpoonup \text{let} \ast = z \in \ast : \top,
\end{align*}
\]

($!,\delta,\epsilon,d,d$) is a strong symmetric monoidal comonad in $C_\lambda$.

Proof. The proof makes heavy use of Lemmas 9.1.25, 9.3.3, 9.3.6, 9.3.7, 9.3.8 and 9.3.15. \hfill \square

Lemma 9.3.15. If we define the maps

\[
\bigtriangleup_A = x : !A \rightharpoonup \langle x^A,x^A \rangle : !A \oplus !A, \quad \lozenge_A = x : !A \rightharpoonup \ast : \top,
\]

the functor $\ast$ is a linear exponential comonad.

Proof. Again, the proof makes heavy use of Lemmas 9.1.25, 9.3.3, 9.3.6, 9.3.7, 9.3.8 and 9.3.15. \hfill \square

Theorem 9.3.16. Together with the maps and the operations on maps defined in Table 9.5, $C_\lambda$ is a linear category for duplication.

Proof. This is a corollary of Lemmas 9.1.25, 9.3.3, 9.3.6, 9.3.7, 9.3.8 and 9.3.15. \hfill \square
Chapter 10

Proof of Theorem 9.2.7

In Chapter 9, we defined a typed lambda-calculus with explicit indexing. The type system is based on linear logic: a special type operator “!” is used to distinguish duplicable and non-duplicable terms. We recall Definitions 9.1.1 and 9.1.3 giving the set of terms and types:

Type $A, B$ ::= $\alpha | (A \rightarrow B) | (A \otimes B) | \top | ![A],$

CoreValue $U, U'$ ::= $x^A | c^A | \ast^n | \lambda x^A.M | (U, U')^n,$

ExtValue $V, W$ ::= $U | \langle V, W \rangle^n | \text{let } x^A = V \text{ in } W | \text{let } \langle x^A, y^B \rangle^n = V \text{ in } W | \text{let } * = V \text{ in } W,$

Term $M, N$ ::= $U | \langle M, N \rangle^n | (MN) | \text{let } \langle x^A, y^B \rangle^n = M \text{ in } N | \text{let } * = M \text{ in } N.$

Terms are separated into core values, extended values and computations. We introduced the notion of valid typing judgement in Section 9.1.2, and we provided an axiomatic equivalence relation on valid typing judgement in Section 9.2. For the axiomatic equivalence relation a notion of substitution is required. This does not come for free due to the subtyping relation: an explicit typecasting is needed and is introduced in Definition 9.1.20: If a term $M$ is valid with type $A$ and if $A <: B$, we inductively define a valid term $\{ M <: B \}$ of type $B$.

One of the desired properties derived from the axiomatic equivalence relation is Theorem 9.2.7, stating that if any two terms are equal without their indexation, they are axiomatically equivalent. In other words, the meaning of a term is not related to the indexation of the term. This chapter is uniquely devoted to the proof of Theorem 9.2.7. The main technical obstacle to a direct proof of this theorem, is the possible “wild” use of the application inside any given term. In order to restrict this, we use the notion of “normalization by evaluation” of (Filinski, 2001) and (Ohori, 1999): we work with a subclass of terms that we call neutral terms on which the result can be proved directly. We then define two rewriting systems yielding in two steps neutral terms from any given terms. A weak normalization result is shown, adapting the techniques described in (Girard et al., 1990, Ch. 4): we show that terms admit a well-founded measure of convergence, which decreases with each reduction of the rewriting system.

10.1 A Handy Tool: Neutral Terms

In this section we define the notion of neutral terms. We prove some useful results and then that any term is axiomatically equivalent to a neutral term.
10.1. A Handy Tool: Neutral Terms

Definition 10.1.1. Following Filinski [2001] and Ohori [1999], the notions of neutral value and neutral term are defined as follows (omitting indexes for readability when possible):

\[ NValue \quad V, W ::= x | c | * | \lambda x.M | (V, W), \]

\[ NTerm \quad M, N ::= V | x V | c V | \text{let } \boxed{\text{def}} = x V \text{ in } M | \text{let } \boxed{\text{def}} = c V \text{ in } M | \]

\[ \text{let } (y, z) = x \text{ in } M | \text{let } (y, z) = c \text{ in } M | \]

\[ \text{let } * = x \text{ in } M | \text{let } * = c \text{ in } M, \]

where \( \boxed{\text{def}} \) means any of \( x, \langle x, y \rangle \) or \( * \). A neutral typing judgement is a typing judgement \( \Delta \triangleright M : A \) where \( M \) is a neutral term.

Lemma 10.1.2. Suppose that \( M \) is a neutral term and that \( \text{Erase}(M) = \text{Erase}(N) \). Then \( N \) is a neutral term.

Proof. Proof by structural induction on \( M \).

Lemma 10.1.3. For valid neutral terms \( \Delta \triangleright M, M' : B \), if \( \text{Erase}(M) = \text{Erase}(M') \) then \( \Delta \triangleright M \approx_{ax} M' : B \).

Proof. We prove it by induction on \( \hat{M} = \text{Erase}(M) \). Note that we also have \( \hat{M} = \text{Erase}(M') \). Base cases:

Cases \( \hat{M} \equiv x, c \) or \( * \). In each case, there is only one typing rule available for \( \Delta \triangleright M : B \) and \( \Delta \triangleright M' : B \), namely \( (ax_1) \) in the fist case, \( (ax_2) \) in the second rule and \( (\top, I) \) in the last case. The terms \( M \) and \( M' \) are determined by the type \( B \), so \( M = M' \) and the result is correct by reflexivity.

Induction cases:

Case \( \hat{M} \equiv \lambda x.\hat{N} \). In this case, \( M \) is of the form \( \lambda^nA.N \) and \( M' \) is of the form \( \lambda^{n'}A'.N' \), where \( \hat{N} = \text{Erase}(N) = \text{Erase}(N') \). Since they are well-typed, from Lemma 9.1.12 the type \( B \) is the raw type of \( M \) and \( M' \) (as in Definition 10.1.2). This implies that \( A = A', n = n' \) and that \( B \) is equal to \( !^n(A \rightarrow C) \) for some type \( C \). Typing trees for \( \Delta \triangleright M : B \) and \( \Delta \triangleright M' : B \) start with a typing rule of the form \( (\lambda_i) \), with \( i = 1 \) if \( n = 0 \), \( i = 2 \) otherwise, and we have the following valid typing judgements:

\[ \Delta, x : A \triangleright N : C, \quad \Delta, x : A \triangleright N' : C. \]

By induction hypothesis, \( \Delta, x : A \triangleright N \approx_{ax} N' : C \). By congruence, we have \( \Delta \triangleright M \approx_{ax} M' : B \).

Case \( \hat{M} \equiv \langle \hat{U}, \hat{V} \rangle \). \( M \) is of the form \( \langle N, P \rangle^n \) and \( M' \) is of the form \( \langle N', P' \rangle^{n'} \), where \( \hat{U} = \text{Erase}(N) = \text{Erase}(N') \) and \( \hat{V} = \text{Erase}(P) = \text{Erase}(P') \). Since \( M \) and \( M' \) are well-typed, from Lemma 9.1.12 the type \( B \) is the raw type of \( M \) and \( M' \). This implies that \( n = n' \) and that \( B \) is equal to \( !^n(A \otimes C) \) for some types \( A \) and \( C \). Typing trees for \( \Delta \triangleright M : B \) and \( \Delta \triangleright M' : B \) start with a typing rule of the form \( (\otimes, I) \), and we have the following valid typing judgements:

\[ !\Delta, \Gamma_1 \triangleright N : !^nA, \quad !\Delta', \Gamma'_1 \triangleright N' : !^nA, \quad !\Delta, \Gamma_2 \triangleright P : !^nC, \quad !\Delta', \Gamma'_2 \triangleright P' : !^nC, \]

where \( \Delta = (\Delta, \Gamma_1, \Gamma_2) = (\Delta', \Gamma'_1, \Gamma'_2) \).

From Lemma 9.1.14 it is possible to have \( \Gamma_1, \Gamma_2, \Gamma'_1 \) and \( \Gamma'_2 \) containing only non-duplicate variables. From Lemma 9.1.17 the sets \( |\Gamma_1| \cap |\Gamma_2| \) and \( |\Gamma'_1| \cap |\Gamma'_2| \) are empty. From Lemma 9.1.17 \( FV(N) = FV(N') \) and \( FV(P) = FV(P') \).
10.1. A Handy Tool: Neutral Terms

This means that \( \Gamma_1 = \Gamma'_1, \Gamma_2 = \Gamma'_2 \) and \( !\hat{\Delta} = !\hat{\Delta}' \). We can then apply the induction hypothesis twice and deduce

\[
!\hat{\Delta}, \Gamma_1 \triangleright N \approx_{ax} N' !^n A, \quad !\hat{\Delta}, \Gamma_2 \triangleright P \approx_{ax} P' !^n C.
\]

Finally, using the congruence rule of the axiomatic equivalence relation, we get that \( \Delta \triangleright M \approx_{ax} M' : B \).

**Case** \( \bar{M} \equiv x\bar{V} \). Since \( M \) and \( M' \) are well-typed, from Lemma \ref{ax-corr}, the type \( B \) is the raw type of \( M \) and \( M' \). This implies that \( M \) is of the form \( x^{A_1 \leftarrow B} V_1 \) and \( M' \) is of the form \( x^{A_2 \leftarrow B} V_2 \), for some neutral values \( V_1 \) and \( V_2 \) and some types \( A_1 \) and \( A_2 \). The typing judgements \( \Delta \triangleright M, M' : B \) comes from the typing rule \( \text{(app)} \): the variable \( x \) occurs in \( \Delta \). The context \( \Delta \) can thus be split into \( (\hat{\Delta}, x : !^n (A' \leftarrow B')) \) for some integer \( n \) where, from Lemma \ref{ax-corr}, \( A_1 <: A', A_2 <: A' \) and \( B' <: B \).

Using Lemma \ref{ax-corr}, one can construct the typing derivations \( \pi \) and \( \pi' \) of the form

\[
\text{(app)} \quad \frac{x : !^n (A' \leftarrow B') \triangleright x^{A_1 \leftarrow B} A_1 \leftarrow B}{\hat{\Delta}, x : !^n (A' \leftarrow B') \triangleright x^{A_1 \leftarrow B} (\Delta_1 \triangleright V_i : A_i)}
\]

where

\[
\hat{\Delta}_i = \begin{cases} \hat{\Delta}, x : !^n (A'' \leftarrow B') & \text{if } x \in FV(V_i), \\ \hat{\Delta} & \text{otherwise}, \end{cases}
\]

for \( i = 1, 2 \). From Lemma \ref{ax-corr}, \( FV(V_1) = FV(V_2) \). This makes \( \hat{\Delta}_1 = \hat{\Delta}_2 \). Call it \( \hat{\Delta}' \). From Lemma \ref{ax-corr}, \( \Delta' \triangleright \{ V_1 <: A' \} : A' \) and \( \hat{\Delta}' \triangleright \{ V_2 <: A' \} : A' \) are valid. Applying induction hypothesis, they are axiomatically equivalent.

Finally, applying axiomatic equivalence rule \( \text{(app)} \), the axiomatic equivalence

\[
\Delta \triangleright x^{A_1 \leftarrow B} V_i \approx_{ax} x^{A' \leftarrow B} \{ V_i <: A' \} : B
\]

is valid for \( i = 1, 2 \). This makes \( \Delta \triangleright M \approx_{ax} M' : B \) valid by congruence and by transitivity.

**Case** \( \bar{M} \equiv c\bar{V} \). This case is similar to the previous case.

Since \( M \) and \( M' \) are well-typed, from Lemma \ref{ax-corr}, the type \( B \) is the raw type of \( M \) and \( M' \). This implies that \( M \) is of the form \( c^{A_1 \leftarrow B} V_1 \) and \( M' \) is of the form \( c^{A_2 \leftarrow B} V_2 \), for some neutral values \( V_1 \) and \( V_2 \) and some types \( A_1 \) and \( A_2 \) such that \( !A_c <: A_1 \leftarrow B \) and \( !A_c <: A_2 \leftarrow B \). The type \( A_c \) is therefore of the form \( A' \leftarrow B' \), with \( A_1 <: A', A_2 <: A' \) and \( B' <: B \).

The typing judgements \( \Delta \triangleright M, M' : B \) comes from the typing rule \( \text{(app)} \). Using Lemma \ref{ax-corr}, one can construct the typing derivation

\[
\Delta \triangleright c^{A_1 \leftarrow B} V_i \approx_{ax} c^{A' \leftarrow B} \{ V_i <: A' \} : B
\]

for \( i = 1, 2 \). From Lemma \ref{ax-corr}, \( \Delta \triangleright \{ V_1 <: A' \} : A' \) and \( \Delta \triangleright \{ V_2 <: A' \} : A' \) are valid. Applying induction hypothesis, they are axiomatically equivalent.

Finally, applying axiomatic equivalence rule \( \text{(app)} \), the axiomatic equivalence

\[
\Delta \triangleright c^{A_1 \leftarrow B} V_i \approx_{ax} c^{A' \leftarrow B} \{ V_i <: A' \} : B
\]

is valid for \( i = 1, 2 \). This makes \( \Delta \triangleright M \approx_{ax} M' : B \) valid by congruence and by transitivity.
Case $\hat{M} \equiv (\text{let } \hat{V} = \hat{P})$. The placeholder $\hat{\cdot}$ stands for $*$, $y$ or $\langle y, z \rangle$, and the placeholder $\hat{\cdot}$ for $x$ or $c$. By $\alpha$-equivalence one can assume that when relevant, the variables $y, z$ are different from $x$ and are not free in $\hat{V}$.

The terms $M$ and $M'$ are well-typed. From Lemma 9.1.12 the type $B$ is the raw type of $M$ and $M'$. One can conclude that $M = (\text{let } \hat{V} = \hat{P})$ and $M' = (\text{let } \hat{V} = \hat{P})$, where $V = \text{Erase}(V_1) = \text{Erase}(V_2)$, $P = \text{Erase}(P_1) = \text{Erase}(P_2)$, and where $(i \text{ being } 1, 2)$

<table>
<thead>
<tr>
<th>$\hat{\cdot}$ is...</th>
<th>$\hat{\cdot}$ is...</th>
<th>$\hat{\cdot}$ is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\ast$</td>
<td>$\ast$</td>
<td>$\perp$</td>
</tr>
<tr>
<td>$\langle y, z \rangle$</td>
<td>$\langle y, z, \hat{D} \rangle$</td>
<td>$\perp(C_1 \circ D_i)$</td>
</tr>
</tbody>
</table>

for some types $C_i$ and $D_i$ and for some integers $n_i$.

In the case $\hat{\cdot} = x$, the variable $x$ is free in $M$ and in $M'$. From Lemma 9.1.11 it is in $\Delta$. From Lemma 9.1.10 the type of $x$ in $\Delta$ is of the form $!n(A' \rightarrow B')$, with $A_1 <: A', A_2 <: A', B' <: B_1$ and $B' <: B_2$.

In the case $\hat{\cdot} = c$, we have $!A_1 <: (A_1 \rightarrow B_1)$ and $!A_2 <: (A_2 \rightarrow B_2)$. Let $!^n(A' \rightarrow B')$ be $A_c$. We then have $A_1 <: A', A_2 <: A', B' <: B_1$ and $B' <: B_2$.

In both cases, this means that if $\hat{\cdot}$ is $\left\{ \begin{array}{ll} * & \text{then } B' \text{ is } \left\{ \begin{array}{ll} \top & \text{where } C' <: C_i, \\ C' & !^n(C' \circ D'), \end{array} \right. \\ (y, z) & \end{array} \right.$.

$D' <: D_i$, and $n' \geq n_i$. Using respectively the identity, the axiomatic equivalence rule ($let^\_x$) and the rule ($let^\_x$), we get that

$$\Delta \triangleright \text{let } \hat{\cdot} = \hat{\square}A_i \rightarrow B_i \text{ in } P_i \approx_{ax} \text{let } \hat{\cdot} = \hat{\square}A_i \rightarrow B_i \text{ in } P_i : B,$$

(10.1.1)

such that if $\hat{\cdot}$ is $\left\{ \begin{array}{ll} * & \text{then } \hat{\cdot} \text{ is } \left\{ \begin{array}{ll} * & \text{where } C' <: C_i, \\ (y, z) & !^n(C' \circ D'). \end{array} \right. \\ (y, z) & \end{array} \right.$.

One can split $\Delta$ as $(!\Delta, \Gamma_1, \Gamma_2)$ such that $\Gamma_1$ contains the free variables of $\hat{V}$ that are not duplicable and $\Gamma_2$ contains the free variables of $\hat{P}$ that are not duplicable: from Lemma 9.1.17 $[\Gamma_1]$ and $[\Gamma_2]$ do not intersect. Invoking Lemma 9.1.12 and Lemma 9.1.19 for $i = 1, 2$ one can write a typing derivation

$$\Delta \triangleright \text{let } \hat{\cdot} = \hat{\square}A_i \rightarrow B_i \text{ in } P_i : B,$$

(10.1.1)

where if $\hat{\cdot}$ is $\left\{ \begin{array}{ll} * & \text{then } (X) \text{ is } \left\{ \begin{array}{ll} \top.E & \text{ where } \Lambda \text{ is } \left\{ \begin{array}{ll} \{ & \text{ (let)} \\ (\otimes.E) & \{ y : C' & !^n(C', z : !^nD'). \right. \\ (y, z) & \end{array} \right. \right. \\ (y, z) & \end{array} \right.$.

One can apply the induction hypothesis on each branch of the derivation. Using the congruence rules of the axiomatic relation and Equation 10.1.1 we obtain finally that $\Delta \triangleright M \approx_{ax} M' : B$.

Case $\hat{M} \equiv (\text{let } \hat{\cdot} = \hat{\square} \text{ in } \hat{P})$. The placeholder $\hat{\cdot}$ stands for $*$ or $\langle y, z \rangle$, and the placeholder $\hat{\cdot}$ for $x$ or $c$. By $\alpha$-equivalence one can assume that when relevant, the variables $y, z$ are different from $x$. 


10.2 Term Rewriting System Number One

The terms \( M \) and \( M' \) are well-typed. From Lemma 10.1.2, the type \( B \) is the raw type of \( M \) and \( M' \). One can conclude that \( M = (\text{let } \alpha = \Box^{B_1} \text{ in } P_1) \) and \( M' = (\text{let } \alpha = \Box^{B_2} \text{ in } P_2) \), where \( P = \text{Erase}(P_1) = \text{Erase}(P_2) \) and where \( i \) being 1, 2.

\[
\begin{array}{|c|c|c|}
\hline
\text{if } \alpha \text{ is...} & \text{if } \alpha \text{ is...} & B_i \text{ is...} \\
\hline
* & * C_i & C_i \\
\hline
y \langle y, z \rangle & y^{C_i} \langle y^{C_i}, z^{D_i} \rangle^{n_i} & !^{n_i} (C_i \otimes D_i) \\
\hline
\end{array}
\]

for some types \( C_i \) and \( D_i \) and for some integers \( n_i \). In the case \( \alpha = x \), the variable \( x \) is free in \( M \) and in \( M' \). From Lemma 9.1.11 it is in \( \Delta \). From Lemma 9.1.16, the type \( A' \) of \( x \) in \( \Delta \) is such that \( A' <: B_1 \) and \( A' <: B_2 \).

In the case \( \alpha = c \), we have \( !^{A_c} <: B_1 \) and \( !^{A_c} <: B_2 \). Let \( A' \) be \( !^{A_c} \).

In both cases, this means that if \( \alpha \) is \( \{ * \} \) then \( A' \) is \( \{ * \} \) where \( C' <: C_i \), \( D' <: D_i \), and \( n' \geq n_i \). Using respectively the identity, the axiomatic equivalence rule \( (\text{let}^{\otimes}) \) and the rule \( (\text{let}^{\otimes}) \), we get that

\[
\Delta \vdash \text{let } \alpha = \Box^{B_i} \text{ in } P_i \approx_{ax} \text{let } \alpha = \Box^{A'} \text{ in } P_i : B,
\]

where, if \( \alpha = x \), \( \Gamma = (x:A') \). One can apply the induction hypothesis on each branch of the derivation. Using the congruence rules of the axiomatic relation and Equation (10.1.2) we obtain finally that \( \Delta \vdash M \approx_{ax} M' : B \).

This ends the list of cases and proves Lemma 10.1.3. \( \square \)

10.2 Term Rewriting System Number One

We define a rewriting system of valid terms yielding neutral terms. We want the denotation to stay constant through the rewriting. The rewriting will be two-fold. First we get rid of "complex computations", and then we get rid of beta-reductions. Note that we are not interested in confluence: the only thing we want is normalization.
Definition 10.2.1. We define the notion of intermediate neutral value and of intermediate neutral term as follows:

\[\begin{align*}
\text{INValue} & : V, W ::=} x^A \mid c^A \mid *^n \mid \lambda^n x^A.M \mid (V, W)^n, \\
\text{INTerm} & : M, N ::=} V \mid x^{A \rightarrow B}V \mid c^{A \rightarrow B}V \mid \text{let } \Box = M \text{ in } N,
\end{align*}\]

where \(\Box\) is a placeholder for any of \(*, x^A\) or \((x^A, y^B)^n\).

Lemma 10.2.2. A neutral term is in intermediate neutral form.

Proof. The proof is done by inspection of the cases. \(\square\)

Remark 10.2.3. A term in intermediate neutral form is not automatically in neutral form. The two main examples of terms that are intermediate neutral but not neutral are

\[\begin{align*}
\text{let } x^A & = (\text{let } y^B = M \text{ in } N) \text{ in } P, & \text{let } x^A & = V \text{ in } M,
\end{align*}\]

where \(V\) is a core value.

Lemma 10.2.4. Suppose that \(\Delta \triangleright M, M' : B\) are valid typing judgements. Suppose moreover that \(\text{Erase}(M) = \text{Erase}(M')\) and that \(M\) is an intermediate neutral term (respectively value). Then \(M'\) is also an intermediate neutral form (respectively value).

Proof. Proof by induction on the size of \(M\). \(\square\)

Lemma 10.2.5. Suppose that \(\Delta = (\Delta', \Gamma_1, \Gamma_2)\), that \(!\Delta' \triangleright V : A\) and \(!\Delta', \Gamma_1, x : A \triangleright M : B\). If \(V\) is an intermediate neutral value and if \(M\) is an intermediate neutral term (respectively intermediate neutral value), then \(M[V/x]\) is an intermediate neutral term (respectively an intermediate neutral value).

Proof. Proof by induction on the size of \(M\). The interesting case is when \(M\) is of the form \(x^{A \rightarrow B}W\): in this situation, the value \(V\) is of type \(A \rightarrow B\), that is, of the form \(\lambda^n y^A.N\) where \(N\) is an intermediate neutral term of type \(B\). Then \(M[V/x] = (\lambda^n y^A.N)W\) which is by definition \((\text{let } y^A = V \text{ in } N)\), an intermediate neutral term. Note that in this case, \(M\) cannot be a value. \(\square\)

Definition 10.2.6. We define the rewrite system number one of terms as the reflexive closure of the relation defined as follows. Given \(x, y\) fresh variables, provided that \(MN : B\), that \(M : A \rightarrow B\) is not a lambda-abstraction, and that \(M\) and \(N\) are not both term variables,

\[MN \rightarrow_{\text{rw1.c1}} \text{let } x^A = M \text{ in } y^A = N \text{ in } x^{A \rightarrow B}y^A.\]

Provided that \((M, N)^n : !^n(A \otimes B)\), and that \(M\) and \(N\) are not both term variables,

\[\langle M, N \rangle^n \rightarrow_{\text{rw1.c2}} \text{let } x^n = M \text{ in } y^n = N \text{ in } \langle x^n, y^n \rangle^n.\]

Finally, we add one congruence rule for each term constructor in the following way: for each rule, \(M\) and \(N\) are terms such that \(M \rightarrow_{\text{rw1.}} M'\) and \(N \rightarrow_{\text{rw1.}} N'\).

\[\begin{align*}
\lambda^n x^A.M & \rightarrow_{\text{rw1.}} \lambda^n x^A.M', & \langle M, N \rangle^n & \rightarrow_{\text{rw1.}} \langle M', N' \rangle^n, \\
MN & \rightarrow_{\text{rw1.}} MN', & \langle M, N \rangle^n & \rightarrow_{\text{rw1.}} \langle M', N' \rangle^n, \\
\text{let } & \langle x^A, y^B \rangle^n = M \text{ in } N \rightarrow_{\text{rw1.g}} \text{let } \langle x^A, y^B \rangle^n = M' \text{ in } N', & \text{let } * = M \text{ in } N \rightarrow_{\text{rw1.}} \text{let } * = M' \text{ in } N'.
\end{align*}\]
Lemma 10.2.7. Suppose that $\Delta \vdash M : C$ is a valid typing judgement, where $M \rightarrow_M M'$. Then $\Delta \vdash M' : C$ is valid and $\Delta \vdash M \approx M' : C$.

Proof. The proof is done by induction of the reduction $M \rightarrow_M M'$.

If reflexivity was used. Then $M = M'$ and the result is immediate.

Case (rw1.2). Here, $M \equiv NP$. From Lemma 10.1.2, $B = C$. Suppose that $\Delta \vdash NP : B$, where $N : A \rightarrow B$. Then one can split $\Delta$ into $(\Delta, \Gamma_1, \Gamma_2)$ where

\[
\begin{array}{c}
\pi_1 \\
\vdots \\
\Delta, \Gamma_1 \vdash N : A \rightarrow B \\
\Delta, \Gamma_2 \vdash P : A \\
\end{array}
\]

is a valid typing derivation. Then if $x$ and $y$ are fresh variables, the derivation

\[
\begin{array}{c}
\pi_2 \\
\vdots \\
\Delta, \Gamma_1 \vdash P : A \\
\Delta, \Gamma_2 \vdash x : A \rightarrow B, y : A \rightarrow x^{A \rightarrow B} y^A : B \\
\end{array}
\]

is valid. The typing judgements $\Delta \vdash NP : B$ and $\Delta \vdash \text{let } x^{A \rightarrow B} = N \text{ in } y^{A} = P$ in $x^{A \rightarrow B} y^A : B$ are axiomatically equivalent by rule (letâ€³).

Case (rw1.2). Here, $M \equiv \langle N, P \rangle^n$. From Lemma 10.1.2, $C = !^n (A \otimes B)$. One can split $\Delta$ into $(\Delta, \Gamma_1, \Gamma_2)$ where

\[
\begin{array}{c}
\pi_1 \\
\vdots \\
\Delta, \Gamma_1 \vdash N : !^n A \\
\Delta, \Gamma_2 \vdash P : !^n B \\
\end{array}
\]

is a valid typing derivation. Then if $x$ and $y$ are fresh variables, the derivation

\[
\begin{array}{c}
\pi_2 \\
\vdots \\
\Delta, \Gamma_1 \vdash P : !^n B \\
\Delta, \Gamma_2 \vdash x : !^n A, y : !^n B \vdash (x^{!^n A} y^{!^n B})^n : !^n (A \otimes B) \\
\end{array}
\]

is valid. The two typing judgements are axiomatically equivalent by rule (letâ€³).

Case (rw1.3). We have $M \equiv \lambda^n x^A . N$. Suppose that $\Delta \vdash \lambda^n x^A . N : C$. Then $C = !^n (A \rightarrow B)$ for some type $B$, the judgement comes from $\Delta, x : A \vdash N : B$ using rule $\lambda_i$, where $i = 1$ if $n = 0$, $i = 2$ otherwise. By induction hypothesis, if $N \rightarrow_N N'$ then $\Delta, x : A \vdash N' : B$ is valid. Then, if $n$ is non null, $\Delta$ is duplicable, and one can apply $\lambda_2$ to get $\Delta \vdash \lambda^n x^A . N' : C$. Otherwise, $n = 0$ and we apply $\lambda_1$ to get $\Delta \vdash \lambda^n x^A . N' : C$.

By induction hypothesis, $\Delta, x : A \vdash M \approx M' : B$. Therefore, by congruence $\Delta \vdash \lambda^n x^A . N \approx \lambda^n x^A . N' : C$. 


Cases rw1.c1, rw1.c2, rw1.c3 and rw1.c4. We have $M = f(N, P)$, where $f(N, P)$ is respectively $NP$, $\langle N, P \rangle^n$, (let $* = N$ in $P$) and $\langle x^A, y^B \rangle^n = N$ in $P$). Suppose that $\Delta \triangleright f(N, P) : C$. Then $\Delta$ splits into $\langle !\Delta, \Gamma_1, \Gamma_2 \rangle$ and the typing judgement is originated from the typing rule $(X)$ and the judgements $\langle !\Delta, \Gamma_1 \triangleright N : C_1 \rangle$ and $\langle !\Delta, \Gamma_2, \Lambda \triangleright P : C_2 \rangle$, where

$$
\begin{array}{c|c|c|c|c}
\text{if } f(N, P) \text{ is...} & (X) \text{ is...} & C_1 \text{ is...} & C_2 \text{ is...} & C \text{ is...} \\
NP & (\text{app}) & A \rightarrow B & A & B \\
\langle N, P \rangle^n & (\otimes. I) & !^n A & !^n B & !^n (A \otimes B) \\
\text{let } * = N \text{ in } P & (\exists. E) & \top & B & B \\
\text{let } \langle x^A, y^B \rangle^n = N \text{ in } P & (\otimes. E) & !^n (A \otimes B) & D & D,
\end{array}
$$

with some types $A$, $B$ and $D$, and such that $\Lambda$ is empty in the three first cases and equal to $(x : !^n A, y : !^n B)$ in the last case.

By induction hypothesis, if $N \rightarrow N'$ and $P \rightarrow P'$, then $!\Delta, \Gamma_1 \triangleright N' : C_1$ and $!\Delta, \Gamma_2, \Lambda \triangleright P' : C_2$ are well-typed. Then, applying $(X)$ we get that $\Delta \triangleright f(N', P') : C$ is valid.

By induction hypothesis again, $!\Delta, \Gamma_1 \triangleright N \approx_{ax} N' : C_1$ and $!\Delta, \Gamma_2, \Lambda \triangleright P \approx_{ax} P' : C_2$. Therefore, by congruence $\Delta \triangleright f(N, P) \approx_{ax} f(N', P') : C$.

This closes the proof of Lemma 10.2.8.

**Lemma 10.2.8.** Suppose that $M, N : C$ and that $\text{Erase}(M) = \text{Erase}(N)$. If $M \rightarrow M'$, then there exists $N'$ such that $\text{Erase}(M') = \text{Erase}(N')$ and such that $N \rightarrow N'$.

**Proof.** The proof is done by induction on the reduction $M \rightarrow M'$.

If reflexivity was used. Then $M = M'$ and the result is immediate by setting $N = N'$.

**Case** rw1.c1. The term $M$ is of the form $M_1 M_2$, where $M_1 : A \rightarrow B$ and where $M_1 M_2 : B$. In this case, $M' = (let \ x^{A\rightarrow B} = M_1 \ in \ y^A = M_2 \ in \ x^{A\rightarrow B} y^A)$. If $N$ is such that $\text{Erase}(M) = \text{Erase}(N)$, then $N = \langle N_1, N_2 \rangle$, where $\text{Erase}(N_1) = \text{Erase}(M_1)$ and $\text{Erase}(N_2) = \text{Erase}(M_2)$.

Since the raw type of $N$ is $B$, there exists a term $A'$ such that $N_1 : A' \rightarrow B$. If we define $N' = (let \ x^{A'\rightarrow B} = N_1 \ in \ y^A = N_2 \ in \ x^{A'\rightarrow B} y^A)$, then by reduction rule rw1.c1, we have $N \rightarrow N'$, and by definition of the map $\text{Erase}$, the terms $M'$ and $N'$ have the same erasure.

**Case** rw1.c2. The term $M$ is of the form $\langle M_1, M_2 \rangle^n$, where $\langle M_1, M_2 \rangle^n : !^n (A \otimes B)$. In this case, $M' = (let \ x^n A = M_1 \ in \ let \ y^n B = M_2 \ in \ (x^n A, y^n B)^n)$. If $N$ is such that $\text{Erase}(M) = \text{Erase}(N)$, then $N = \langle N_1, N_2 \rangle$, where $\text{Erase}(N_1) = \text{Erase}(M_1)$ and $\text{Erase}(N_2) = \text{Erase}(M_2)$.

Since $N : !^n (A \otimes B)$, the raw type of $N$ is $!^n (A \otimes B)$. If we define $N' = (let \ x^n A = N_1 \ in \ let \ y^n B = N_2 \ in \ (x^n A, y^n B)^n)$, then by reduction rule rw1.c2, we have $N \rightarrow N'$, and by definition of the map $\text{Erase}$, the terms $M'$ and $N'$ have the same erasure.

**Case** rw1.c3. The term $M$ is of the form $\lambda^n x^A.M$. In this case, $M' = \lambda^n x^A.\hat{M}$. Where $\hat{M} \rightarrow \hat{M}'$.

Since $\text{Erase}(M) = \text{Erase}(N)$, the term $N$ is also of the form $\lambda^n x^A.\hat{N}$, with $\text{Erase}(\hat{M}) = \text{Erase}(\hat{N})$. By induction hypothesis there exists $N'$ such that $\hat{N} \rightarrow \hat{N}'$. Let $N' = \lambda^n x^A.\hat{N}'$. One has $\text{Erase}(\hat{N}) = \text{Erase}(\hat{N}')$. Using congruence rule rw1.c3, we deduce that $N \rightarrow N'$.

**Cases** rw1.c4, rw1.c5, rw1.c6 and rw1.c7. In these cases, the term $M$ is equal to $f(M_1, M_2)$, where $f(M_1, M_2)$ is respectively of the form $M_1 M_2$, $\langle M_1, M_2 \rangle^n$, (let $* = M_1$ in $M_2$) and of the form $\langle x^A, y^B \rangle^n = M_1$ in $M_2$, with $M_1 \rightarrow M'_1$ and $M_2 \rightarrow M'_2$. We have that $M \rightarrow M'$ where $M' = f(M'_1, M'_2)$.
Since $\text{Erase}(M) = \text{Erase}(N)$, the term $N = g(N_1, N_2)$, where $g(N_1, N_2)$ is respectively of the form $N_1N_2$, $(N_1, N_2)^m$, (let $* = N_1$ in $N_2$) and (let $(x^A, y^B)^m = N_1$ in $N_2$).

By induction hypothesis, $N_1 \rightarrow_1 N_1'$ and $N_2 \rightarrow_1 N_2'$ such that $\text{Erase}(N_1') = \text{Erase}(M_1')$ and $\text{Erase}(N_2') = \text{Erase}(M_2')$. This means, using respectively rules $\text{(rw1.ξ2)}$, $\text{(rw1.ξ3)}$, $\text{(rw1.ξ4)}$ and $\text{(rw1.ξ5)}$, that $g(N_1, N_2) \rightarrow_1 g(N_1', N_2')$.

Since $\text{Erase}(g(N_1', N_2')) = \text{Erase}(f(M_1', M_2'))$, we can define $N' = g(N_1', N_2')$ and we have that $\text{Erase}(M') = \text{Erase}(N')$ and $N \rightarrow_1 N'$.

This closes the proof of Lemma $\text{(10.2.N)}$.

**Definition 10.2.9.** We define the non-negative integer measure $m(M)$ of a typed term $M$ by induction on $M$ as follows (we omit indices for legibility):

$$m(x) = 0,$$
$$m(c) = 0,$$
$$m(*) = 0,$$
$$m(x y) = 0,$$
$$m(x, y) = 0,$$
$$m(\lambda x. N) = m(N),$$
$$m(NP) = 1 + m(N) + m(P),$$
$$m((N, P)) = 1 + m(N) + m(P),$$
$$m(\text{let } * = N \text{ in } P) = m(N) + m(P),$$
$$m(\text{let } x = N \text{ in } P) = m(N) + m(P),$$
$$m(\text{let } (x, y) = N \text{ in } P) = m(N) + m(P).$$

In the case $m(NP)$, we assume that $N$ is not a lambda-abstraction. In the cases $m(NP)$ and $m((N, P))$, we assume that $N$ and $P$ are not both term variables.

**Lemma 10.2.10.** Suppose that $M \rightarrow_1 M'$. Then $M$ is a lambda abstraction if and only if $M'$ is.

**Proof.** The proof is done by case inspection: there are only two possible reductions of the form $\lambda^n x^A.N \rightarrow_1 M'$, namely $\text{(rw1.ξ1)}$, and the identity. In both cases, $M'$ is of the form $\lambda^n x^A.N'$.

Similarly, the only rules of the form $M \rightarrow_1 \lambda^n x^A.N'$ are $\text{(rw1.ξ2)}$, and the trivial one. Again, $M$ is of the form $\lambda^n x^A.N$ in both cases.

**Lemma 10.2.11.** Suppose that $M \rightarrow_1 M'$ where $M \neq M'$. Then $m(M') < m(M)$.

**Proof.** Proof by induction on the reduction. Note that reflexivity is not a possibility since we want $M \neq M'$.

**Case** $\text{(rw1.ξ1)}$. In this case, $M' = \text{let } x^{A \rightarrow B} = N \text{ in let } y^A = P \text{ in } x^{A \rightarrow B} y^A$ and $M = NP$ for some types $A$ and $B$, where $N$ is not a lambda-abstraction and $N$ and $P$ are not both term variables. Since $m(M) = 1 + m(N) + m(P)$ and $m(M') = m(N) + m(P)$, the strict inequality $m(M') < m(M)$ is valid.

**Case** $\text{(rw1.ξ2)}$. In this case, $M' = \text{let } x^n.A = N \text{ in let } y^n.B = P \text{ in } x^n.A, y^n.B)^n$ and $M = (N, P)^n$ for some types $A$ and $B$, where $N$ and $P$ are not both term variables. Since $m(M) = 1 + m(N) + m(P)$ and $m(M') = m(N) + m(P)$, the inequality $m(M') < m(M)$ is valid.

**Case** $\text{(rw1.ξ3)}$. In this case, $M = \lambda^n x^A.N$ and $M' = \lambda^n x^A.N'$ where $N \rightarrow_1 N'$. By induction hypothesis, $m(N') < m(N)$. By definition, we then have that $m(M') = m(N') < m(N) = m(M)$.
10.2. Term Rewriting System Number One

Case \[\text{rw1.} \xi_1] \quad \text{We have } M = NP, \text{ where } N \rightarrow N' \text{ and } P \rightarrow P'. \text{ The terms } N \text{ and } P \text{ therefore cannot be both a term variable. By induction hypothesis, } m(N') \prec m(N) \text{ or } N' = N, \text{ and } m(P') \prec m(P) \text{ or } P' = P, \text{ but equality do not hold for both.}

If } N \text{ is a lambda abstraction, } m(NP) = m(N) + m(P). \text{ Using Lemma } 10.2.10 \text{, the term } N' \text{ is a lambda abstraction: we have } m(N'P') = m(N') + m(P'). \text{ One can conclude that } m(M') = m(N') + m(P') \preceq m(N) + m(P) = m(M).

If } N \text{ is not a lambda abstraction, then we have } m(NP) \npreceq 1 + m(N) + m(P). \text{ By Lemma } 10.2.10, N' \text{ is not a lambda-abstraction: } m(N'P') \npreceq 1 + m(N') + m(P'). \text{ Therefore } m(M') = 1 + m(N') + m(P') \prec 1 + m(N) + m(P) = m(M).

Case \[\text{rw1.} \xi_2] \quad \text{We have } M = \langle N, P \rangle^n, \text{ where } N \rightarrow N' \text{ and } P \rightarrow P'. \text{ The terms } N \text{ and } P \text{ therefore cannot be both a term variable. By induction hypothesis, } m(N') \prec m(N) \text{ or } N' = N, \text{ and } m(P') \prec m(P) \text{ or } P' = P \text{ (but equality do not hold for both).}

We have \(m(\langle N, P \rangle^n) = 1 + m(N) + m(P)\) and \(m(\langle N', P' \rangle^n) = 1 + m(N') + m(P')\). This is enough to say that \(m(M') = 1 + m(N') + m(P') \prec 1 + m(N) + m(P) = m(M)\).

Cases \[\text{rw1.} \xi_3 \text{ and } \text{rw1.} \xi_4] \quad \text{We have } M \text{ respectively of the form } (\text{let } * = N \text{ in } P) \text{ and of the form } \langle x^A, y^B \rangle^n = N^m \text{ in } P', \text{ with } N \rightarrow N' \text{ and } P \rightarrow P'. \text{ We have that } M \rightarrow M' \text{ wherever } M' \text{ is respectively.} \langle x^A, y^B \rangle^n = N^m \text{ in } P'

By induction hypothesis, \(m(N') \prec m(N) \text{ or } N' = N, \text{ and } m(P') \prec m(P) \text{ or } P' = P \text{ (but not } N' = N \text{ and } P' = P\). \text{ Since in both cases, } m(M) = m(N) + m(P) \text{ and } m(M') = m(N') + m(P'), \text{ we have } m(M') \prec m(M).

This ends the induction, and proves the lemma. \hfill \Box

Lemma 10.2.12. Rewrite system number one is normalizing: For any term } M \text{ and any sequence } (M_i)_i \text{ such that } M = M_0 \text{ and such that for all } i \geq 0, M_i \rightarrow_1 M_{i+1}, \text{ there exists a number } n \text{ such that for all } i \geq n, M_i = M_{i+1}.

Proof. We prove the lemma by contradiction. Suppose there exists a term } M \text{ and a sequence } (M_i)_i \text{ such that } M = M_0 \text{ and such that for all } i \geq 0, M_i \rightarrow_1 M_{i+1} \text{ and such that for all } n \text{ there exists a number } n' \geq n \text{ such that } M_{n'} \neq M_n.

Define a sequence } (n(i))_i \text{ as follows. First, } n(0) = 0. \text{ Then, for all } i \geq 0, \text{ define } n(i+1) \text{ as the first number } n' > n(i) \text{ such that } M_{n'} \neq M_{n(i)}. \text{ Note that in this case, for all } i \text{ we have } n(i+1) = n(i+1) \text{ and } M_{n(i+1)} \neq M_{n(i+1)}. \text{ By Lemma } 10.2.11, \text{ this means that } m(M_{n(i+1)}) \leq m(M_{n(i)}) - 1. \text{ We prove by induction on } i \text{ that for all } i, m(M_{n(i+1)}) \leq m(M) - i:

Case } i = 0. \text{ In this case, } M_{n(0)} = M_0 = M, \text{ therefore } m(M_{n(0)}) = m(M) = 0.

Case } i > 0. \text{ Suppose that } m(M_{n(i)}) \leq m(M) - i. \text{ Since } m(M_{n(i+1)}) < m(M_{n(i+1)} - 1), \text{ we have } m(M_{n(i+1)}) \leq m(M_{n(i)}) - 1 \leq m(M) - i - 1 \leq m(M) - (i+1).

Therefore, by induction on } i, m(M_{n(i)}) \leq m(M) - i. \text{ But for } i > m(M), \text{ the value } m(M_i) \text{ is negative, contradicting the non-negativity of the measure. Therefore there exists a number } n \text{ such that for all } i \geq n, M_i = M_{i+1}. \hfill \Box

Lemma 10.2.13. Suppose that } \Delta > M : B \text{ is valid and that for all } M' \text{ such that } M \rightarrow_1 M', M = M'. \text{ Then } M \text{ is in intermediate neutral form.}

Proof. We prove the lemma by induction on the size of } M.

Case } M \equiv x^A, e^A \text{ and } *^n. \text{ Then } M \text{ is in intermediate neutral form.
Case $M \equiv \lambda^n x^A. N$. The only applicable rule is $\text{rw1.c}_1$, meaning that the set of possible $M'$ is the set of terms of the form $\lambda^n x^A. N'$, where $N \rightarrow_1 N'$. Since $M = M'$, we have $N = N'$. By induction hypothesis, $N$ is in intermediate neutral form. This makes $M$ in intermediate neutral form.

Case $M \equiv NP$. There are three possible subcases:

Case $N$ and $P$ are both term variables. Then $M$ is in intermediate neutral form.

Case $N \equiv \lambda^n x^A. N$. The only applicable rewriting rule is $\text{rw1.c}_2$. Since $\Delta \triangleright M : B$ is valid, $n = 0$ and $M \equiv \text{let } x^A = P \text{ in } N$.

In this case, the set of $M'$ such that $M \rightarrow_1 M'$ is spanned by all the terms of the form $\text{let } x^A = P' \text{ in } N'$, when $N \rightarrow_1 N'$ and $P \rightarrow_1 P'$. Since $M' = M$, one has $N' = N$ and $P' = P$. By induction hypothesis, this means that $N$ and $P$ are in intermediate neutral form. The term $M$ is thus in intermediate neutral form.

Otherwise. It is always possible to apply rule $\text{rw1.c}_1$, in which case $M'$ is not equal to $M$. This case is not to be considered.

Case $M \equiv \langle N, P \rangle^n$. There are two possible subcases:

Case $N$ and $P$ are both term variables. Then $M$ is in intermediate neutral form.

Otherwise. It is always possible to apply rule $\text{rw1.c}_2$, in which case $M'$ is not equal to $M$. This case is not to be considered.

Cases $M \equiv \langle \text{let } \ast = N \text{ in } P \rangle$ and $\langle \text{let } \langle x^A, y^B \rangle^n = N \text{ in } P \rangle$. For these two cases, the only applicable rules are respectively $\text{rw1.c}_1$ and $\text{rw1.c}_2$, which means that $M'$ is respectively equal to $\langle \text{let } \ast = N' \text{ in } P' \rangle$ and $\langle \text{let } \langle x^A, y^B \rangle^n = N' \text{ in } P' \rangle$, with $N \rightarrow_1 N'$ and $P \rightarrow_1 P'$. Since $M = M'$, we have $N = N'$ and $P = P'$. By induction hypothesis, $N$ and $P$ are in intermediate neutral form. This makes $M$ in intermediate neutral form.

By exhaustion of the cases, the lemma is verified.

\[ \square \]

10.3 Term Rewriting System Number Two

We now define a rewriting system that takes intermediate neutral terms and returns neutral terms. The proof of the convergence of the rewriting system requires several notions of measures on terms.

10.3.1 The Rewriting System

Definition 10.3.1. We define the rewrite system number two of valid typed intermediate neutral terms. We write $M \rightarrow_2 N$ if either $M = N$, or $M \rightarrow_{23} N$ or $M \rightarrow_{2c} N$, where $(\rightarrow_{23})$ and $(\rightarrow_{2c})$ are defined as follows. First,

\[
\begin{align*}
\text{let } x^A &= V \text{ in } M \rightarrow_{23} M[V/x], & (\text{rw2.} \beta_1) \\
\text{let } \langle x^A, y^B \rangle^n &= \langle V, W \rangle^n \text{ in } M \rightarrow_{23} M[V/x, W/y], & (\text{rw2.} \beta_2) \\
\text{let } \ast &= \ast \text{ in } M \rightarrow_{23} M, & (\text{rw2.} \beta_3)
\end{align*}
\]

(provided that $x, y$ are fresh variables). Then,

\[
\begin{align*}
\text{let } \Box = (\text{let } \Box = M \text{ in } N) \text{ in } P \\
\rightarrow_{2c} \text{ let } \Box = M \text{ in let } \Box = N \text{ in } P, & (\text{rw2.c}_1)
\end{align*}
\]
10.3. Term Rewriting System Number Two

\[ \lambda^n x^A . M \to_{2i} \lambda^n x^A . M', \]
\[ MN \to_{2i} M' N', \]
\[ \langle M, N \rangle^n \to_{2i} \langle M', N' \rangle^n, \]
\[ \text{let } \langle x^A, y^B \rangle^n = M \text{ in } N \to_{2i} \text{ let } \langle x^A, y^B \rangle^n = M' \text{ in } N', \]
\[ \text{let } * = M \text{ in } N \to_{2i} \text{ let } * = M' \text{ in } N'. \]

If \( M \to_{2i} N \) if and only if \( M = N \), we say that \( M \) is in \( \to_{2i} \)-normal form.

**Lemma 10.3.2.** Let \( M \) be an intermediate neutral term (respectively intermediate neutral value). If \( M \to_{2i} N \), then \( N \) is an intermediate neutral term (respectively intermediate neutral value).

**Proof.** Proof by structural induction on \( M \).

**Lemma 10.3.3.** If \( \text{Erase}(M) = \text{Erase}(N) \) and if \( M \to_{2i} M' \) there exists \( N' \) such that \( \text{Erase}(M') = \text{Erase}(N') \) and such that \( N \to_{2i} N' \).

**Proof.** Proof by induction on the reduction \( M \to_{2i} M' \).

**Lemma 10.3.4.** Suppose that \( \Delta \triangleright M : A \) is a valid typing judgements such that \( M \to_{2i} N \). Then \( \Delta \triangleright N : A \) is valid and \( \Delta \triangleright M \approx_{ax} N : A \).

**Proof.** Proof by induction on the reduction \( M \to_{2i} N \).

**Lemma 10.3.5.** Let \( M \) be an intermediate neutral term. If \( M \) is in \( \to_{2\beta} \)-normal form and in \( \to_{2i} \)-normal form then it is a neutral term.

**Proof.** Proof by structural induction on \( M \).

**Lemma 10.3.6.** Suppose that \( V \) is an intermediate neutral value such that \( V \to_{2i} V' \). Suppose that \( M \to_{2i} M' \). Then \( M[V/x] \to_{2i}^* M'[V'/x] \) and \( M[V/x] \to_{2i}^* M'[V/x] \).

**Proof.** Proof by structural induction on \( M \).

**Lemma 10.3.7.** Let \( V \) and \( W \) be intermediate neutral values and let \( M \) be a neutral term.

- If \( \text{let } x^A = V \text{ in } N \to_{2i}^* M \) then \( N[V/x] \to_{2i}^* M \);
- If \( \text{let } \langle x^A, y^B \rangle^n = \langle V, W \rangle^n \text{ in } N \to_{2i}^* M \) then \( N[V/x,W/y] \to_{2i}^* M \);
10.3. Term Rewriting System Number Two

- If \( (let \ * = * \ in \ N) \rightarrow^*_2 M \) then \( N \rightarrow^*_2 M \);

Proof. We prove the result for all the cases in parallel. We consider a term \( P \) of the form \((let \ x^A = V \ in \ N), (let \ (x^A, y^B)^n = (V, W)^n \ in \ N) \) or \((let \ * = * \ in \ N)\) reducing to a neutral term \( M \) in \( n \) steps and proceed by induction on \( n \).

In each case, there is at least one reduction possible (using respectively \([\text{rw}2.3]\), \([\text{rw}2.5]\) and \([\text{rw}2.7]\)), and then the reduction \( P \rightarrow^*_2 M \) can be decomposed into \( P \rightarrow M' \rightarrow^*_2 M \). The first reduction can be one of the following cases:

- \([\text{rw}2.3]\), \([\text{rw}2.5]\) and \([\text{rw}2.7]\). Then \( M' \) is respectively of the form \( N[V/x], N[V/x, W/y] \) and \( N \), and we are done.

- \([\text{rw}2.9]\). Then \( M' \) is of the form \( let \ x^A = V \ in \ N' \). By induction hypothesis, \( N'[V/x] \) reduces to \( M \). Since \( N[V/x] = N'[V/x] \), we have the result.

- \([\text{rw}2.10]\). This case is similar to the previous one. \( M' \) is of the form

\[
let \ x_1^{A_1} = V_1 \ in \ let \ x_2^{A_2} = V_2 \ in \ N',
\]

and \( V = (V_1, V_2)^n \). Applying the induction hypothesis twice and noticing that \( N[V/x] \rightarrow^*_2 N'[V_1/x_1, V_2/x_2] \), we obtain that \( N[V/x] \rightarrow^*_2 M \).

- \([\text{rw}2.11]\). In this case, \( V = *^n \) and \( M' \) is of the form \( let \ x^A = *^n \ in \ N' \). Applying induction hypothesis, we get that \( N'[V/x] \rightarrow^*_2 M \). Since \( N[V/x] \rightarrow^*_2 N'[V/x] \), we get the result.

Congruence cases. These cases are taken care of by using the induction hypothesis, Lemma 10.3.6 and Lemma 10.3.9.

10.3.2 Height of Terms

Definition 10.3.8. Let \( h(M) \) be the height of the term \( M \) to be the positive integer defined as follows:

\[
\begin{align*}
    h(x^A) &= h(c^A) = h(*^n) = 1, \\
    h(x^n \cdot x^A, M) &= h(M) + 1 \\
    h((V, W)^n) &= h(V) + h(W) + 1, \\
    h(c^A \rightarrow^* B, V) &= h(V) + 1, \\
    h(x^A \rightarrow^* B, V) &= h(V) + 1, \\
    h(let \ Q = M \ in \ N) &= 2^{h(M)} + h(N).
\end{align*}
\]

Lemma 10.3.9. Suppose that \( M : A \) and that \( A <: B \). Then \( h\{M <: B\} = h(M) \).

Proof. Proof by structural induction on \( M \).

Lemma 10.3.10. For all intermediate neutral terms \( P, Q \) and \( R \), the following equality is valid:

\[
h(let \ Q = P \ in \ let \ Q = Q \ in \ R) < h(let \ Q = (let \ Q = P \ in \ Q) \ in \ R).
\]

Proof. We have

\[
h(let \ Q = (let \ Q = P \ in \ Q) \ in \ R) = 2^{h(P) + h(Q)} + h(R) = 2^{h(P)} \cdot 2^{h(Q)} + h(R)
\]
and
\[ h(let \mathbf{=} (let \mathbf{=} P \text{ in } Q) \text{ in } R) = 2^{h(P)} + 2^{h(Q)} + h(R). \]

Since for all \( x \geq 1 \) and for all \( y, z \geq 2 \), the inequalities \( 2^x < 2^{2^x} \) and \( y + z \leq y \cdot z \) hold, the lemma is valid.

\[ \square \]

### 10.3.3 Degree of Terms

**Definition 10.3.11.** We define the **degree** \( \delta(A) \) of a type \( A \) as follows:

\[
\begin{align*}
\delta(\top) &= 1, \\
\delta(\alpha) &= 1, \\
\delta(!A) &= \delta(A), \\
\delta(A \otimes B) &= \delta(A \to B) = \max(\delta(A), \delta(B)) + 1.
\end{align*}
\]

The degree of an intermediate neutral term is defined as follows:

\[
\begin{align*}
d(x^A) &= 0, \\
d(c^A) &= 0, \\
d(*^n) &= 0, \\
d((V, W)^n) &= \max(d(V), d(W)) \\
d(\text{let } x^A = V \text{ in } N) &= \max(d(V), d(N), \delta(A \to C)) \\
d(\text{let } \langle x^A, y^B \rangle^n = (V, W)^n \text{ in } N) &= \max(d(V), d(W), d(N), \delta(A \to C), \delta(B \to C)) \\
d(\text{let } * = * \text{ in } N) &= \max(d(N), d(\top \to C)) \\
d(\text{let } \mathbf{=} (let \mathbf{=} M \text{ in } N) \text{ in } P) &= d(\text{let } \mathbf{=} M \text{ in } let \mathbf{=} N \text{ in } P)
\end{align*}
\]

and in all other cases,

\[
d(\text{let } \mathbf{=} M \text{ in } N) = \max(d(M), d(N))
\]

**Lemma 10.3.12.** For all types \( A \), \( \delta(A) \geq 0 \).

*Proof.* Proof by structural induction on \( A \).

**Lemma 10.3.13.** For all terms \( M \), \( d(M) \geq 0 \).

*Proof.* Proof by structural induction on \( M \), using Lemma 10.3.12.

**Lemma 10.3.14.** If \( A <: B \), then \( \delta(A) = \delta(B) \).

*Proof.* By structural induction on a derivation of \( A <: B \).

**Lemma 10.3.15.** Suppose that \( M : A \) and that \( A <: B \). Then \( d(M) = d\{M <: B\} \).

*Proof.* By structural induction on \( M \).

**Lemma 10.3.16.** Suppose that \( M \) is a neutral term. Then \( d(M) = 0 \).

*Proof.* Proof by structural induction on \( M \).
Lemma 10.3.17. The following inequalities are valid:
\[
\begin{align*}
&d(\text{let } (x^A, y^B)^n = M \text{ in } N^C) \leq \max(\delta(A \rightarrow C), \delta(B \rightarrow C), d(M), d(N)), \\
&d(\text{let } x^A = M \text{ in } N^C) \leq \max(\delta(A \rightarrow C), d(M), d(N)), \\
&d(\text{let } * = M \text{ in } N^C) \leq \max(\delta(\top \rightarrow C), d(M), d(N)), \\
&d(\text{let } \square^A = M \text{ in } N) \geq \max(d(M), d(N)).
\end{align*}
\]

Proof. The proof is done by induction on the height of let \( \square^A = M \text{ in } N^C \). We proceed by case distinction on \( \square^A = M \).

Cases \((x^A = V), ((x^A, y^B)^n = \langle V, W \rangle^n)\) and \((*=*)\). In these three cases, the result is true by the definition of the degree.

Case \(\square^A = (\text{let } \square^B = P \text{ in } Q)\). By definition:
\[
\begin{align*}
&d(\text{let } \square^A = M \text{ in } N) = d(\text{let } \square^B = P \text{ in let } \square^A = Q \text{ in } N), \\
&\max(\delta(A \rightarrow C), d(M), d(N)) = \\
&\max(\delta(A \rightarrow C), d(\text{let } \square^B = P \text{ in } Q), d(N)), \\
&\max(d(M), d(N)) = \max(d(\text{let } \square^B = P \text{ in } Q), d(N)),
\end{align*}
\]

We prove the equality by case distinction on \(\square^B = P\):

Subcase \((x^B = V)\). The terms in Equations \(10.3.1\)–\(10.3.3\) become
\[
\begin{align*}
&d(\text{let } \square^A = M \text{ in } N) = \max(d(P), d(\text{let } \square^A = Q \text{ in } N), \delta(B \rightarrow C)), \\
&\max(\delta(A \rightarrow C), d(M), d(N)) = \max(d(P), d(Q), d(N), \delta(A \rightarrow C), \delta(B \rightarrow C)), \\
&\max(d(M), d(N)) = \max(d(P), d(Q), d(N), \delta(B \rightarrow C)).
\end{align*}
\]

By induction hypothesis,
\[
\max(d(Q), d(N)) \leq d(\text{let } \square^A = Q \text{ in } N) \leq \max(d(Q), d(N), \delta(A \rightarrow C)).
\]

Therefore,
\[
\begin{align*}
&\max(d(P), d(Q), d(N), \delta(B \rightarrow C)) \\
&\leq \max(d(P), d(\text{let } \square^A = Q \text{ in } N), \delta(B \rightarrow C)) \\
&\leq \max(d(P), d(Q), d(N), \delta(A \rightarrow C), \delta(B \rightarrow C)).
\end{align*}
\]

Subcases \((x^B, y^B)^n = \langle V, W \rangle^n\) and \((*=*)\). These cases are similar to the previous one.

Subcase \(\square^B = (\text{let } \square^D = R \text{ in } S)\). Then
\[
\begin{align*}
&\max(\delta(A \rightarrow C), d(M), d(N)) \\
&= \max(\delta(A \rightarrow C), d(\text{let } \square^D = R \text{ in } S), d(N)), \\
&\max(d(M), d(N)) = \max(d(\text{let } \square^D = R \text{ in } S), d(N)),
\end{align*}
\]

By definition,
\[
d(\text{let } \square^A = (\text{let } \square^D = (\text{let } \square^D = R \text{ in } S) \text{ in } Q) \text{ in } N)
\]
We define \( n_i(M) \) to be a non-negative integer as follows:

\[
\begin{align*}
    n^i(x^A) &= 0, & n^i(x^{A \rightarrow B} M) &= n^i(M), \\
    n^i(e^A) &= 0, & n^i(e^{A \rightarrow B} M) &= n^i(M), \\
    n^i(e^{n}) &= 0, & n^i(\lambda^n x^A M) &= n^i(M), \\
    n^i((V, W)^n) &= n^i(V) + n^i(W), & n^i((V, W)^n) &= n^i(V) + n^i(W) + e^i_{A \rightarrow C}, \\
    n^i(\text{let } x^A = V \text{ in } N^C) &= n^i(V) + n^i(N) + e^i_{A \rightarrow C, B \rightarrow C}, & n^i(\text{let } x^A = V \text{ in } N^C) &= n^i(V) + n^i(N) + e^i_{A \rightarrow C, B \rightarrow C}, \\
    n^i(\text{let } * = * \text{ in } N^C) &= n^i(N) + e^i_{\top \rightarrow C}, & n^i(\text{let } * = * \text{ in } N^C) &= n^i(N) + e^i_{\top \rightarrow C}, \\
    n^i(\text{let } x^B = M \text{ in } N) &= n^i(\text{let } x^B = M \text{ in } N) + n^i(M) + n^i(N) + e^i_{\top \rightarrow C}. & n^i(\text{let } x^B = M \text{ in } N) &= n^i(\text{let } x^B = M \text{ in } N) + n^i(M) + n^i(N) + e^i_{\top \rightarrow C}.
\end{align*}
\]

and in all other cases,

\[
n^i(\text{let } x^B = M \text{ in } N) = n^i(M) + n^i(N)
\]

We define \( n(M) = n^{d(M)}(M) \), and call it the maximal number of \( M \).

Proof. Proof by structural induction on $M$. \[\square\]

Lemma 10.3.20. For all $i$ we have $n^i(\text{let } M = M \text{ in } N) \geq \max(n^i(M), n^i(N))$.  

Proof. Proof by induction on $M$. \[\square\]

Lemma 10.3.21. Suppose that $M : C$ and that $i > d(M)$. Then $n^i(M) = 0$.  

Proof. The proof is done by double induction on the size and on the height of $M$.

Case $M \equiv \langle V, W \rangle^n$. If $i > d(M)$, then $i > d(V)$ and $i > d(W)$. By induction hypothesis (the size of $V$ and the size of $W$ being strictly smaller than the size of $M$), we have $n^i(V) = n^i(W) = 0$. Since $n^i(M) = n^i(V) + n^i(W)$, it is also null.

Case $M \equiv \langle \text{let } x^A, y^B = \langle V, W \rangle \text{ in } N \rangle$. Here, $d(M) = \max(d(V), d(W), d(N), \delta(A \leftarrow C)) \leftarrow \delta(B \leftarrow C))$, and $n^i(M) = n^i(V) + n^i(W) + n^i(N) + \varepsilon^i_{A \leftarrow C, B \leftarrow C}$. If $i > d(M)$, by induction hypothesis, $n^i(V) = n^i(W) = n^i(N) = 0$. Also, by definition $\varepsilon^i_{A \leftarrow C, B \leftarrow C} = 0$. Thus $n^i(M) = 0$.

Case $M \equiv \langle \text{let } N = \text{ in } P \rangle$. In this case, $M \rightarrow_{2c} M'$ where $M' = \text{let } N = \text{ in } P$. By Lemma 10.3.21, $h(M') < h(M)$. Since $d(M) = d(M')$ and $n^i(M) = n^i(M')$, by induction hypothesis $n^i(M) = 0$.

The remaining cases are similar. \[\square\]

10.3.5 Putting Everything Together

The degree, the number and the height of a term are related: if $M$ is not neutral, there exists $N$ such that $M \rightarrow_2 N$ and such that the triple $(d(N), n(N), h(N))$ is smaller with the lexicographic order to the triple $(d(M), n(M), h(M))$.

Definition 10.3.22. We define a function $\mu$ from intermediate neutral terms to $\mathbb{N}^3$ as follows:

$$\mu(M) = (d(M), n(M), h(M)).$$

We consider the lexicographic ordering on $\mathbb{N}^3$: $(a, b, c) < (a', b', c')$ if and only if

$$(a < a') \lor \left((a = a') \land (b < b')\right) \lor \left((a = a') \land (b = b') \land (c < c')\right).$$

Lemma 10.3.23. Suppose that $(a\nu, b\nu, c\nu)$ is a sequence in $\mathbb{N}^3$ such that for all $\nu$, the inequality $(a_{\nu+1}, b_{\nu+1}, c_{\nu+1}) \leq (a\nu, b\nu, c\nu)$ holds. Then there exists an integer $n_0$ such that for all $\nu \geq n_0$, $(a\nu, b\nu, c\nu) = (a_{n_0}, b_{n_0}, c_{n_0})$.

Proof. Consider the sequence $(a\nu)$, by definition, $a_{\nu+1} \leq a\nu$. Since this is a decreasing sequence of natural numbers: there exists $n_0$ such that $a\nu = a_{n_0}$ for all $\nu \geq n_0$. Consider the sequence $(b\nu)$. By definition, it is a decreasing sequence of natural numbers. Again, there exists some $n_0$ such that for all $\nu \geq n_0$, $b\nu = b_{n_0}$. Finally, consider the sequence $(c\nu)$. By definition, it is a decreasing sequence of natural numbers: there exists some $n_0$ such that or all $\nu \geq n_0$, $c\nu = c_{n_0}$. Thus, for all $\nu \geq n_0$, $(a\nu, b\nu, c\nu) = (a_{n_0}, b_{n_0}, c_{n_0})$. \[\square\]

Lemma 10.3.24. Suppose that let $x^A = V$ in $M : B$, where $V$ is an intermediate neutral value and $M$ an intermediate neutral term. Suppose moreover that let $x^A = V$ in $M$ is in normal form with respect to $\rightarrow_{2c}$. Then
1. \( d(M[V/x]) \leq \max(d(M), d(V), \delta(A)) \);

2. for all \( i \geq \max(d(M), d(V), \delta(A) + 1) \), \( n^i(M[V/x]) = n^i(M) + \xi_M \cdot n^i(V) \), where \( \xi_M \) is the number of free occurrences of \( x \) in \( M \).

**Proof.** First note that is let \( x^A = V \) in \( M \) is in normal form with respect to \( \rightarrow_{2c} \), then any subterm of \( V \) and \( M \) are also in normal form with respect to \( \rightarrow_{2c} \). The proof is done by induction on the size of \( M \) plus the size of \( V \). Cases where \( M \) is an intermediate neutral value:

**Case** \( M \equiv x^B \). Then \( A < : B \), and \( M[V/x] = \{ V < : B \} \).

1. From Lemma 10.3.15, \( d(V < : B) = d(V) \leq \max(d(M), d(V), \delta(A) + 1) \).
2. From Lemma 10.3.19, for all integers \( i \), \( n^i(V < : B) = n^i(V) = n^i(M) + 1 \cdot n^i(V) \).

**Cases** \( M \equiv y^B, M \equiv x^B \) and \( M \equiv \ast^n \). In these three cases, \( M[V/x] = M \).

1. \( d(M[V/x]) = d(M) \leq \max(d(M), d(V), \delta(A) + 1) \).
2. Since \( \xi_M = 0 \), for all integers \( i \), \( n^i(M[V/x]) = n^i(M) + \xi_M \cdot n^i(V) \).

**Case** \( M \equiv \lambda^n y^C \cdot N \). The type \( B \) is of the form \( \forall(C \rightarrow D) \), with \( N : D \).

Using \( \alpha \)-equivalence one can assume that \( y \neq x \). Therefore, the term \( M[V/x] \) is equal to \( \lambda^n y^C \cdot (N[V/x]) \). By induction hypothesis,

\[
\begin{align*}
d(N[V/x]) &\leq \max(d(N), d(V), \delta(A)), \\
\forall i &\geq \max(d(N), d(V), \delta(A) + 1), \\
n^i(N[V/x]) &\leq n^i(N) + \xi_N \cdot n^i(V).
\end{align*}
\]

Note that \( M[V/x] = \lambda^n y^C \cdot N[V/x] \). Therefore:

1. Since \( d(M) = d(N) \) and \( d(M[V/x]) = d(N[V/x]) \),
\[
d(M[V/x]) \leq \max(d(N), d(V), \delta(A) + 1) = \max(d(M), d(V), \delta(A) + 1) \).
\]

2. Since \( x \neq y \), we have \( \xi_M = \xi_N \). Finally, since \( n^i(M) = n^i(N) \) and since \( d(M) = d(N) \), for all \( i \geq \max(d(M), d(V), \delta(A) + 1) \),
\[
n^i(M[V/x]) = n^i(N[V/x]) = n^i(N) + \xi_N \cdot n^i(V) = n^i(M) + \xi_M \cdot n^i(V).
\]

**Case** \( M \equiv (W_1, W_2)^n \). The substitution \( M[V/x] \) is equal to \( (W_1[V/x], W_2[V/x])^n \), and the type \( B \) is of the form \( \forall^n (B_1 \otimes B_2) \) with \( W_1 : \forall^n B_1 \) and \( W_2 : \forall^n B_2 \).

By induction hypothesis, for \( j = 1, 2 \)
\[
\begin{align*}
d(W_j[V/x]) &\leq \max(d(W_j), d(V), \delta(A)), \\
\forall i &\geq \max(d(W_j), d(V), \delta(A) + 1), \\
n^i(W_j[V/x]) &\leq n^i(W_j) + \xi_{W_j} \cdot n^i(V).
\end{align*}
\]

Note that \( M[V/x] = (W_1[V/x], W_2[V/x])^n \).

1. The degree of \( M[V/x] \) satisfies the following:
\[
\begin{align*}
d(M[V/x]) &= \max(d(W_1[V/x]), d(W_2[V/x])) \\
&\leq \max(d(W_1), d(W_2), d(V), \delta(A)) \\
&= \max(d(M), d(V), \delta(A)).
\end{align*}
\]
2. Since \( \xi_M = \xi_{W_1} + \xi_{W_2} \) and since for \( j = 1, 2 \) we have \( d(M) \geq d(W_j) \), then for all \( i \) greater or equal to \( \max(d(M), d(V), \delta(A) + 1) \),
\[
n'(M[V/x]) = n'(W_1[V/x]) + n'(W_2[V/x]) \\
= n'(W_1) + \xi_{W_1} \cdot n'(V) + n'(W_2) + \xi_{W_2} \cdot n'(V) \\
= n'(M) + \xi_M \cdot n'(V).
\]

The cases where \( M \) is not a value are the following.

Case \( M \equiv x^{C\to B}W \). Here, \( W \) is an intermediate neutral value with \( W : C \). From Lemma 9.1.16, \( A <: C \to B \). This means that \( A = !n(C' \to B') \), where \( B' <: B \) and \( C <: C' \).

Since \( V \) is of type \( !n(C' \to B') \), it is of the form \( \lambda^n y^{C'}.N \), and then
\[
M[V/x] = \{ \lambda^n y^{C'}.N <: C \to B \}(W[V/x]) \\
= \{ \lambda^n y^{C'}.(N <: B) \}(W[V/x]) \\
= (\text{let } y^{C} = W[V/x] \text{ in } (N <: B)).
\]

By induction hypothesis,
\[
d(W[V/x]) \leq \max(d(W), d(V), \delta(A)), \\
\forall i \geq \max(d(W), d(V), \delta(A) + 1), \ n'(W[V/x]) = n'(W) + \xi_W \cdot n'(V).
\]

From Lemma 10.3.16, \( W[V/x] \) is an intermediate neutral value. Note that \( M[V/x] = (\text{let } y^{C} = W[V/x] \text{ in } (N <: B)) \).

1. Using Lemma 10.3.14, \( \delta(A) = \delta(C' \to B') = \delta(C \to B) \). From Lemma 10.3.16 we have \( d\{N <: B\} = d(N) \). Finally, \( d(N) = d(V) \) and \( d(M) = d(W) \). Thus,
\[
d(M[V/x]) = \max(d(W[V/x]), d\{N <: B\}, \delta(C \to B)) \\
\leq \max(d(W), d(V), \delta(A), d\{N <: B\}, \delta(C \to B)) \\
\leq \max(d(M), d(V), \delta(A)).
\]

2. From Lemma 10.3.19, \( n'(N <: B) = n'(N) \). By definition, \( n'(N) = n'(V) \) and \( n'(W) = n'(M) \). Finally, \( \xi_M = 1 + \xi_W \). Since \( d(M) = d(W) \), for all \( i \geq \max(d(M), d(V), \delta(A) + 1) \), we have \( e_{C\to B} = 0 \) and thus
\[
n'(M[V/x]) = n'(W[V/x]) + n'(N <: B) = n'(W) + \xi_W \cdot n'(V) + n'(N <: B) \\
= n'(M) + \xi_W \cdot n'(V) + n'(V) = n'(M) + \xi_M \cdot n'(V).
\]

Cases \( M \equiv y^{C\to B}W \) and \( M \equiv y^{C\to B}W \), with \( y \neq x \). The term \( W \) is an intermediate neutral value such that \( W : C \) and the term \( M[V/x] \) is respectively \( y^{C\to B}(W[V/x]), y^{C\to B}(W[V/x]) \). From Lemma 10.2.4, \( W[V/x] \) is an intermediate neutral value. By induction hypothesis,
\[
d(W[V/x]) \leq \max(d(W), d(V), \delta(A)), \\
\forall i \geq \max(d(W), d(V), \delta(A) + 1), \ n'(W[V/x]) = n'(W) + \xi_W \cdot n'(V).
\]

Note that \( M[V/x] = e^{C\to B}(W[V/x]) \).

1. The degree of \( M[V/x] \) is equal to \( d(W[V/x]) \). Thus \( d(M[V/x]) \leq \max(d(W), d(V), \delta(A)) = \max(d(M), d(V), \delta(A)) \).
2. Since \(d(M) = d(W)\) and \(\xi_M = \xi_W\), for all \(i \geq \max(d(M), d(V), \delta(A) + 1)\),
\[
n^i(M[V/x]) = n^i(W[V/x]) = n^i(W) + \xi_W \cdot n^i(V) = n^i(M) + \xi_M \cdot n^i(V).
\]

**Case** \(M \equiv \text{(let } y^C = W \text{ in } N\)). Here, the term \(W\) is an intermediate neutral value, and \(W : C\) and \(N : B\). Using \(\alpha\)-equivalence, one can assume that \(y \neq x\). We have \(M[V/x] = \text{(let } y^C = W[V/x] \text{ in } N[V/x])\).

By induction hypothesis,
\[
\begin{align*}
d(W[V/x]) &\leq \max(d(W), d(V), \delta(A)), \\
d(N[V/x]) &\leq \max(d(N), d(V), \delta(A)), \\
\forall i \geq \max(d(W), d(V), \delta(A) + 1), n^i(W[V/x]) = n^i(W) + \xi_W \cdot n^i(V), \\
\forall i \geq \max(d(N), d(V), \delta(A) + 1), n^i(N[V/x]) = n^i(N) + \xi_N \cdot n^i(V).
\end{align*}
\]

From Lemma 10.2.6: \(W[V/x]\) is an intermediate neutral value. Note that the degree \(d(M)\) is equal to \(\max(d(W), d(N), \delta(C \rightarrow B))\):

1. The degree of \(M[V/x]\) satisfies
\[
d(M[V/x]) = \max(d(W[V/x]), d(N[V/x]), \delta(C \rightarrow B)) \\
\leq \max(d(W), d(V), \delta(A), d(N), d(V), \delta(A), \delta(C \rightarrow B)) \\
= \max(d(M), d(V), \delta(A)).
\]

2. Note that \(\xi_M = \xi_W + \xi_N\), that \(d(M) \geq d(W)\) and \(d(M) \geq d(N)\), and that \(n^i(M) = n^i(W) + n^i(N) + e^e_{C \rightarrow B}\). For all \(i \geq \max(d(M), d(V), \delta(A) + 1)\), we have
\[
n^i(M[V/x]) = n^i(W[V/x]) + n^i(N[V/x]) + e^e_{C \rightarrow B} \\
= n^i(W) + \xi_W \cdot n^i(V) + n^i(N) + \xi_N \cdot n^i(V) + e^e_{C \rightarrow B} \\
= n^i(M) + \xi_M \cdot n^i(V).
\]

**Case** \(M \equiv \text{let } \langle y^C, z^D \rangle^n = (W_1, W_2)^n \text{ in } N\).

Idem.

**Case** \(M \equiv \text{let } * = * \text{ in } N\).

Idem.

**Case** \(M \equiv \text{let } [x] = \text{let } [x] = N \text{ in } P\) in \(Q\). In this case,
\[
\hat{M} = \text{let } [x] = N \text{ in let } [x] = P \text{ in } Q
\]
is such that \(M \rightarrow_2 \hat{M}\) but \(M \neq \hat{M}\). Therefore \(M\) is not in \(\rightarrow_2\)-normal form: We do not consider this case.

**Catch-all case**: \(M \equiv \text{let } [x] = N \text{ in } P\). Here, \([x]\) is respectively *, \(y^C\) and \(\langle y^C, z^D \rangle^n\). By \(\alpha\)-equivalence, one can assume that \(x \neq y\) and \(x \neq z\). Then by definition, the term \(M[V/x]\) is equal to \(\text{let } [x] = N[V/x] \text{ in } P[V/x]\). We claim that if we are indeed in the catch-all case, then so is \(\text{let } [x] = N[V/x] \text{ in } P[V/x]\).

We study the four other possible cases for \(\boxed{} = N[V/x]\):

**Case** \(y^C = W\). Here, \(W\) is a value. For \(W = N[V/x]\) to be a value, \(N\) must be a value: we are not in the catch-all case.
Suppose that Lemma 10.3.25. This situation occurs either when \( N \) is a core value of the form \( (W_1, W_2)^n \), not possible since we are in the catch-all case, or when \( N \) is the variable \( x^{n(C \otimes D)} \) and \( V = (V_1, V_2)^n \). We have

\[
(\text{let } x^A = V \text{ in } M)
\]

\[
= (\text{let } x^{n(C \otimes D)} = (W_1, W_2)^n \text{ in let } (y^C, Z^D)^n = x^{n(C \otimes D)} \text{ in } P)
\]

\[
\rightarrow_{2c} \text{let } x^{n(C \otimes D)} = (W_1, W_2)^n \text{ in let } y^C = W_1 \text{ in let } Z^D = W_2 \text{ in } P.
\]

which contradicts the hypothesis of the lemma. Therefore this case is not to be considered.

Case \((* = *)\). This case is obtained when either \( N = * \), not possible since we are in the catch-all case, or when \( N = x^V \) and \( V = *^n \). In this situation, \( A = !!^n \). We have

\[
(\text{let } x^A = V \text{ in } M) = (\text{let } x^{n^V} = *^n \text{ in let } * = x^V \text{ in } P)
\]

\[
\rightarrow_{2c} \text{let } x^{n^V} = *^n \text{ in } P
\]

which contradicts the hypothesis of the lemma. Therefore this case is not to be considered.

Case \((□^F = (\text{let } □^D = Q \text{ in } R))\). There are two subcases. Either \( N \equiv \text{let } □^D = S \text{ in } T \), but then we are not in the catch-all case, or we have \( N \equiv x^{D^{-c}C}S \) with \( S \) a value and \( V \equiv \lambda^n y^{D^c} \cdot R \). In this case,

\[
(\text{let } x^A = V \text{ in } M) = (\text{let } x = \lambda y. R \text{ in let } □^F = (\text{let } y^D = S \text{ in } R) \text{ in } P)
\]

\[
\rightarrow_{2c} \text{let } x = \lambda y. R \text{ in let } y^D = S \text{ in let } □^F = R \text{ in } P,
\]

which contradicts the hypothesis of the lemma. Therefore this case is not to be considered.

Thus the term \( M[V/x] = (\text{let } □^F = N[V/x] \text{ in } P[V/x]) \) is in the catch-all form. By induction hypothesis,

\[
d(N[V/x]) \leq \max(d(N), d(V), \delta(A)),
\]

\[
d(P[V/x]) \leq \max(d(P), d(V), \delta(A)),
\]

\[
\forall i \geq \max(d(N), d(V), \delta(A) + 1), \ n^i(N[V/x]) = n^i(N) + \xi_N \cdot n^i(V),
\]

\[
\forall i \geq \max(d(P), d(V), \delta(A) + 1), \ n^i(P[V/x]) = n^i(P) + \xi_P \cdot n^i(V).
\]

Now:

1. Since the degrees \( d(M) \) and \( d(M[V/x]) \) are respectively equal to \( \max(d(P), d(N)) \) and equal to \( \max(d(P[V/x]), d(N[V/x])) \), we have \( d(M[V/x]) \leq \max(d(M), d(V), \delta(A)) \).

2. We have \( \xi_M = \xi_N + \xi_P \), \( d(M) \geq d(N) \) and \( d(M) \geq d(P) \). Therefore, for all integer \( i \geq \max(d(M), d(V), \delta(A) + 1) \),

\[
n^i(M[V/x]) = n^i(N[V/x]) + n^i(P[V/x])
\]

\[
= n^i(N) + \xi_N \cdot n^i(V) + n^i(P) + \xi_P \cdot n^i(V)
\]

\[
= n^i(M) + \xi_M \cdot n^i(V).
\]

Thus, by induction the degree of \( M[V/x] \) is smaller or equal to \( \max(d(M), d(V), \delta(A)) \), and for all integers \( i \) bigger or equal to \( \max(d(M), d(V), \delta(A) + 1) \),

\[
n^i(M[V/x]) = n^i(M) + \xi_M \cdot n^i(V).
\]

**Lemma 10.3.25.** Suppose that \( M : B \) is in \( \rightarrow_{2c} \)-normal form. Then one of the following three statements is valid:
1. $M$ is in $\rightarrow_{2\beta}$-normal form.

2. $n(M) = 0$ and there exists $N \neq M$ such that $M \rightarrow_2 N$ with $d(N) < d(M)$.

3. $n(M) \neq 0$ and there exists $N \neq M$ such that $M \rightarrow_2 N$ with $d(M) < d(N)$ or $d(M) = d(N)$ and $n(N) < n(M)$.

Proof. Suppose that $M$ is not in $\rightarrow_{2\beta}$-normal form. We prove the result by induction on $M$.

Case $M \equiv (let \ [P = P \in Q] \ in \ R)$. In this case, $M$ is not in $\rightarrow_{2\gamma}$-normal form. Therefore this case is not to be considered.

Case $M \equiv (let \ x^A = V \ in \ P)$. The degree of $M$ is equal to $\max (d(V), d(P), \delta (A \rightarrow B))$, and $n(M) = n^{d(M)}(P) + n^{d(M)}(V) + e^{d(M)}_{\delta \rightarrow B}$. Note that since $M$ is in $\rightarrow_{2\gamma}$-normal form, so are $V$ and $P$.

Subcase $n(M) = 0$. We construct a term $N$ such that $d(N) < d(M)$ and $M \rightarrow_{2\beta} N$.

From Lemma 10.3.13 $n^{d(M)}(P) = n^{d(M)}(V) = e^{d(M)}_{A \rightarrow B} = 0$. Since $d(M) \geq \delta (A \rightarrow B)$, this means $d(M) > \delta (A \rightarrow B)$. Note that $(V), d(P) \leq d(M)$.

Suppose that $d(V) = d(M)$. Then $n(V) = n^{d(M)}(V) = 0$. Since $M$ is in $\rightarrow_{2\gamma}$-normal form, so is $V$. Then by induction hypothesis, there exists $V'$ such that $V \rightarrow_{2\beta} V'$ with $d(V') < d(V)$. From lemma 10.3.13, the term $V'$ is an intermediate neutral value. If $d(V') < d(M)$, define $V'$ to be $V$. Therefore, in both cases we obtain an intermediate neutral value $V'$ such that $V \rightarrow_{2\beta} V'$ with $d(V') < d(M)$.

Suppose that $d(P) = d(M)$. Then $n(P) = n^{d(M)}(P) = 0$. By induction hypothesis, there exists $P'$ such that $P \rightarrow_{2\beta} P'$ with $d(P') < d(P)$. If $d(P') < d(M)$, define $P'$ to be $P$. Therefore, in both cases we obtain a term $P'$ such that $P \rightarrow_{2\beta} P'$ with $d(P') < d(M)$.

Define $N$ to be $(let \ x^A = V' \ in \ P')$. Since $V'$ is an intermediate neutral value, $d(N) = \max (d(V'), d(P'), \delta (A \rightarrow B))$.

Since $d(V'), d(P'), \delta (A \rightarrow B) < d(M)$, we also have $d(N) < d(M)$.

Subcase $n(M) \neq 0$. We construct a term $N$ such that $M \rightarrow_{2\beta} N$ with $d(N) < d(M)$ or with $d(M) = d(N)$ and $n(N) < n(M)$.

Suppose that $n^{d(M)}(P) \neq 0$. From Lemma 10.3.24 and since $d(P) \leq d(M)$, the degree of $P$ is equal to the degree of $M$. Therefore, $n(P) \neq 0$ and we can apply the induction hypothesis: there exists a term $P'$ such that $P \rightarrow_{2\beta} P'$, $d(P') = d(P)$ and $n(P') < n(P)$. Let $N$ be $(let \ x^A = V \ in \ P')$. We have $M \rightarrow_{2\beta} N$ with $d(N) = \max (d(V), d(P'), \delta (A \rightarrow B)) = d(M)$ and $n(N) = n^{d(M)}(P') + n^{d(M)}(V) + e^{d(M)}_{\delta \rightarrow B} < n(M)$.

Now, suppose that $n^{d(M)}(V) \neq 0$. Similarly, from Lemma 10.3.24 and since $d(V) \leq d(M)$, the degree $d(V) = d(M)$. This means $n(V) \neq 0$ and we can apply the induction hypothesis: there exists a term $V'$ such that $V \rightarrow_{2\beta} V'$, $d(V') = d(V)$ and $n(V') < n(V)$. Let $N$ be $(let \ x^A = V' \ in \ P)$. We have $M \rightarrow_{2\beta} N$ with $d(N) = \max (d(V'), d(P), \delta (A \rightarrow B)) = d(M)$ and $n(N) = n^{d(M)}(P) + n^{d(M)}(V') + e^{d(M)}_{\delta \rightarrow B} < n(M)$.

Finally, suppose that both $n^{d(M)}(V)$ and $n^{d(M)}(P)$ are null. Then $n(M) = e^{d(M)}_{\delta \rightarrow B} = 1$. Let $N$ be $P[V/x]$. Since $V$ is an intermediate neutral value, $M \rightarrow_{2\beta} N$. By Lemma 10.3.24 $d(N) \leq \max (d(P), d(V), \delta (A)) \leq d(M)$ and for all $i \geq \max (d(P), d(V), \delta (A) + 1)$, $n(i) = n'(P) + \xi_{P} \cdot n'(V)$. If $d(N) < d(M)$, we are done. If $d(N) = d(M)$, then $d(M) \geq \max (d(P), d(V), \delta (A) + 1)$, thus $n(N) = n^{d(M)}(N) = 0$. Hence $d(N) < d(M)$, and we are also done.

The two cases $M \equiv (let \ (x^A, y^B)^n = (V, W)^n \ in \ P)$ and $N \equiv (let \ * = \ * \ in \ M)$ are done similarly. Finally, the congruence cases are trivial.
Definition 10.3.26. We say that an intermediate term \( M \) satisfies reduction if the following is valid:

“If \( M \rightarrow_{2c} N \), then there exists \( N' \) such that \( M \rightarrow_{2}^* N' \) and \( \mu(N') < \mu(M) \).”

Lemma 10.3.27. Let \( M \) be an intermediate neutral term satisfying reduction, then either \( M \) is a neutral term or there exists \( N \) such that \( \mu(N) < \mu(M) \) and \( M \rightarrow_{2}^* N \).

Proof. Consider an intermediate neutral term \( M \) satisfying reduction. If it is already a neutral term, we are done. If it is not, from Lemma 10.3.5 then it is not in \( \rightarrow_{2c} \)-normal form. There are two cases:

- \( M \) is not in \( \rightarrow_{2c} \)-normal form. By the reduction property of \( M \) there is \( N \) such that \( M \rightarrow_{2}^* N \) and \( \mu(N) < \mu(M) \).

- \( M \) is in \( \rightarrow_{2c} \)-normal form. It is not in \( \rightarrow_{2} \beta \)-normal form, and from Lemma 10.3.25 there exists \( N \) such that \( M \rightarrow_{2} \beta N \) with \( \mu(N) < \mu(M) \).

In both cases, we have as requested the existence of some intermediate neutral term \( N \) such that \( M \rightarrow_{2}^* N \).

Corollary 10.3.28. Let \( M \) be an intermediate neutral term satisfying reduction. Then there exists a neutral term \( N \) such that \( M \rightarrow_{2}^* N \).

Proof. Let \( S \) be the set of terms \( M \) such that \( M \rightarrow_{2}^* M' \). Let \( I = \mu(S) \). From Lemma 10.3.23, this set has a minimum element. Let \( N \in S \) be a term such that \( \mu(N) \) is this minimum. Lemma 10.3.27 states that \( N \) is neutral.

Lemma 10.3.29. Every intermediate term satisfies reduction, as stated in Definition 10.3.26.

Proof. Suppose that \( M \rightarrow_{2c} N \). We prove the result by induction on the size \( M \). Case distinction on the last rule used in the derivation of \( M \rightarrow_{2c} N \):

Case \( \text{rw2.c1} \). In this case, by definition, the two sides of the relation have the same degree and the same maximal number, but a smaller height by Lemma 10.3.10. Choose \( N' \) to be equal to \( N \) and this satisfies the lemma.

Case \( \text{rw2.c2} \). Suppose that \( P : B \). The left hand side is

\[
M = (\text{let } x^m(D \rightarrow_C) = \lambda^n y^P \text{ in let } x^{C'} = x^{D' \rightarrow_C} S \text{ in } P)
\]

Its degree is \( d(M) = \max(d(R), \delta((D \rightarrow C) \rightarrow B), d(S), d(P)) \). Note that \( S \) is an intermediate value.

The right hand side is

\[
N = (\text{let } x^m(D \rightarrow_C) = \lambda^n y^P \text{ in let } y^{C'} = S \text{ in let } x^{C'} = \{ R < : C' \} \text{ in } P)
\]

Its degree is

\[
d(N) = \max(d(R), \delta((D \rightarrow C) \rightarrow B), d(S), \delta(D' \rightarrow_B), d(\text{let } x^{C'} = \{ R < : C' \} \text{ in } P))
\]

From Lemma 10.3.17 we get \( d(N) = d(M) \).

We proceed by case distinction on \( d(M) \) to find the term \( N' \).
Suppose that \( d(M) > \delta (D \rightarrow C \rightarrow B) \). Consider \( X \) being the terms among \( R, S \) and \( P \) such that \( d(X) = d(M) \). Whether \( X \) are or not in \( \rightarrow 2C \)-normal form, one of Lemma 10.3.25 or the induction hypothesis applies: Either \( X \) is in \( \beta \)-normal form, and thus by Lemma 10.3.16 \( d(X) = 0 \), or \( X \) reduces to \( X' \) with \( d(X') < d(X) \) or with \( d(X') = d(X) = d(M) \) and \( n(X') < n(M) \). In this last case, since \( d(X') = d(M) \), this means that \( n(N') < n(M) \) and \( d(N') = d(M) \) if \( N' \) is \( M \) with \( X' \) in place of \( X \).

Otherwise, we have a term \( N' \) with \( M \rightarrow N' \) and \( d(N') < d(M) \).

Suppose that \( d(M) = 1 + \delta (D \rightarrow C) \) and \( d(M) > 1 + \delta (B) \). The terms \( R \) and \( S \) are smaller than \( M \): By induction hypothesis they satify the lemma. Then by Lemma 10.3.28, there exist neutral terms \( R' \) and \( S' \) such that \( R \rightarrow_2 R' \) and \( S \rightarrow_2 S' \). By Lemma 10.3.16, we have \( d(R') = 0 \) and \( d(S') = 0 \).

Since let \( x^\nu (D \rightarrow C) = \lambda^\nu y^D.R \) in \( P \) is smaller than \( M \), by the induction hypothesis one can apply Lemma 10.3.28 and it reduces to a neutral term \( P' \). From Lemma 10.3.17 \( P[V/x] \) reduces to the same neutral term \( P' \). Therefore \( M \) reduces to

\[
M \rightarrow 2 \text{ let } y^D = S'[\lambda^\nu y^D.R/x] \text{ in let } \Box' = \{R' < : C'\} \text{ in } P[\lambda^\nu y^D.R/x] \\
\rightarrow 2 \text{ let } y^D = S'[\lambda^\nu y^D.R/x] \text{ in let } \Box' = \{R' < : C'\} \text{ in } P'.
\]

Let \( N' \) be this last term. Since from Lemma 10.3.24 \( S'[\lambda^\nu y^D.R/x] \) is a value, the term \( let x^\nu (D \rightarrow C) = \lambda^\nu y^D.R \) in \( S' \) is in \( \rightarrow 2C \)-normal form. Thus Lemma 10.3.24 applies:

\[
d(N') = \max(\delta(D \rightarrow B), d(S'[\lambda^\nu y^D.R/x]), d(\text{let } \Box') = \{R' < : C'\} \text{ in } P')) \\
\leq \max(\delta(D \rightarrow B), d(S'), d(R'), \delta(D \rightarrow C), d(\text{let } \Box') = \{R' < : C'\} \text{ in } P')). \\
\leq \max(\delta(D \rightarrow B), d(S'), d(R'), \delta(D \rightarrow C), d(\{R' < : C'\}), d(P'), \delta(C' \rightarrow B)).
\]

Since \( d(S') = d(R') = d(P') = 0 \), \( d(C') \) is smaller, and since \( d(M) > \delta(D) + 1 \), \( d(M) > \delta(C) + 1 \) and \( d(M) > \delta(B) + 1 \), we have \( d(N') < d(M) \).

Suppose that \( d(M) = 1 + \delta (B) \). Let \( Q = (let y^P' = S \) in let \( \Box' = \{R < : C'\} \) in \( P \). The term \( Q \) is smaller than \( M \), so induction hypothesis applies.

Suppose that \( Q \) is not in \( \rightarrow 2C \)-normal form. Then there exists \( Q' \) such that \( Q \rightarrow_2 Q' \) with \( \mu (Q') < \mu (Q) \). Let \( N' = (let x^\nu (D \rightarrow C) = \lambda^\nu y^D.R \) in \( Q' \). Note that \( M \rightarrow_2 N' \). We have \( d(N') = \max(\delta(D \rightarrow C \rightarrow B), d(R), d(Q')) = 1 + \delta (B) = d(M) \), and \( n(N') < n(M) \). Finally, since \( h(Q') < h(Q) \), we have \( h(N') < h(M) \). Therefore \( \mu (N') < \mu (M) \).

Now, suppose that \( Q \) is in \( \rightarrow 2C \) normal form. Then so is \( N \), and we have the result using Lemma 10.3.24.

**Case \([rw2.c]\)**: Suppose that \( P : B \). The left hand side is

\[
M = (let x^\nu (C \otimes D) = \langle V, W \rangle^n \text{ in let } y^C, z^{D'}^m = x^\nu (C' \otimes D) \text{ in } P)
\]

Its degree is \( d(M) = \max(d(V), d(W), \delta((D \otimes C) \rightarrow B), d(P)) \). The right hand side is

\[
N = (let x^\nu (C \otimes D) = \langle V, W \rangle^n \text{ in } y^m C' = \{V < : !^m C'\} \text{ in let } z^{m D'} = \{W < : !^m D'\} \text{ in } P),
\]

and its degree is the same as the one of \( M \).

We proceed by case distinction on \( d(M) \) to find the term \( N' \). The cases are treated similarly as in the previous case.
Suppose that \( d(M) > \delta((D \otimes C) \rightarrow B) \). Using Lemma 10.3.18, one can find \( V', W' \) and \( P' \) such that \( V \rightarrow_2 V', W \rightarrow_2 W \) and \( P \rightarrow_2 P' \) such that
\[
d(\text{let } x'^m(C \otimes D)) = (V', W')^m \text{ in let } (y'^C, z'^D)^m = x'^m(C' \otimes D') \text{ in } P' < d(M).
\]

Suppose that \( d(M) = 1 + \delta(D \otimes C) \) and \( d(M) > 1 + \delta(B) \). Since \( V, W \), and let \( x = (V, W)^n \) in \( P \) are strictly smaller than \( M \), the induction hypothesis applies and they satisfy the lemma. Thus Lemma 10.3.28 applies and they reduces to some neutral terms \( V', W' \) and \( P' \). From Lemma 10.3.4 \( P((V, W)^n/x) \) also reduces to \( P' \). Therefore \( M \) reduces to
\[
N' = (\text{let } y'^C, z'^D)^m = (V', W')^m \text{ in } P'.
\]

We have
\[
d(N') = \max(d(V'), d(W'), d(P'), \delta(C' \rightarrow B), \delta(D' \rightarrow B)).
\]

From Lemma 10.3.11 \( d(N') < d(M) \).

Suppose that \( d(M) = 1 + \delta(B) \). This time, we choose
\[
Q = (\text{let } y'^mC' = \{V < :!^mC'\} \text{ in let } z'^mD' = \{W < :!^mD'\} \text{ in } P)
\]

The term \( Q \) being smaller than \( N \), the induction hypothesis applies.

Suppose that it is not in \( \rightarrow_2 \)-normal form. Then there exists \( Q' \) such that \( Q \rightarrow_2 Q' \) with \( \mu(Q') < \mu(Q) \). Let \( N' = (\text{let } x'^m(C \otimes D)) = (V', W')^m \text{ in } Q' \). We have \( M \rightarrow_2 N' \), with \( d(N') = d(M) \), \( n(N') \leq n(M) \), and \( h(N') < h(M) \). Thus \( \mu(N') < \mu(M) \).

Now, suppose that it is still \( \rightarrow_2 \)-normal form. Then it is \( N \), and we have the result by Lemma 10.3.4.

Case \( (tw2.\xi_1) \). In this case,
\[
M = (\text{let } x'^m \uparrow = s^m \text{ in let } * = x \uparrow \text{ in } P), \quad N = (\text{let } x'^m \uparrow = s^m \text{ in } P).
\]

Note that \( d(M) = d(N) \), that \( n(N) = n(P) \lesssim n(M) \) and that \( h(N) < h(M) \). Therefore \( \mu(N) < \mu(M) \). Choose \( N' = N \).

Cases \( (tw2.\xi_2) \). One can assume that \( M \) is not in one of the form requested by the previous cases. The induction hypothesis can therefore be applied and the result is obtained directly.

By case exhaustion, the lemma is then true. \( \square \)

**Lemma 10.3.30.** Suppose that \( M \) is an intermediate neutral term. Then either \( M \) is a neutral term or there exists \( N \) such that \( \mu(N) < \mu(M) \) and \( M \rightarrow_2 N \).

**Proof.** From Lemma 10.3.22 every intermediate term satisfies reduction. Then from Lemma 10.3.27 for all intermediate neutral term \( M \), either \( M \) is a neutral term or there exists \( N \) such that \( \mu(N) < \mu(M) \) and \( M \rightarrow_2 N \). \( \square \)

## 10.4 Proof of Theorem 9.2.7

The proof of Theorem 9.2.7 is done in two steps, by reducing first to intermediate neutral terms and then to neutral terms. We make these steps explicit in Lemma 10.3.11 and Lemma 10.3.24.
Lemma 10.4.1. Suppose that $\Delta \triangleright M, N : A$ are two valid typing judgments such that $\text{Erase}(M) = \text{Erase}(N)$. Then there exists two intermediate neutral terms $M'$ and $N'$ such that $\Delta \triangleright M' : A$ and $\Delta \triangleright N' : A$ are valid, such that $\text{Erase}(M') = \text{Erase}(N')$ and such that $\Delta \triangleright M \approx_{ax} M' : A$ and $\Delta \triangleright N \approx_{ax} N' : A$.

Proof. Let $S$ be the set of all possible sequences of terms $(M_i)$, such that $M_0 = 0$ and $M_i \leftarrow M_{i+1}$.

From Lemma 10.2.12 one can define the function $f$ from $S$ to the integers picking out the smallest $n$ such that for all $i > n$, $M_i = M_n$.

Consider the function $g$ mapping a sequence $(M_i)_i$ in $S$ to the value $m(M_f((M_i)_i))$. Since the measure yields non-negative integers, the set $g(S)$ is a subset of the non-negative integers. It contains then an attainable minimal element $m_0$. Let $(M_j)_j$ be a sequence of $S$ such that $g((M_j)_j) = m_0$.

Let $n_0 = f((M_j)_j)$. We claim that $M_{n_0}$ is an intermediate neutral term. Indeed, suppose otherwise. Then by Lemma 10.2.13 there exists a term $M'$ such that $M_{n_0} \rightarrow M'$ and $M' \neq M_{n_0}$. We can now construct a sequence of terms $(M_i)_i$ as follows: $M_i = M_i$ for all $i = 0 \ldots n_0$, $M_i = M'$ for all $i > n_0$. Note that $(M_i)_i$ belongs in $S$. However, using Lemma 10.4.1 we deduce that $g((M_i)_i) < m_0$, contradicting the minimality of $m_0$.

Now, using Lemma 10.2.8 one can construct a sequence of terms $(N_i)_i$ such that $N_0 = N$ and such that for all $i$, $\text{Erase}(N_i) = \text{Erase}(M_i)$ and $N_i \rightarrow N_{i+1}$. Using Lemma 10.2.7 for all $i$ the typing judgments $\Delta \triangleleft M_{n_0}, N_{n_0} : B$ are valid, and $\Delta \triangleright M \approx_{ax} M_{n_0} : B$ and $\Delta \triangleright N \approx_{ax} N_{n_0} : B$. Using Lemma 10.2.7 the term $N_{n_0}$ is in intermediate neutral form. This makes the terms $M' = M_{n_0}$ and $N' = N_{n_0}$ fulfill the requirements of the lemma.

Lemma 10.4.2. Suppose that $\Delta \triangleright M, N : A$ are two valid typing judgments, where $M$ and $N$ are intermediate neutral terms such that $\text{Erase}(M) = \text{Erase}(N)$. Then there exists two neutral terms $M'$ and $N'$ such that $\text{Erase}(M') = \text{Erase}(N')$ and such that $\Delta \triangleright M \approx_{ax} M' : A$ and $\Delta \triangleright N \approx_{ax} N' : A$.

Proof. Consider two valid typing judgments $\Delta \triangleright M, N : A$ such that $M$ and $N$ are intermediate neutral terms with $\text{Erase}(M) = \text{Erase}(N)$.

Using Lemma 10.3.3 it is possible to construct sequences of terms $(M_i)_i$ such that $M_0 = M$, and such that for all $i$, either $M_i$ is a neutral value or $M_i \rightarrow M_{i+1}$ with $\mu(M_{i+1}) < \mu(M_i)$. From Lemma 10.3.28 there exists $n_0$ such that for all $n \geq n_0$, $\mu(M_n) = \mu(M_{n_0})$. Using the definition of the sequence, this means that for all $n \geq n_0$, $M_n = M_{n_0}$ is a neutral term. Using Lemma 10.3.3 one can build a sequence $(N_n)_n$ such that for all $n$, $\text{Erase}(N_n) = \text{Erase}(M_n)$ and such that $N_{n} \rightarrow N_{n+1}$. From Lemma 10.2.7 the typing judgments $\Delta \triangleright M_{n_0}, N_{n_0} : A$ are valid, and $\Delta \triangleright M \approx_{ax} M_{n_0} : A$ and $\Delta \triangleright N \approx_{ax} N_{n_0} : A$.

The requested terms $M'$ and $N'$ can be respectively taken as $M_{n_0}$ and $N_{n_0}$.

We are now ready to prove Theorem 9.2.7.

Proof of Theorem 9.2.7. Suppose that $M$ and $N$ are two terms such that $\text{Erase}(M) = \text{Erase}(N)$ and such that $\Delta \triangleright M, N : A$ are valid typing judgments.

Using Lemma 10.4.1 there exists two intermediate neutral terms $M'$ and $N'$ such that $\Delta \triangleright M', N' : A$ and such that $\Delta \triangleright M \approx_{ax} M' : A$ and $\Delta \triangleright N \approx_{ax} N' : A$ and such that $\text{Erase}(M') = \text{Erase}(N')$. Using Lemma 10.4.1 there exists two neutral terms $M''$ and $N''$ such that $\text{Erase}(M'') = \text{Erase}(N'')$ and such that $\Delta \triangleright M'' \approx_{ax} M' : A$ and $\Delta \triangleright N'' \approx_{ax} N' : A$. Using Lemma 10.4.1 we have $\Delta \triangleright M'' \approx_{ax} N'' : A$.

We obtain $\Delta \triangleright M \approx_{ax} N : A$ using the transitivity of the axiomatic relation.
Chapter 11

Categorical Semantics

In Chapter 8 we described the categorical structure believed to be required for interpreting the language described in Chapter 9. In this chapter, we show that one can indeed interpret the language in a linear category for duplication, and we prove a soundness and completeness result.

11.1 Denotational Semantics

The ambient category this section is concerned with is a linear category for duplication $\mathcal{C}$, with the notation of Definition 8.4.1.

Convention 11.1.1. For notation purposes, we assume the category to be strict monoidal. This can be safely assumed, thanks to Theorem 2.8.2.

11.1.1 Interpretation of the Type System

Definition 11.1.2. We define an interpretation of the type system to be a map $\Theta$ that assigns to each constant type $\alpha$ an object $\Theta(\alpha)$. Each type $A$ is interpreted as an object of $\mathcal{C}$:

\[
[\alpha]_{\Theta} = \Theta(\alpha), \quad [\top]_{\Theta} = \top, \\
[!A]_{\Theta} = L[A]_{\Theta}, \quad [A \otimes B]_{\Theta} = [A]_{\Theta} \otimes [B]_{\Theta}, \quad [A \multimap B]_{\Theta} = [A]_{\Theta} \multimap [B]_{\Theta}.
\]

Consider the alphabet $\{\alpha \mid \alpha$ is a constant type\}, and the set $\mathcal{A}$ of types. If $G(A) = [A]_{\Theta}$, we are in the context of Theorem S.3.8, with the list of $F_i$’s being $(\otimes, \multimap)$: any two maps $A \rightarrow B$ in $\mathcal{C}^G$ are equal.

Definition 11.1.3. Given a valid subtyping $A <: B$, there exists a unique arrow $[A]_{\Theta} \rightarrow [B]_{\Theta}$ in $\mathcal{C}^G$, as defined in Theorem S.3.8. We extend the map $\Theta$ to interpret $A <: B$ as this unique arrow and we denote it by $I_{A,B}$.

11.1.2 Interpretation of the Language

Convention 11.1.4. Typing contexts were defined as sets. In the case we are interested in, we need them to be lists. We will therefore consider them to be lists in this section, the typing rules of Table 9.1 being physically unchanged. In order to still be able to reorder typing contexts, we add a set of new rules $(X_s)$, one for each permutation $s$ on $\{1, \ldots, n\}$:

\[
\frac{x_1 : A_1, \ldots, x_n : A_n \triangleright M : A}{x_{s(1)} : A_{s(1)}, \ldots, x_{s(n)} : A_{s(n)} \triangleright M : A} \quad (X_s)
\]
Definition 11.1.5. We define the denotation of a typing context \( \Delta = (x_1 : A_1, \ldots, x_n : A_n) \) by the following:

\[
[\Delta] = [A_1] \otimes \cdots \otimes [A_n].
\]

Definition 11.1.6. We use the following shortcut definitions, where \( A, B, A_1, \ldots, A_n \) are types and where \( \Delta, \Gamma \) and \( \Gamma_1 \) and \( \Gamma_2 \) are typing contexts:

- Given a natural transformation \( n : F \to G \), we write \( n_A \) in place of \( n_{[A]} \). If \( \Delta = \{x_1 : A_1, \ldots, x_n : A_n\} \) we define \( n_\Delta = n_{A_1} \otimes \cdots \otimes n_{A_n} \).
- For the coherence map \( d^L_{A,B} : LA \otimes LB \to L(A \otimes B) \), if \( \Delta = \{x_1 : A_1, \ldots, x_n : A_n\} \), we define \( d^L_\Delta \) to be the map

\[
L[A_1] \otimes \cdots \otimes L[A_n] \xrightarrow{id \otimes d^L_{[A_{n-1}], [A_n]}} L[A_1] \otimes \cdots \otimes L[A_{n-1} \otimes A_n] \xrightarrow{\sim} L[A_1 \otimes \cdots \otimes A_n].
\]

- We define \( \text{Split}_{\Delta, \Gamma_1, \Gamma_2} \) to be the canonical map from the monoidal structure and using the map \( \Delta_\Lambda : LA \to LA \otimes LA \) from Definition 11.1.6.

\[
\text{Split}_{\Delta, \Gamma_1, \Gamma_2} : \llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_1 \rrbracket] \otimes [\llbracket \Gamma_2 \rrbracket] \to [\llbracket \Delta \rrbracket] \otimes [\llbracket \Gamma_1 \rrbracket] \otimes [\llbracket \Delta \rrbracket] \otimes [\llbracket \Gamma_2 \rrbracket].
\]

- Given \( f : \llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_1 \rrbracket] \to [\llbracket A \rrbracket] \) and \( g : \llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_2 \rrbracket] \to [\llbracket B \rrbracket] \), we define the map \( f \otimes_{\Delta} g : \llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_1 \rrbracket] \otimes [\llbracket \Gamma_2 \rrbracket] \to [\llbracket A \rrbracket] \otimes [\llbracket B \rrbracket] \) as follows:

\[
\llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_1 \rrbracket] \otimes [\llbracket \Gamma_2 \rrbracket] \xrightarrow{\text{Split}_{\Delta, \Gamma_1, \Gamma_2}} \llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_1 \rrbracket] \otimes \llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_2 \rrbracket] \xrightarrow{f \otimes g} [\llbracket A \rrbracket] \otimes [\llbracket B \rrbracket].
\]

Lemma 11.1.7. Suppose that \( f : \llbracket \Delta, \Gamma_2 \rrbracket \to [\llbracket A \rrbracket] \). Suppose that \( \Gamma_1 \) is a context of fresh variables. Then

\[
\text{Split}_{\Delta, \Gamma_1, \Gamma_2} (\hat{\Diamond}_{\Delta, \Gamma_1} \otimes f) = (\sigma_{\llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_1 \rrbracket]} \otimes id_{\Gamma_2}) (\hat{\Diamond}_{\Delta, \Gamma_1} \otimes f) : \llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_1 \rrbracket] \to [\llbracket A \rrbracket].
\]

Proof. Using the equations of comonoids. \( \square \)

Lemma 11.1.8. Suppose that \( f : \llbracket \Delta, \Gamma_1 \rrbracket \to [\llbracket A \rrbracket] \) and that \( g : \llbracket \Delta, \Gamma_2 \rrbracket \to [\llbracket B \rrbracket] \). Suppose moreover that \( \llbracket A \rrbracket \) is a context of fresh variables. Then

\[
(\hat{\Diamond}_{\Delta} \otimes f) \otimes_{\Delta, \Gamma_1} (\hat{\Diamond}_{\Delta} \otimes g) = \hat{\Diamond}_{\Delta} \otimes (f \otimes_{\Delta} g) : \llbracket \Delta \rrbracket \otimes [\llbracket \Gamma_1 \rrbracket] \to [\llbracket A \rrbracket] \otimes [\llbracket B \rrbracket].
\]

Proof. It is enough to show that the maps

\[
\llbracket \Delta, \Gamma_1, \Gamma_2 \rrbracket \xrightarrow{\text{Split}_{\Delta, \Gamma_1, \Gamma_2}} \llbracket \Delta, \Gamma_1, \Gamma_1, \Delta, \Gamma_1, \Gamma_2 \rrbracket \xrightarrow{\hat{\Diamond}_{\Delta} \otimes f \otimes_{\Delta} g} [A_1] \otimes [A_2]
\]

and

\[
\llbracket \Delta, \Gamma_1, \Gamma_2 \rrbracket \xrightarrow{\hat{\Diamond}_{\Delta} \otimes id} \llbracket \Delta, \Gamma_1, \Gamma_2 \rrbracket \xrightarrow{\text{Split}_{\Delta, \Gamma_1, \Gamma_2}} \llbracket \Delta, \Gamma_1, \Delta, \Gamma_2 \rrbracket \xrightarrow{f \otimes g} [A_1] \otimes [A_2]
\]

are equal. This is done using the comonoid structure of \( (\llbracket A \rrbracket, \Delta_\Lambda, \hat{\Diamond}_\Lambda) \). \( \square \)

Lemma 11.1.9. Suppose that \( f : \llbracket A, \Delta, \Gamma_1 \rrbracket \to [\llbracket A \rrbracket] \) and that \( g : \llbracket \Delta, \Gamma_2 \rrbracket \to [\llbracket B \rrbracket] \). Then,

\[
f \otimes_{\Delta, \Gamma_1} (\hat{\Diamond}_{\Delta} \otimes g) = (id_{\Delta} \otimes \text{Split}_{\Delta, \Gamma_1, \Gamma_2}) (f \otimes g) : \llbracket A, \Delta, \Gamma_1, \Gamma_2 \rrbracket \to [\llbracket A \rrbracket] \otimes [\llbracket B \rrbracket].
\]

Proof. Proof using the comonoid structure of \( (\llbracket A \rrbracket, \Delta_\Lambda, \hat{\Diamond}_\Lambda) \). \( \square \)
Lemma 11.1.10. Suppose that $f : [\Gamma_1] \to [A]$ and that $g : [A] \to [B]$. Then, if $\Delta$ is a context of fresh variables,
\[
(\Diamond_{\Delta} \otimes f); g \equiv (\Diamond_{\Delta} \otimes (f; g)) : [\Delta, \Gamma_1] \to [B].
\]

Proof. In our strict monoidal category, the map $(\Diamond_{\Delta} \otimes f); g$ is
\[
(\Diamond_{\Delta} \otimes f); g = (\Diamond_{\Delta} \otimes f); \lambda_A; g
\]
\[
= (\Diamond_{\Delta} \otimes f); (id_{\Delta} \otimes g); \lambda_B
\]
by naturality of $\lambda$,
\[
= (\Diamond_{\Delta} \otimes (f; g)); \lambda_B
\]
by bifunctoriality of $\otimes$.

And this map is precisely $\Diamond_{\Delta} \otimes (f; g)$. \qed

Lemma 11.1.11. Suppose that $f : [\Delta, \Gamma_1] \to [A]$, $g : [\Delta, \Gamma_2] \to [B]$, $h : [A] \to [C]$ and $k : [B] \to [D]$. Then
\[
(f; h) \otimes_{\Delta, \Gamma_1, \Gamma_2} (g; k) = (f \otimes_{\Delta, \Gamma_1, \Gamma_2} g; (h \otimes k)) : [\Delta, \Gamma_1, \Gamma_2] \to [C] \otimes [D].
\]

Proof. The proof uses the bifunctoriality of $\otimes$. \qed

Lemma 11.1.12. Suppose that $f : [\Delta, \Gamma_1] \to [A]$, $g : [\Delta, \Gamma_2] \to [B]$. Then
\[
(f \otimes_{\Delta} g); \sigma_{A,B} = (id_{\Delta} \otimes \sigma_{[f],[g]}); (g \otimes_{\Delta} f) : [\Delta, \Gamma_1, \Gamma_2] \to [B \otimes A].
\]

Proof. The proof is done using the correspondence between the symmetry and the comonoid multiplication. \qed

Definition 11.1.13. The map $\Theta$ as in Definition 11.1.2 is said to be an interpretation of the language if moreover it assigns to each constant term $c : !A_c$ an arrow $\Theta(c) : \top \to [!A_c]$ in $\mathcal{C}$.

Given a linear category for duplication $\mathcal{C}$, it is possible to interpret the typing derivation of a well-typed value as a map in $\mathcal{C}$ and the typing derivation of a valid computation as a map in the Kleisli category $\mathcal{C}_T$.

- If $x_1 : A_1, \ldots, x_n : A_n \triangleright V : B$ is a value with typing derivation $\pi$, its value interpretation $[\pi]^v_\Theta$ is an arrow $[A_1] \otimes \ldots \otimes [A_n] \to \mathcal{C} [B]$;
- If $x_1 : A_1, \ldots, x_n : A_n \triangleright M : A$ is a term with typing derivation $\pi$, its computational interpretation $[\pi]^c_\Theta$ is an arrow $[A_1] \otimes \ldots \otimes [A_n] \to \mathcal{C} T([B])$.

We define them inductively in Tables 11.1, 11.2 and 11.3. Moreover, considering Convention 11.1.4 if $s$ is a permutation on $\{1, \ldots, n\}$:
\[
[x_{s(1)} : A_{s(1)}, \ldots, x_{s(n)} : A_{s(n)} \triangleright M : A]^c =
\sigma_{[A_1, \ldots, A_n], [A_{s(1)}, \ldots, A_{s(n)}]}; [x_1 : A_1, \ldots, x_n : A_n \triangleright M : A]^c,
\]
\[
[x_{s(1)} : A_{s(1)}, \ldots, x_{s(n)} : A_{s(n)} \triangleright M : A]^v =
\sigma_{[A_1, \ldots, A_n], [A_{s(1)}, \ldots, A_{s(n)}]}; [x_1 : A_1, \ldots, x_n : A_n \triangleright M : A]^v.
\]

Convention 11.1.14. We say that two morphisms
\[
f : [f_1 : A_1, \ldots, x_n : A_n] \to [A], \quad g : [x_{s(1)} : A_{s(1)}, \ldots, x_{s(n)} : A_{s(n)}] \to [A]
\]
are equal whenever $f = \sigma_{[A_1, \ldots, A_n], [A_{s(1)}, \ldots, A_{s(n)}]}; g$. \qed
Lemma 11.1.15. Suppose that

\[ f = [!\Delta, \Gamma_1 \triangleright N : A]^c, \quad g = [!\Delta, \Gamma_2, x : A \triangleright P : B]^c. \]

Then

\[ [!\Delta, \Gamma_1, \Gamma_2 \triangleright \text{let } x^A = N \text{ in } P : B]^c = (f \otimes \Delta \text{id}); \sigma; t; g^c. \]

Proof. The proof is done by computing \([!\Delta, \Gamma_1, \Gamma_2 \triangleright (\lambda^0 x^A. P) N : B]^c\). □

Lemma 11.1.16. Given a valid typing judgement \(\Delta \triangleright M : B\) with no dummy variables, there exists \(f_c : [\Delta] \rightarrow [B]\) such that for any dummy context \(!\Lambda\) and for any typing derivation \(\pi\) of \(!\Lambda, \Delta \triangleright M : B\),

\[ [\pi]^c = [!\Lambda] \otimes [\Delta] \xrightarrow{\odot_{!\Lambda} \otimes f_c} T[B]. \]

Moreover, if \(M = V\) is a value, there exists some \(f_c : [\Delta] \rightarrow [B]\) such that for any dummy context \(!\Lambda\) and for any typing derivation \(\pi\) of \(!\Lambda, \Delta \triangleright V : B\),

\[ [\pi]^c = [!\Lambda] \otimes [\Delta] \xrightarrow{\odot_{!\Lambda} \otimes f_c} [B]. \]

Proof. Consider a typing judgement \(\Delta \triangleright M : A\) where \(|\Delta| = \text{FV}(M)\). We prove the lemma by structural induction on \(M\).

Case \(M \equiv \lambda^0 x^B. N\). In this case, \(A = B \rightarrow C\), and if \(\Delta \triangleright \lambda^0 x^B. N : B \rightarrow C\) is valid, then so is \(\Delta, x : B \triangleright N : C\). By hypothesis, \(|\Delta| = \text{FV}(M)\). Thus \(|\Delta| = \text{FV}(N) \setminus \{x\}\).

Let \(\hat{\Delta}\) be the subcontext of \((\Delta, x : B)\) consisting of the free variables of \(N\).

The induction hypothesis states that there exists a function \(f_c : [\hat{\Delta}] \rightarrow [T[C]]\) such that for all dummy typing contexts \(!\Lambda\) and for all typing derivations \(\pi'\) the denotation \([\pi']^c\) is \(\odot_{!\Lambda} \otimes f_c\).

There are two cases.

If \(x \in \text{FV}(N)\). Then \(|\hat{\Delta}| = |\Delta, x : B|\). We define the required \(f_c\) and \(f_c\) respectively by \(\Phi^{-1}(f_c')\) and \(\Phi^{-1}(f_c'); \eta_{B \rightarrow C}\).

If \(x \notin \text{FV}(N)\). In this case, from Lemma 9.1.19 the type \(B\) is of the form \(!\hat{B}\). The context \(|\hat{\Delta}| = |\Delta|\), and \(x\) is a dummy variable. We define the required \(f_c\) and \(f_c\) respectively by \(\Phi^{-1}(\odot_{!\hat{B}} \otimes f_c')\) and \(\Phi^{-1}(\odot_{!\hat{B}} \otimes f_c'); \eta_{B \rightarrow C}\).
Consider a dummy context $!\Lambda$ for $M$ and a typing derivation $\pi$ of $!\Lambda, \Delta \triangleright M : A$. It starts with

$$
\pi' : \frac{!\Lambda, \Delta, x : B \triangleright N : C}{!\Lambda, \Delta \triangleright \lambda^0x^B. N : B \rightarrow C} \quad (\alpha_1)
$$

for some derivation $\pi'$. By definition,

$$
[\pi']^\circ = \Phi^{-1}([\pi']^\circ) \quad [\pi']^\circ = \Phi^{-1}([\pi']^\circ) ; \eta_{B \rightarrow C}.
$$

We aim at showing that $[\pi']^{\circ \circ} = \diamond_1A \otimes f_c$ and that $[\pi']^{\circ \circ} = \diamond_1A \otimes f_c$.

There are two cases.

**If** $x \in FV(N)$. By induction hypothesis, $[\pi']^{\circ \circ} = \diamond_1A \otimes f'_c$. By naturality of $\Phi$,

$$
[\pi']^{\circ \circ} = \Phi^{-1}(\diamond_1A \otimes f'_c) ; \eta_{B \rightarrow C} = \diamond_1A \otimes \Phi^{-1}(f'_c) ; \eta_{B \rightarrow C},
$$

$$
[\pi']^{\circ \circ} = \Phi^{-1}(\diamond_1A \otimes f'_c) = \diamond_1A \otimes \Phi^{-1}(f'_c).
$$

**If** $x \notin FV(N)$. By induction hypothesis, $[\pi']^{\circ \circ} = \diamond_1A \diamond_1B \diamond f'_c$. By naturality of $\Phi$,

$$
[\pi']^{\circ \circ} = \Phi^{-1}(\diamond_1A \diamond_1B \diamond f'_c) ; \eta_{B \rightarrow C} = \diamond_1A \diamond_1B \diamond f'_c ; \eta_{B \rightarrow C},
$$

$$
[\pi']^{\circ \circ} = \Phi^{-1}(\diamond_1A \diamond_1B \diamond f'_c) = \diamond_1A \diamond_1B \diamond f'_c.
$$
11.1. Denotational Semantics

First, if $U$ is a core value, $[\Delta \triangleright U : A]_\Theta^e = [\Delta \triangleright U : A]_\Theta^e; \eta_A$.

$[[\Delta, \Gamma_1 \triangleright M : A \rightarrow B]]_\Theta^e = [[\Delta, \Gamma_1] \rightarrow T([A \rightarrow B])]$

$[[\Delta, \Gamma_2 \triangleright N : A]]_\Theta^e = [[\Delta, \Gamma_2] \rightarrow T([A])$

$[\Delta, \Gamma_1, \Gamma_2 \triangleright MN : B]_\Theta^e = [[\Delta, \Gamma_1, \Gamma_2] \rightarrow T([A \rightarrow B]) \otimes T[A]]$

$\Psi_i \rightarrow T[[A \rightarrow B] \otimes A] \overset{\varepsilon_{\Theta, B}^n}{\rightarrow} T[B]$

$[[\Delta, \Gamma_1 \triangleright M : !^n(A_1 \otimes A_2)]_\Theta^e = [[\Delta, \Gamma_1] \rightarrow TL^n[A_1 \otimes A_2]$

$[[\Delta, \Gamma_2, x : !^m A_1, y : !^m A_2 \triangleright N : C]_\Theta^e = [[\Delta, \Gamma_2] \otimes L^n[A_1] \otimes L^n[A_2] \rightarrow T[C]$

$[[\Delta, \Gamma_1, \Gamma_2 \triangleright \text{let } * = M \text{ in } N : C]_\Theta^e =$

$\frac{f_{\Theta n} \rightarrow T(L^n[A_1] \otimes L^n[A_2]) \rightarrow T[C] \Psi_i \rightarrow T[C]}{[\Delta, \Gamma_1 \triangleright M : T^n]_\Theta^e = [[\Delta, \Gamma_1] \rightarrow T(T)}$

$[[\Delta, \Gamma_1 \triangleright N : C]_\Theta^e = [[\Delta, \Gamma_2] \rightarrow T[C]$

$[[\Delta, \Gamma_1, \Gamma_2 \triangleright \text{let } * = M \text{ in } N : C]_\Theta^e =$

$\frac{f_{\Theta n} \rightarrow T(L^n[A_1] \otimes L^n[A_2]) \rightarrow T[C] \Psi_i \rightarrow T[C]}{[\Delta, \Gamma_1 \triangleright M : !^n A]_\Theta^e = [[\Delta, \Gamma_1] \rightarrow TL^n[A]$

$[[\Delta, \Gamma_2 \triangleright N : !^n B]_\Theta^e = [[\Delta, \Gamma_2] \rightarrow TL^n[B]$

$[[\Delta, \Gamma_1, \Gamma_2 \triangleright (M, N) : !^n(A \otimes B)]_\Theta^e =$

$\frac{f_{\Theta n} \rightarrow TL^n[A] \otimes TL^n[B] \rightarrow TL^n[A \otimes B] \Psi_i : TL^n[A \otimes B]}{[\Delta, \Gamma_1, \Gamma_2 \triangleright (M, N) : !^n(A \otimes B)]_\Theta^e}$

Table 11.3: Interpretation of computations.

Case $M \equiv \lambda^n x^{m+1} B \cdot N$. In this case, $A = !^n x^{m+1} B \cdot N : B \rightarrow C$ is valid, then so is $\Delta, x : B \triangleright N : C$. By hypothesis, $[\Delta] = TV(M)$. Thus $[\Delta] = TV(N) \setminus \{x\}$.

Let $\Delta$ be the subcontext of $(x : B, \Delta)$ consisting of the free variables of $N$.

The induction hypothesis states that there exists a function $f'_e : [\Delta] \rightarrow T[C]$ such that for all dummy typing contexts $!^n \Gamma$ and for all typing derivations $\pi'$ the denotation $[\pi']^e$ is $\hat{\Delta} \otimes f_c$.

Note that $\Delta$ is of the form $\hat{\Delta}$. There are two cases.

If $x \in TV(N)$. Then $[\Delta] = [x : B, \Delta]$. We define the requested $f_v$ and $f_c$ respectively by

$f_v = \delta_\Delta ; d_{\Gamma_2}^L ; L \Phi^{-1}(f'_e) ; I_{((B \rightarrow C) \cdot !^n x^{m+1} B \rightarrow C)}$

$f_c = \delta_\Delta ; d_{\Gamma_2}^L ; L \Phi^{-1}(f'_e) ; I_{((B \rightarrow C) \cdot !^n x^{m+1} B \rightarrow C) ; \eta_{n+1}(B \rightarrow C)}$

If $x \not\in TV(N)$. In this case, from Lemma 11.1.9 the type $B$ is of the form $!^n \hat{B}$. The context $[\Delta] = [\Delta]$ and $x$ is a dummy variable. We define the requested $f_v$ and $f_c$ respectively by

$f_v = \delta_\Delta ; d_{\Gamma_2}^L ; L \Phi^{-1}(\hat{\Delta} \otimes f'_e) ; I_{((B \rightarrow C) \cdot !^n \hat{B} \rightarrow C)}$

$f_c = \delta_\Delta ; d_{\Gamma_2}^L ; L \Phi^{-1}(\hat{\Delta} \otimes f'_e) ; I_{((B \rightarrow C) \cdot !^n \hat{B} \rightarrow C) ; \eta_{n+1}(B \rightarrow C)}$
Consider a dummy context $!\Lambda$ for $M$ and a typing derivation $\pi$ of $!\Lambda, \Delta \triangleright M : A$. It starts with

$$
!\Lambda, \Delta, x : B \triangleright N : C
$$

for some derivation $\pi'$. By definition,

$$
[\pi]^v = \delta_{!\Lambda,\Delta}; d^L_{!\Lambda,\Delta}; L\Phi^{-1}(\delta_{!\Lambda,\Delta}; f^v) ; I_{L(B \rightarrow C),!\Lambda} ,\Pi_{n+1(B \rightarrow C)}.
$$

$$
[\pi]^c = \delta_{!\Lambda,\Delta}; d^L_{!\Lambda,\Delta}; L\Phi^{-1}(\delta_{!\Lambda,\Delta}; f^c) ; I_{L(B \rightarrow C),!\Lambda} ,\Pi_{n+1(B \rightarrow C)}.
$$

We aim at showing that $[\pi]^v = \diamond !\Lambda \otimes f_v$ and that $[\pi]^c = \diamond !\Lambda \otimes f_c$.

One can show that for all $g : [\Delta] \rightarrow [D]$, $\delta_{!\Lambda,\Delta}; d^L_{!\Lambda,\Delta}; L(\diamond !\Lambda \otimes id_{\Delta}); (L(id_T \otimes g) = \diamond !\Lambda \otimes (\delta_{!\Lambda,\Delta}; d^L_{!\Lambda,\Delta}; L(id_{\Delta}; Lg))$  \hspace{1cm} (11.1.1)

by using the monoidality of $d^L$ and $\delta$, and by using the fact that the category is strict. There are two cases.

If $x \in FV(N)$. By induction hypothesis, $[\pi]^v = \diamond !\Lambda \otimes f_v$. By naturality of $\Phi$, $\Phi^{-1}(\diamond !\Lambda \otimes f_v) = \diamond !\Lambda \otimes \Phi^{-1}(f_v)$. One can then conclude, by using the functoriality of $L$ and $\otimes$ and replacing $g$ with $\Phi^{-1}(f_v')$ in Equation \ref{eq:11.1.1}

If $x \notin FV(N)$. By induction hypothesis, $[\pi]^c = \diamond !\Lambda \otimes f_c$.

By naturality of $\Phi$, $\Phi^{-1}(\diamond !\Lambda \otimes \diamond !\Lambda \otimes f_v) = \diamond !\Lambda \otimes \Phi^{-1}(\diamond !\Lambda \otimes f_v')$. One can then conclude, by using the functoriality of $L$ and $\otimes$ and replacing $g$ with $\Phi^{-1}(\diamond !\Lambda \otimes f_v')$ in Equation \ref{eq:11.1.1}

Case $M \equiv NP$. In this case, one can split $\Delta$ into $(!\Delta', \Gamma_1, \Gamma_2)$, where $\Gamma_1$ consists of all the free variables in $N$ but not in $P$, $\Gamma_2$ of all the free variables in $P$ but not in $N$, and $!\Delta$ of all the free variables both in $N$ and in $P$. Note that these are the only possibilities, since $\Delta$ does not contain any dummy variables.

Using Lemma \ref{lem:split}. If $\Delta \triangleright NP : A$, then there exists some $B$ such that $!\Delta, \Gamma_1 \triangleright N : B \rightarrow A$ and $!\Delta, \Gamma_2 \triangleright P : B$.

By induction hypothesis, there exists $f'_v : [[!\Delta]] \otimes [\Gamma_1] \rightarrow T[B \rightarrow A]$ such that for all dummy contexts $!\Lambda$ for $N$ and for all typing derivations $\pi_1$ for $!\Lambda, !\Delta, \Gamma_1 \triangleright N : B \rightarrow A$ the denotation $[\pi_1]^v = \diamond !\Lambda \otimes f'_v$.

Similarly, by induction hypothesis, there exists $g'_c : [[!\Delta]] \otimes [\Gamma_2] \rightarrow T[B]$ such that for all dummy contexts $!\Lambda$ for $P$ and for all typing derivations $\pi_2$ for $!\Lambda, !\Delta, \Gamma_2 \triangleright P : B$ the denotation $[\pi_2]^c = \diamond !\Lambda \otimes g'_c$.

Let $f_c$ be the map

$$
[[!\Delta]] \otimes [\Gamma_1] \otimes [\Gamma_2] \xrightarrow{\lambda^L_{!\Lambda,\Delta}; f'_v} T[B \rightarrow A] \otimes T[B] \xrightarrow{\Phi^{-1}} T[\mu_{!\Lambda,\Delta}; T[B \rightarrow A] \otimes T[B]] \xrightarrow{\varepsilon_{\lambda^L_{!\Lambda,\Delta}; f'_v}} T[A].
$$

Consider a dummy context $!\Lambda$ for $NP$ and a valid derivation $\pi$ for $!\Lambda, \Delta \triangleright NP : A$. This derivation starts with

$$
\pi_1 \vdash \pi_2
$$

$!\Delta, \Gamma_1 \triangleright N : B' \rightarrow A$ $!\Delta, \Gamma_2 \triangleright P : B'$ (app)
The remaining cases are handled similarly. From Lemma 11.1.12 \( B' = B \). From Lemma 11.1.11 we have \(|Δ| \leq |Δ|, |Γ_1| \leq |Δ, Γ_1|\) and \(|Γ_2| \leq |Δ, Γ_2|\). Let us split \(!Δ, Γ_1, Γ_2\) into
\[ !Δ = (!Δ dnp, !Δ dnp, !Δ dnp), \]
\[ Γ_1 = (Γ_1 dnp, Γ_1 dnp), \]
\[ Γ_2 = (Γ_2 dnp, Γ_2 dnp), \]
where for each context of the form \( X dY_1, ..., Z_i, \) if \( x \in |X dY_1, ..., Z_i| \), then \( x \in FV(Z_1) \cap \cdots \cap FV(Z_i) \) but \( x \notin FV(Y_1) \cup \cdots \cup FV(Y_k) \). We did not include the four contexts \( !Δ dnp, Γ_1 dnp, Γ_2 dnp, \) which are empty by definition: otherwise the context \( (Δ, Γ_1, Γ_2) \) would have duplicates. We can rewrite the following contexts:
\[ !Δ = (!Δ dnp, !Δ dnp, !Δ dnp), \]
\[ !Δ = !Δ dnp, \]
\[ !Δ = !Δ dnp, \]
\[ !Δ = !Δ dnp, \]
\[ !Δ = !Δ dnp, \]
\[ !Δ = !Δ dnp, \]
Note that \( !Δ dnp, Γ_1 dnp, Γ_2 dnp \), are duplicable.
By definition, \( [π]^c = \( [π_1]^c \otimes ![Δ]^c \) \); \( Ψ_1; ε_A B \). We want to show that \( [π]^c = \Diamond A ⊗ f_c \). We have from the induction hypothesis that if \( f^c_0 \) is the morphism \( !Δ dnp, !Δ dnp, Γ_1 dnp, Γ_2 dnp \), then \( [π_1]^c \) and \( [π_2]^c \) are respectively \( f^c_0 \otimes f_c^0 \) and \( g^c_0 \otimes g_c^0 \), and
\[
\begin{align*}
\Diamond_A = & \Diamond_A dnp, \Diamond_A dnp, \Diamond_A dnp, \varepsilon_A B, \\
\Diamond_A = & \Diamond_A dnp, \varepsilon_A B, \\
\Diamond_A = & \Diamond_A dnp, \varepsilon_A B, \\
\Diamond_A = & \Diamond_A dnp, \varepsilon_A B.
\end{align*}
\]
Now, since from Lemma 11.1.13 and Lemma 11.1.14
\[
(\Diamond_A dnp, \Diamond_A dnp, \Diamond_A dnp, \varepsilon_A B)
\]
the denotation \( [π]^c \) is then equal to
\[
[π]^c = \left( \Diamond_A dnp, \Diamond_A dnp, \Diamond_A dnp, \varepsilon_A B \right) ; Ψ_1; ε_A B
\]
\[
= (\Diamond_A ⊗ (f^c_0 ⊗ g^c_0)); Ψ_1; ε_A B.
\]
One concludes using Lemma 11.1.10.

The remaining cases are handled similarly.

Theorem 11.1.17. Given a valid typing judgement \( Δ \triangleright M : B \) with two typing derivations \( π \) and \( π' \), for any interpretation \( Θ \) we have \([π]^v = [π']^v \) if \( M \) is a value.

Proof. We consider denotations with respect to \( Θ \). The context \( Δ \) splits into \( |Δ|, |Δ, Γ_1|\), where \( |Δ| \) is a dummy context and where \( |Δ| = FV(M) \).

From Lemma 11.1.11 \( Δ \triangleright M : A \) is valid. We are in the context of Lemma 11.1.11 there exists a function \( f_c : |Δ| → T[A] \) such that \( [π]^c \) and \( [π]'^c \) are both equal to \( \Diamond_A ⊗ f_c \). If \( M \) is a value, then there exists a function \( f_v : |Δ| → [A] \) such that \( [π]^v \) and \( [π]'^v \) are both equal to \( \Diamond_A ⊗ f_v \).
11.2. Soundness of the Denotation

Definition 11.1.18. Given a interpretation Θ of the language in a category C, we define the denotation of a valid typing judgement Δ ⊢ M : A with typing derivation π to be $[\Delta \vdash M : A]^{\Theta} = [\pi]^{\Theta}$ and $[\Delta \vdash M : A]^{\Theta} = [\pi]^{\Theta}$ if M is a value.

Remark 11.1.19. From Theorem 11.1.17, Definition 11.1.18 is valid.

11.2 Soundness of the Denotation

The axiomatic equivalence and the categorical semantics are two faces of the same coin. Indeed, as we will prove in this section, two terms in the same axiomatic equivalence class have the same denotation. A corollary is that the indexation of terms does not influence the denotation. This proves semantically the fact that it is safe to work with untyped terms. An alternate justification of this fact is of course the operational semantics, which was given in Section 6.

Lemma 11.2.1. Suppose that $\Delta' \prec: \Delta$ and that $\Delta \vdash M : A$. Then

$$[\Delta' \vdash M : A]^{\Theta} = I_{\Delta', \Delta}; [\Delta \vdash M : A']^{\Theta}. $$

If M = V is a value, we have moreover

$$[\Delta' \vdash V : A]^{\Theta} = I_{\Delta', \Delta}; [\Delta \vdash V : A']^{\Theta}. $$

Proof. Proof by induction on the size of M. □

Lemma 11.2.2. Suppose that $\Delta \vdash M : A$ and that $A <: A'$. Then

$$[\Delta \vdash \{ M <: A' \} : A']^{\Theta} = [\Delta \vdash M : A]^{\Theta}; T(I_{A, A'}).$$

If M = V is a value, from Lemma 9.1.27, $\{ V <: A' \}$ is a value. Then

$$[\Delta \vdash \{ V <: A' \} : A']^{\Theta} = [\Delta \vdash V : A']^{\Theta}; I_{A, A'}.$$  

Proof. Proof by induction on the size of M. □

Lemma 11.2.3. Suppose that $\Delta \vdash M : A$ is a valid typing judgement and that $!\Lambda$ is a context of dummy variables for M. Then

$$[!\Lambda, \Delta \vdash M : A]^{\Theta} = \Diamond_{\Lambda} \otimes [\Delta \vdash M : A]^{\Theta}. $$

If M = V is a value,

$$[!\Lambda, \Delta \vdash V : A]^{\Theta} = \Diamond_{\Lambda} \otimes [\Delta \vdash V : A]^{\Theta}. $$

Proof. Proof by induction on the size of M. □

Lemma 11.2.4 (Substitution). Given two valid typing judgements $!\Delta, \Gamma_1, x : A \vdash M : B$ and $!\Delta, \Gamma_2 \vdash V : A$, the typing judgement $!\Delta, \Gamma_1, \Gamma_2 \vdash M[V/x] : B$ is valid. Let h be the denotation $[[\Delta, \Gamma_1, \Gamma_2 \vdash M[V/x] : B]^{\Theta}$ and h′ be $[[\Delta, \Gamma_1, \Gamma_2 \vdash W[V/x] : B]^{\Theta}$, in the case where M = W is a value. Then they are defined by

$$[!\Delta] \otimes [\Gamma_1] \otimes [\Gamma_2] \xrightarrow{\text{Split}_{\Delta, \Gamma_1, \Gamma_2}} [[\Delta, \Gamma_1, x : A \vdash M : B]^{\Theta}$$

$$[[\Delta] \otimes [\Gamma_1] \otimes [\Delta] \otimes [\Gamma_2] \xrightarrow{\text{id} \otimes [[\Delta, \Gamma_2 \vdash V : A]^{\Theta}} [[\Delta] \otimes [\Gamma_1] \otimes [A],$$

(11.2.1)
11.2. Soundness of the Denotation

\[ [\Delta] \otimes [\Gamma_1] \otimes [\Gamma_2] \overset{h'}{\longrightarrow} [B] \]

(11.2.2)

\[ [\Delta] \otimes [\Gamma_1] \otimes [\Gamma_2] \overset{id \otimes [\Delta, \Gamma_2 \triangleright V : A]^{\diamond}}{\longrightarrow} [\Delta] \otimes [\Gamma_1] \otimes [A]. \]

Proof. Let \( v \) be the map \([\Delta, \Gamma_2 \triangleright V : A]^{\diamond}\). We do the proof by induction on the size of \( M \).

Cases where \( M \) is a core value. Case \( M \equiv x^B \). The term \( M \) is a core value: we have to show Equation (11.2.1) and Equation (11.2.2). We show the former, the latter being exactly similar.

The typing derivation \( !\Delta, \Gamma_1, x : A \triangleright x^B : B \) comes from typing rule \((ax_1)\). This means that \( \Gamma_1 \) is of the form \( !\Gamma_1 \), and that \( A < : B \). Using Lemma (11.2.2), the map \( h \) is

\[ h = [\Delta, !\Gamma'_1, \Gamma_2 \triangleright \{V < : B\} : B]^{\diamond} = [\Delta, !\Gamma'_1, \Gamma_2 \triangleright V : A]^{\diamond}; T(I_{A,B}). \]

Since \( V \) is a core value and using Lemma (11.2.3) and (11.2.4)

\[ h = [\Delta, !\Gamma'_1, \Gamma_2 \triangleright V : A]^{\diamond}; \eta_A; T(I_{A,B}) \]

\[ = Split_{\Delta, !\Gamma'_1, \Gamma_2}([[\Delta, \Gamma_2 \triangleright V : A]^{\diamond}); \eta_A; T(I_{A,B}) \] (11.2.3)

By definition

\[ [\Delta, !\Gamma'_1, x : A \triangleright x^B : B]^{\diamond} = \Diamond_{\Delta, \Gamma_1} \otimes I_{A,B}; \eta_B. \]

Thus

\[ Split_{\Delta, !\Gamma'_1, \Gamma_2}([id \otimes [\Delta, \Gamma_2 \triangleright V : A]^{\diamond}); [\Delta, !\Gamma'_1, x : A \triangleright x^B : B]^{\diamond} \]

\[ = Split_{\Delta, !\Gamma'_1, \Gamma_2}([id \otimes [\Delta, \Gamma_2 \triangleright V : A]^{\diamond}); \Diamond_{\Delta, \Gamma_1} \otimes I_{A,B}; \eta_B] \]

\[ = Split_{\Delta, !\Gamma'_1, \Gamma_2}([[\Delta, \Gamma_2 \triangleright V : A]^{\diamond}); \Diamond_{\Delta, \Gamma_1} \otimes I_{A,B}; \eta_B) \] (bifunc. of \( \otimes \))

which is equal to Formula (11.2.3), the naturality of \( \eta \).

Case \( M \equiv s^v, c^B \) and \( y^B \), where \( y \neq x \). Again in these cases, the term \( M \) is a core value: we have to show Equation (11.2.1) and Equation (11.2.2). We show the former, the latter being exactly similar.

The typing judgement \( !\Delta, \Gamma_1, x : A \triangleright M : B \) comes from respectively rules \((\Pi.J), (ax_2)\) and \((ax_1)\). In all of these cases, \( \Gamma_1 \) is of the form \( !\Gamma' \) and \( A \) of the form \( !A' \). From Lemma (11.2.1), the context \( \Gamma_2 \) is of the form \( \Gamma'_2 \). Since the term \( M[V/x] \) is equal to \( M \) in all three cases, the maps \( h \) and \( h' \) are of the form \( \Diamond_{\Delta, !\Gamma'_1, \Gamma'_2}; g \), for some map \( g \). The map \([\Delta, !\Gamma'_1, x : !A' \triangleright M : B]^{\diamond}\) is of the form \( \Diamond_{\Delta, !\Gamma'_1, !A'}; g \) for the same map \( g \). The bottom part of Diagram (11.2.1) is

\[ Split_{\Delta, !\Gamma'_1, \Gamma'_2}([id \otimes [\Delta, !\Gamma'_2 \triangleright V : A]^{\diamond}); \Diamond_{\Delta, !\Gamma'_1, !A'}; g = \Diamond_{\Delta, !\Gamma'_1, !A'}; g \]

using Equation (2.7.11). This is precisely the map \([\Delta, !\Gamma'_1, x : !A' \triangleright M : B]^{\diamond}\) for this case.

Case \( M \equiv \lambda^y y^C.N \). In this case, \( B = C \rightarrow D \) for some type \( D \), and the typing judgement \( !\Delta, \Gamma_1, x : A \triangleright M : B \) comes from typing rule \((\lambda_1)\). That is, \( !\Delta, \Gamma_1, y : C, x : A \triangleright N : C \) is valid.

We have \( y \neq x \); this means that \( M[V/x] = \lambda^y y^C.N[V/x] \). By induction hypothesis, the morphism \( k = [\Delta, \Gamma_1, y : C, \Gamma_2 \triangleright N[V/x] : D]^{\diamond} \) satisfies the following commutative diagram:

\[ [\Delta, \Gamma_1, y : C, \Gamma_2] \overset{k}{\longrightarrow} T([D]) \]

(11.2.1)

\[ [\Delta, \Gamma_1, y : C] \otimes [\Delta, \Gamma_2] \overset{id \otimes [\Delta, \Gamma_2 \triangleright V : A]^{\diamond}}{\longrightarrow} [\Delta, \Gamma_1, y : C] \otimes [A]. \]
Now, by definition,
\[
[!\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] : C \Rightarrow D]^v = \Phi^{-1}(k),
\]
\[
[!\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] : C \Rightarrow D]^c = \Phi^{-1}(k); \mu_{C \Rightarrow D},
\]
\[
[!\Delta, \Gamma_1 \triangleright M : C \Rightarrow D]^v = \Phi^{-1}([!\Delta, \Gamma_1, y : C \Rightarrow N : D]^v),
\]
\[
[!\Delta, \Gamma_1 \triangleright M : C \Rightarrow D]^c = (\Phi^{-1}([!\Delta, \Gamma_1, y : C \Rightarrow N : D]^c); \mu_{C \Rightarrow D}).
\]

Equations \ref{11.2.1} and \ref{11.2.2} are derived using the naturality of \(\Phi\).

\textbf{Case} \(M \equiv \lambda^{n+1}x^C . N\). This case is similar to the previous one. The only difference is in that the equations under consideration are encapsulated into
\[
f \mapsto \delta_{!\Delta} \triangleright d^H_{!\Delta}; L(f); I_{(A \Rightarrow B), t^{n+1}(A \Rightarrow B)}.
\]

\textbf{Cases} \(M \equiv \text{let } \mathbf{f} = N \text{ in } P\). In all these cases, the typing judgement \(!\Delta, \Gamma_1, x : A \triangleright M : B\) comes from a typing rule \((X)\) with hypotheses
\[
[!\Delta', \Gamma_{11} \triangleright N : C], \quad [!\Delta', \Gamma_{12}, \Lambda \triangleright P : B],
\]
for some context \(\Lambda\), where \(([!\Delta', \Gamma_{11}, \Gamma_{12}] = ([!\Delta, \Gamma_1, x : A]).\) If we call \(f\) and \(g\) the following maps:
\[
f = [!\Delta', \Gamma_{11} \triangleright N : C]^v, \quad g = [!\Delta', \Gamma_{12}, \Lambda \triangleright P : B]^v,
\]
we have
\[
[!\Delta, \Gamma_1, x : A \triangleright M : B]^v = (f \otimes_{!\Delta} \text{id}) ; (T(F) \otimes \text{id}) ; \sigma ; t ; g^v,
\]
for a given map \(F\), depending on \(\mathbf{f}\). If \(M\) is an extended value, so are \(N\) and \(P\). If we call \(f'\) and \(g'\) the following maps:
\[
f' = [!\Delta', \Gamma_{11} \triangleright N : C]^v, \quad g' = [!\Delta', \Gamma_{12}, \Lambda \triangleright P : B]^v,
\]
we have
\[
[!\Delta, \Gamma_1, x : A \triangleright M : B]^v = (f' \otimes_{!\Delta} \text{id}) ; (F \otimes \text{id}) ; \sigma ; g'.
\]

Note that we might need to add a permutation in front of \(f\), \(g\), \(f'\) or \(g'\), depending on the order of their respective input.

By \(\alpha\)-equivalence one can assume that the variables occurring in \(\Lambda\) does not occur anywhere in the other contexts. From Lemma \ref{11.1.1} one can assume that \(\Gamma_{11}\) and \(\Gamma_{12}\) do not contain any duplicable variables, implying that \([!\Delta] \subseteq [!\Delta']\). Thus there exists some context \(!\Psi\) such that \([!\Delta'] = ([!\Psi, !\Delta]).\) In particular, this means that
\[
([!\Psi, \Gamma_{11}, \Gamma_{12}] = ([\Gamma_1, x : A]). \tag{11.2.4}
\]
This equation is the main point that will allow us to apply the induction hypothesis, and thus finish the proof. The variable \(x : A\) belongs to either \(!\Psi\), \(\Gamma_{11}\) or \(\Gamma_{12}\). We study each one of these three possibilities.

\textbf{If} \(x \in [!\Psi]\). In this case, \(A = !A'\) and \(!\Psi = ([!\Psi', x : !A']).\) The contexts \(([!\Delta', \Gamma_{11}]\) and \(([!\Delta', \Gamma_{12}, \Lambda])\)
becomes respectively \(([!\Delta, \Psi', \Gamma_{11}, x : !A']\) and \(([!\Delta, \Psi', \Gamma_{12}, \Lambda, x : !A']\), meaning that the typing judgements \(!\Delta, \Psi', \Gamma_{11}, x : !A' \triangleright N : C\) and \(!\Delta, \Psi', \Gamma_{12}, \Lambda, x : !A' \triangleright P : B\) are valid.
Since $A = !A'$ and since $V$ is a value, by Lemma 11.1.13, the context $\Gamma_2$ is of the form $!\Gamma_2'$. We have $M[V/x] = \langle let \Gamma' = N[V/x] in P[V/x] \rangle$, and

$$M[V/x] : C, \quad \Delta, !\Psi', \Gamma_1, \Gamma_2, A : P[V/x]$$

are valid typing judgements, such that by induction hypotheses their respective computational denotations $\hat{f}$ and $\hat{g}$ are

$$\hat{f} : T[C], \quad \hat{g} : T[B]$$

By definition, the denotation $h = [[\Delta, \Gamma_1, \Gamma_2] \triangleright M[V/x] : B]$ is equal to

$$[[\Delta, \Gamma_1, \Gamma_2] \triangleright M[V/x] : B] = [\Delta, !\Psi', \Gamma_1, \Gamma_2, !\Delta, !\Psi', \Gamma_1, \Gamma_2, \Gamma_2']$$

Using Equations 11.2.5 and 11.2.6, one can rewrite $h$ as follows:

$$[[\Delta, !\Psi', \Gamma_1, \Gamma_2, \Gamma_2'] \triangleright M[V/x] : B] = [\Delta, !\Psi', \Gamma_1, \Gamma_2, !\Delta, !\Psi', \Gamma_1, \Gamma_2, \Gamma_2']$$

where $sw_1$ and $sw_2$ are permutations. Note that the map $Split_{\Delta, (\Psi', \Gamma_1, \Gamma_2)}$ is $\Delta_2$ followed by a permutation. It is then possible to lift the second occurrence of $\nu$ to the top, thus getting $h$ in the required format.

The computation for $h' = [[\Delta, \Gamma_1, \Gamma_2] \triangleright M[V/x] : B]$ is similar.
If \( x \in \Gamma_{11} \). This time, the context \( \Gamma_{11} \) is of the form \((\Gamma_1', x : A)\), and \( \Gamma_1 \) can be split into \((\Delta, !\Psi, \Gamma_1', \Gamma_2)\). We have \( M[V/x] = (let \quad \Box^C = N[V/x] in P) \), and

\[
\Delta, !\Psi, \Gamma_{11}, \Gamma_2 \triangleright N[V/x] : C, \quad \Delta, !\Psi, \Gamma_{12}, \Lambda \triangleright P : B
\]

are valid typing judgements. By induction hypothesis, the computational denotation of the former is

\[
\begin{array}{c}
\text{perm; Split in } (\Delta, !\Psi, (\Gamma_1', \Gamma_2), \Gamma_1) ; (\text{perm; Split}_{\Delta, \Gamma_1', \Gamma_2}) \otimes (id \otimes (id) : v \otimes id) \\
\Rightarrow [\Delta, !\Psi, \Gamma_{11}, \Gamma_2, \Gamma_1] \text{perm}_{\Delta, \Gamma_1', \Gamma_2} [\Delta, !\Psi, \Gamma_{11}, \Gamma_2] \otimes [\Delta, !\Psi, \Gamma_{12}] \\
\Rightarrow f \otimes id \Rightarrow T[C] \otimes [\Delta, !\Psi, \Gamma_{12}] \\
\Rightarrow (T(F) \otimes id) : \sigma : t \Rightarrow T[\Delta, !\Psi, \Gamma_{12}, \Lambda] \\
\Rightarrow g^* \Rightarrow T[B].
\end{array}
\]

Using the Equation (11.2.7), this is equal to

\[
\begin{array}{c}
[\Delta, !\Psi, (\Gamma_1', \Gamma_2), \Gamma_1] \text{perm}_{\Delta, \Gamma_1', \Gamma_2} [\Delta, !\Psi, \Gamma_{11}, \Gamma_2] \\
\Rightarrow f \otimes id \Rightarrow T[\Delta, !\Psi, \Gamma_{12}] \\
\Rightarrow (T(F) \otimes id) : \sigma : t \Rightarrow T[\Delta, !\Psi, \Gamma_{12}, \Lambda] \\
\Rightarrow g^* \Rightarrow T[B],
\end{array}
\]

where \text{perm} is a permutation. Using the coherence properties of the symmetry and the comonoid multiplication, the map

\[
\text{perm; Split}_{\Delta, \Gamma_1', \Gamma_2} (id \otimes v \otimes id)
\]

that is, \((id \otimes (id) : v \otimes id)\): the map \( h \) is in the requested form.

Again, the computation for \( h' = [\Delta, !\Psi, \Gamma_{11}, \Gamma_2] \triangleright M[V/x] : B \) \(^c\) is similar.

Case \( x \in \Gamma_{12} \). The context \( \Gamma_{12} \) is of the form \((\Gamma_1', x : A)\), and \( \Gamma_1 \) is equal to \((\Delta, !\Psi, \Gamma_1, \Gamma_{12})\).

We have \( M[V/x] = (let \quad \Box^C = N in P[V/x]) \), and

\[
\Delta, !\Psi, \Gamma_{11} \triangleright N : C, \quad \Delta, !\Psi, \Gamma_{12}, \Lambda \triangleright P[V/x] : B
\]
are valid typing judgements. By induction hypothesis, the computational denotation of the latter is

\[
\begin{align*}
\text{![}\Delta, \Psi, \Gamma_1', \Lambda, \Gamma_2]\text{~} & \xrightarrow{\text{Split}_{\Delta, (\Psi, \Gamma_1', \Lambda) \cdot R_2}} T[B] \\
\tilde{g} &
\end{align*}
\]

(11.2.8)

By definition, the denotation \( h = \text{![}\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] : B]^{c} \) is equal to

\[
\begin{align*}
\text{![}\Delta, \Psi, \Gamma_{11}, \Gamma_{12}', \Gamma_2] & \xrightarrow{\text{Split}_{\Delta, (\Psi, \Gamma_{11}, \Gamma_{12}') \cdot R_2}} \text{![}\Delta, \Psi, \Gamma_{11}] \otimes \text{![}\Delta, \Psi, \Gamma_{12}', \Gamma_2] \\
\text{!T} & \xrightarrow{f \otimes \text{id}} T[C] \otimes \text{![}\Delta, \Psi, \Gamma_{12}', \Gamma_2] \\
\text{!T} & \xrightarrow{(T(F) \otimes \text{id}) \cdot \sigma \cdot t} T[\Delta, \Psi, \Gamma_{12}', \Gamma_2, \Lambda] \\
\text{!T} & \xrightarrow{T(\text{id} \otimes \sigma)} T[\Delta, \Psi, \Gamma_{12}', \Lambda, \Gamma_2] \\
\tilde{g} & \xrightarrow{T[B]}
\end{align*}
\]

Using the Equation (11.2.8), this is equal to

\[
\begin{align*}
\text{![}\Delta, \Psi, \Gamma_{11}, \Gamma_{12}', \Gamma_2] & \xrightarrow{\text{Split}_{\Delta, (\Psi, \Gamma_{11}, \Gamma_{12}') \cdot R_2}} \text{![}\Delta, \Psi, \Gamma_{11}] \otimes \text{![}\Delta, \Psi, \Gamma_{12}', \Gamma_2] \\
\text{!T} & \xrightarrow{f \otimes \text{id}} T[C] \otimes \text{![}\Delta, \Psi, \Gamma_{12}', \Gamma_2] \\
\text{!T} & \xrightarrow{(T(F) \otimes \text{id}) \cdot \sigma \cdot t} T[\Delta, \Psi, \Gamma_{12}', \Gamma_2, \Lambda] \\
\text{!T} & \xrightarrow{T(\text{id} \otimes \sigma)} T[\Delta, \Psi, \Gamma_{12}', \Lambda, \Gamma_2] \\
\text{T} & \xrightarrow{T(\text{id} \otimes \sigma)} T[\Delta, \Psi, \Gamma_{12}', \Lambda, \Gamma_2] \\
\tilde{g} & \xrightarrow{T[B]}
\end{align*}
\]

Using the same technique as in the case where \( x \in \text{![}\Psi] \), one can move up the occurrence of \( v \), and thus get \( h \) in the requested form.

Again, the computation for \( h' = \text{![}\Delta, \Gamma_1, \Gamma_2 \triangleright M[V/x] : B]^{c} \) is similar.

**Cases M \equiv NP and M \equiv (N, P)^n.** As in the previous case, the typing judgement \( !\Delta, \Gamma_1, x : A \triangleright M : B \) comes from a typing rule \( (X) \) with hypotheses

\[
!\Delta', \Gamma_{11} \triangleright N : C, \quad !\Delta', \Gamma_{12} \triangleright P : D,
\]

for some types \( C \) and \( D \), where \((!\Delta', \Gamma_{11}, \Gamma_{12}) = (!\Delta, \Gamma_1, x : A)\). If we call \( f \) and \( g \) the following maps:

\[
f = [!\Delta', \Gamma_{11} \triangleright N : C]^c, \quad g = [!\Delta', \Gamma_{12} \triangleright P : D]^c,
\]

we have

\[
[!\Delta, \Gamma_1, x : A \triangleright M : B]^c = ([f \otimes \Delta] g)^c; F
\]
for a given map $F$, depending if $M$ is of the form $NP$ or of the form $(N, P)^n$. If $M$ is an extended value, so are $N$ and $P$. If we call $f'$ and $g'$ the following maps:

$$f' = [!\Delta', \Gamma_{11} \triangleright N : C]^v,$$

$$g' = [!\Delta', \Gamma_{12} \triangleright P : D]^v,$$

we have

$$[!\Delta, \Gamma_1, x : A \triangleright M : B]^v = (f' \otimes \Delta) ; G,$$

for a given map $G$, depending if $M$ is of the form $NP$ or of the form $(N, P)^n$. From Lemma 11.2.4 one can assume that $\Gamma_{11}$ and $\Gamma_{12}$ do not contain any duplicable variables, implying that $[\Delta] \subseteq [!\Delta']$. Thus there exists some context $\Psi$ such that $![\Delta'] = (\Psi, ![\Delta])$. In particular, this means that

$$(\Psi, \Gamma_{11}, \Gamma_{12}) = (\Gamma_1, x : A).$$

The variable $x : A$ belongs to either $\Psi$, $\Gamma_{11}$ or $\Gamma_{12}$. The study of each one of these three possibilities is similar as in the previous case.

This ends the list of cases: the lemma is verified.

**Theorem 11.2.5 (Soundness).** If $\Delta \triangleright M \approx_{ax} M' : A$ then we have $[\Delta \triangleright M : A]_{\Theta}_v = [\Delta \triangleright M' : A]_{\Theta}_v$ (and $[\Delta \triangleright M : A]_{\Theta} = [\Delta \triangleright M' : A]_{\Theta}$ if $M$ and $M'$ are values) for every interpretation $\Theta$.

**Proof.** Proof by induction on the size of the derivation of $M \approx_{ax} M'$. Case distinction on the last rule used. The cases corresponding to reflexivity, symmetry, transitivity and congruence are trivial.

We prove the result for the other cases:

**Rule ($\beta_\lambda$).** Here, we are considering $\Delta \triangleright$ let $x = V$ in $M \approx_{ax} M[V/x] : A$. We have directly from Lemma 9.1.19 that $[M[V/x]]^v = [\text{let } x = V \text{ in } M]^v$, and $[M[V/x]]^v = [\text{let } x = V \text{ in } M]^v$ if they are extended values.

**Rule ($\beta_{\otimes}$).** We are considering $\Delta \triangleright$ let $(x^C, y^P)^n = (V, W)^n$ in $M \approx_{ax} M[V/x, W/y] : A$. By $\alpha$-equivalence one can assume that $x$ is not free in $W$: we have $M[V/x, W/y] = (M[W/y])[V/x]$. One can split $\Delta$ into $(![\Delta'], \Gamma_1, \Gamma_2, \Gamma_3)$, such that $[\Gamma_1]$ contains only the free variables of $V$, $[\Gamma_2]$ only the free variables of $W$ and $[\Gamma_3]$ only the ones of $M$. From Lemma 9.1.19 the typing judgements

$$![\Delta'], \Gamma_1 \triangleright V : !^n C, \quad ![\Delta'], \Gamma_2 \triangleright W : !^n D, \quad ![\Delta'], \Gamma_3, x : !^n C, y : !^n D \triangleright M : A,$$

are valid. Let $f$, $g$ and $h$ be the denotations

$$f = [![\Delta'], \Gamma_1 \triangleright V : !^n C]^v,$$

$$g = [![\Delta'], \Gamma_2 \triangleright W : !^n D]^v,$$

$$h = [![\Delta'], \Gamma_3, x : !^n C, y : !^n D \triangleright M : B]^v.$$

From Lemma 9.1.19

$$[![\Delta'], \Gamma_3, x : !^n C, \Gamma_2 \triangleright M[W/y] : A]_{\Theta}$$

$$= (id \otimes ![\Delta'], \Gamma_2 \triangleright W : !^n D]^v) ; [![\Delta'], \Gamma_3, x : !^n C, y : !^n D \triangleright M : A]^v,$$

thus, still from Lemma 9.1.19

$$[![\Delta'], \Gamma_3, \Gamma_2, \Gamma_1 \triangleright (M[W/y])[V/x] : A]_{\Theta}$$
On another hand, by definition we have

\[
\llbracket \Delta', \Gamma_1, \Gamma_2 \triangleright (V, W)^n : !^n (C \otimes D) \rrbracket^C
\]

\[
= ((f; \eta_\circ C) \otimes !^n! (g; \eta_\circ D)); \Psi_1; TD_{C,D}^{L_n}
\]

\[
\llbracket \Delta', \Gamma_1, \Gamma_2 \triangleright \text{let } \langle x^C, y^D \rangle^n = (V, W)^n \text{ in } \langle x, y \rangle^C : A \rangle^C
\]

\[
= \left( \left( \left( (f; \eta_\circ C) \otimes !^n! (g; \eta_\circ D)); \Psi_1; TD_{C,D}^{L_n} \right) \otimes \Delta \right)^C \right) ; \sigma; t; h^*
\]

\[
= \left( \left( (f; \eta_\circ C) \otimes !^n! (g; \eta_\circ D)); \Psi_1 \right) \otimes !^n\Delta \right) ; (TD_{C,D}^{L_n} \otimes \id); (T \left( (d_{C,D}^{L_n})^{-1} \otimes \id \right) ; \sigma; t; h^*
\]

which makes the same map (modulo permutation of inputs) as in the previous calculation.

The case of the value denotation is similar.

**Rule \( \beta_\ast \).** We have \( \Delta \triangleright \text{let } \ast = \ast \text{ in } M : A \).

The typing judgement \( \Delta \triangleright \text{let } \ast = \ast \text{ in } M : A \) comes from rule \((\top, E)\). The typing judgements \( \triangleright \ast : \top \) and \( \Delta \triangleright M : A \) are valid, and since \( \llbracket \triangleright \ast : \top \rrbracket^C = \id^C \), if we call

\[
g = \llbracket \Delta \triangleright M : A \rrbracket^C,
\]

\[
h = \llbracket \Delta \triangleright \text{let } \ast = \ast \text{ in } M : A \rrbracket^C,
\]

then \( h = (\eta_\top \otimes g); \Psi_1 = g \). Similarly, if \( M \) is an extended value, and if we call

\[
g' = \llbracket \Delta \triangleright M : A \rrbracket^V,
\]

\[
h' = \llbracket \Delta \triangleright \text{let } \ast = \ast \text{ in } M : A \rrbracket^V,
\]

then \( h' = (\id^V \otimes g') = g' \).

**Rule \( \eta_\lambda \).** We have \( \Delta \triangleright \lambda^n x^A. \{ V : A \rightarrow B \} x^A \approx_{ax} V : !^n (A \rightarrow B) \). Both \( V \) and \( \lambda^n x^A. \{ V : A \rightarrow B \} x^A \) are values.

Let \( f = \llbracket \Delta \triangleright V : !^n (A \rightarrow B) \rrbracket^V \).

If \( n \neq 0 \). Then from Lemma \[11.2.5\] \( \Delta = !\Delta' \).

Let \( g = \llbracket \Delta, x : A \triangleright \{ V : A \rightarrow B \} x^A : B \rrbracket^C \). From Lemma \[11.2.6\] we have

\[
g = ((f; I^n_{(A \rightarrow B), A \rightarrow B} \otimes \eta_B) \otimes \eta_A); \Psi_1; \varepsilon_{A,B}
\]

\[
= ((f; I^n_{(A \rightarrow B), A \rightarrow B} \otimes \id_A) \otimes \eta_A); \Psi_1; \varepsilon_{A,B}
\]

\[
= ((f; I^n_{(A \rightarrow B), A \rightarrow B} \otimes \id_A); \varepsilon_{A,B}
\]

By naturality of \( \Phi \),

\[
\Phi^{-1} (\llbracket (f; I^n_{(A \rightarrow B), A \rightarrow B} \otimes \id_A); \varepsilon_{A,B} \rrbracket) = f; I^n_{(A \rightarrow B), A \rightarrow B} \Phi^{-1} (\varepsilon_{A,B})
\]
Thus, if \( h = \lbrack \Delta \triangleright \lambda^n x^A, \{ V <; A \rightarrow B \} x^A : !^n (A \rightarrow B) \rbrack^v \),
\[
\begin{align*}
h & = \delta_{\Delta}; d_{\Delta}^2; L(\Phi^{-1}(g)) ; I_{(A \rightarrow B), !^n (A \rightarrow B)} \\
& = \delta_{\Delta}; d_{\Delta}^2; L(f) ; I_{(A \rightarrow B), !^n (A \rightarrow B)} ; I_{(A \rightarrow B), !^n (A \rightarrow B)} \\
& = \delta_{\Delta}; d_{\Delta}^2; L(f) ; \epsilon !^n (A \rightarrow B) \\
& = \delta_{\Delta}; d_{\Delta}^2; \epsilon_\Delta; f \\
& = f.
\end{align*}
\]

If \( n = 0 \). The computation is similar, although simpler since there is no reference to \(!\) nor to \( L \). Indeed, \( \{ V <; A \rightarrow B \} = V \) from Lemma 11.1.15 and if \( g = \lbrack \Delta, x : A \triangleright V x^A : B \rbrack^v \),
\[
\begin{align*}
g & = (f \otimes id_A); (\eta_{A \rightarrow B}) \otimes (\eta_A); \Psi_1; \epsilon_{A,B} \\
& = (f \otimes id_A); (\eta_{A \rightarrow B}) \otimes (\eta_A); \Psi_1; \epsilon_{A,B} \\
& = (f \otimes id_A); \epsilon_{A,B}.
\end{align*}
\]

By naturality of \( \Phi \), if \( h = \lbrack \Delta \triangleright \lambda^n x^A, \{ V <; A \rightarrow B \} x^A : A \rightarrow B \rbrack^v \),
\[
h = L(\Phi^{-1}(g)) = f
\]

Finally, in the case of the computational denotation, since both terms are core values, we have the result by definition.

**Rule \((\beta^2)\).** We have \( \Delta \triangleright \lambda^n x^A = N \) in \( x^A \cong_{\alpha x} N : A \). By \( \alpha \)-equivalence one can assume that \( x \) is not a free variable of \( N \).

Suppose that \( N \) is an extended value, and let \( f \) be \( \lbrack \Delta \triangleright N : A \rbrack^v \). Then if \( h \) is the denotation \( \lbrack \Delta \triangleright \lambda^n x^A = N \) in \( x^A : A \rbrack^v \), we have
\[
h = (f \otimes id_\top); \sigma_{A,\top}; id_A = f.
\]

Now, suppose that \( N \) is any term, and let \( f' \) be \( \lbrack \Delta \triangleright N : A \rbrack^v \). From Lemma 11.1.15 if \( h' = \lbrack \Delta \triangleright \lambda^n x^A = N \) in \( x^A : A \rbrack^v \),
\[
h' = (f' \otimes id_\top); \sigma_{T[A],\top}; t; id_A = (f' \otimes id_\top); \sigma_{A,\top}; id_A = f'.
\]

**Rule \((\eta_\otimes)\).** We have \( \Delta \triangleright \lambda^n x^A, y^B)^n = N \) in \( (x^A, y^B)^n \cong_{\alpha x} N : !^n (A \otimes B) \). By \( \alpha \)-equivalence one can assume that neither \( x \) nor \( y \) are free variables of \( N \).

Suppose that \( N \) is an extended value, and let \( f \) be \( \lbrack \Delta \triangleright !^n (A \otimes B) \rbrack^v \). Then if \( h \) is the denotation \( \lbrack \Delta \triangleright \lambda^n x^A, y^B)^n = N \) in \( (x^A, y^B)^n : !^n (A \otimes B) \rbrack^v \), using the fact that the category is strongly monoidal and monoidal strict,
\[
h = (f \otimes id_\top); \left( (d^n_{[A]_{(B)}})^{-1} \otimes id_\top \right); \sigma_{\alpha x (A \otimes B), \top}; d^n_{[A]_{(B)}} \\
= f; \left( (d^n_{[A]_{(B)}})^{-1} \right); d^n_{[A]_{(B)}} \\
= f.
\]
11.2. Soundness of the Denotation

Now, suppose that $N$ is any term, and let $f'$ be $[\Delta \triangleright N : !^n(A \otimes B)]^\circ$. If $h'$ is the denotation $[\Delta \triangleright \langle x^A, y^B \rangle^n = N \in \langle x^\sim A, y^\sim B \rangle^n : !^n(A \otimes B)]^\circ$,

$$h' = (f' \otimes \text{id}_\tau); \left( T\left( d_{\partial}^{\partial} \right)^{-1} \otimes \text{id}_\tau \right); \sigma_{T[\Delta \triangleright \langle x^A, y^B \rangle^n : !^n(A \otimes B)]}; \tau; t; \left( d_{\partial}^{\partial} \right)^*$$

$$= f'; T\left( d_{\partial}^{\partial} \right)^{-1}; Td_{\partial}^{\partial}$$

Using Lemma 11.1.2 and Lemma 8.3.5, we have $\Delta \triangleright H = \{ \{ !\Delta \triangleright \langle x^A, y^B \rangle^n : N, !^n(A \otimes B) \} \}^\circ$.

Now, suppose that $N$ is any term, and let $f$ be $[\Delta \triangleright N : !^n\top]^\circ$. Then if $h$ is the denotation $[\Delta \triangleright \langle x^A, y^B \rangle^n = M \in \langle x^\sim A, y^\sim B \rangle^n : !^n(A \otimes B)]^\circ$, using Lemma 11.1.19 and Lemma 8.3.5

$$h = (f; T_{!\Delta \triangleright \langle x^A, y^B \rangle^n : \top}; d_{\partial}^{\partial}) = f; T_{!\Delta \triangleright \langle x^A, y^B \rangle^n : \top}; d_{\partial}^{\partial} = f.$$

Now, suppose that $N$ is any term, and let $f'$ be the denotation $[\Delta \triangleright N : !^n\top]^\circ$. If $h'$ is the denotation $[\Delta \triangleright \langle x^A, y^B \rangle^n = M \in \langle x^\sim A, y^\sim B \rangle^n : !^n(A \otimes B)]^\circ$,

$$h' = ((f'; T_{!\Delta \triangleright \langle x^A, y^B \rangle^n : \top}; d_{\partial}^{\partial}) \otimes (d_{\partial}^{\partial} \otimes \eta_{!\Delta \triangleright \langle x^A, y^B \rangle^n : \top})); \Psi_1$$

$$= ((f'; T_{!\Delta \triangleright \langle x^A, y^B \rangle^n : \top}; d_{\partial}^{\partial}) \otimes (\eta_T; Td_{\partial}^{\partial})); \Psi_1$$

$$= (f' \otimes \eta_T); (T_{!\Delta \triangleright \langle x^A, y^B \rangle^n : \top}; d_{\partial}^{\partial}); \Psi_1$$

$$= (f' \otimes \eta_T); \Psi_1; T_{!\Delta \triangleright \langle x^A, y^B \rangle^n : \top}; d_{\partial}^{\partial})$$

$$= f'; T_{!\Delta \triangleright \langle x^A, y^B \rangle^n : \top}; d_{\partial}^{\partial})$$

$$= f'.$$

Rule (let). We have

$$\Delta \triangleright \{ \text{let } \square = \text{let } \square = M \in N \}$$

Using Lemma 11.1.19 there exist contexts $!\Delta', \Gamma_1, \Gamma_2, \Gamma_3$, $\Lambda_1$ and $\Lambda_2$ such that $\Lambda_1$ contains the variables in $\square$. $\Lambda_2$ the variables in $\square$, such that $\Delta = (\Delta', \Gamma_1, \Gamma_2, \Gamma_3)$ and such that

$$!\Delta', \Gamma_1, \Gamma_2, \Gamma_3 \triangleright M : D, \quad !\Delta', \Gamma_2, \Lambda_1 \triangleright N : C, \quad !\Delta', \Gamma_3, \Lambda_2 \triangleright P : A.$$

Let $h_1$ and $h_2$ be

$$h_1 = \{ [\Delta', \Gamma_1, \Gamma_2, \Gamma_3 \triangleright \{ \text{let } \square = \text{let } \square = M \in N \} \}^\circ,$$

$$h_2 = \{ [\Delta', \Gamma_1, \Gamma_2, \Gamma_3 \triangleright \{ \text{let } \square = \text{let } \square = M \in N \} \}^\circ.$$

Let us define the following maps:

$$f_M = [\Delta', \Gamma_1 \triangleright M : D]^\circ$$

$$f_N = [\Delta', \Gamma_2, \Lambda_1 \triangleright N : C]^\circ$$

$$f_P = [\Delta', \Gamma_3, \Lambda_2 \triangleright P : A]^\circ$$

$$g_1 = [\Delta', \Gamma_1, \Gamma_2 \triangleright \text{let } \square = \text{let } \square = M \in N : C]^\circ$$

$$g_2 = [\Delta', \Gamma_2, \Lambda_1, \Gamma_3 \triangleright \text{let } \square = \text{let } \square = M \in N : A]^\circ.$$
There exists a map $F : [D] \rightarrow [\Lambda_1]$ and a map $G : [C] \rightarrow [\Lambda_2]$, respectively based upon the value of $\Box$ and $\mathbf{a}$, such that

\begin{align*}
g_1 &= (f_M \otimes h \otimes \text{id}_{\Delta', \Gamma_2}); (TF \otimes \text{id}_{\Delta', \Gamma_2}); \sigma_{T[\Lambda_1], \Delta', \Gamma_2}; t; f_N', \\
g_2 &= (f_N \otimes h \otimes \text{id}_{\Delta', \Gamma_2}); (TG \otimes \text{id}_{\Delta', \Gamma_2}); \sigma_{T[\Lambda_1], \Delta', \Gamma_2}; t; f_P', \\
h_1 &= (g_1 \otimes_t \text{id}_{\Delta', \Gamma_3}); (TG \otimes \text{id}_{\Delta', \Gamma_3}); \sigma_{T[\Lambda_1], \Delta', \Gamma_3}; t; f_P', \\
h_2 &= (f_M \otimes h \otimes \text{id}_{\Delta', \Gamma_3}); (TF \otimes \text{id}_{\Delta', \Gamma_3}); \sigma_{T[\Lambda_1], \Delta', \Gamma_3}; t; T(id \otimes \sigma_{[\Gamma_3], [\Lambda_1]}); g'_2.
\end{align*}

Using Lemma 11.1.11 one can rewrite $h_1$ as

\[ h_1 = (((f_M; TF) \otimes h \otimes \text{id}_{\Delta', \Gamma_2}) \otimes \text{id}_{\Delta_1, \Gamma_2}); ((\sigma; t; f_N') \otimes \text{id}_{\Delta_1, \Gamma_2}); \sigma; t; f_P'. \]

Using Lemma 11.1.12 one can show that

\[ T[\Lambda_1] \otimes [\Delta', \Gamma_2, \Gamma_3] \xrightarrow{\sigma \otimes_t} T[\Delta', \Gamma_2, \Gamma_3, \Lambda_1] \xrightarrow{T(id \otimes \sigma)} T[\Delta', \Gamma_2, \Lambda_1, \Gamma_3] \xrightarrow{T((f_N; TG) \otimes \Delta, id)} T(T[\Lambda_2] \otimes [\Delta', \Gamma_3]) \]

is equal to

\[ T[\Lambda_1] \otimes [\Delta', \Gamma_2, \Gamma_3] \xrightarrow{(id \otimes \sigma) \otimes \sigma} [\Delta', \Gamma_2, \Gamma_3] \otimes T[\Lambda_1] \xrightarrow{T(id \otimes \sigma)} [\Delta', \Gamma_3, \Gamma_2, \Lambda_1] \xrightarrow{T((f_N; TG))} T([\Delta', \Gamma_3] \otimes T[\Lambda_2]) \xrightarrow{T \circ \sigma} T(T[\Lambda_2] \otimes [\Delta', \Gamma_3]). \]

Now, using Equations 3.4.25 and 5.3.4, the following diagram is commutative:

\[ \begin{align*} & [\Delta', \Gamma_3, \Delta', \Gamma_2] \otimes T[\Lambda_1] \\
\xrightarrow{\text{id} \otimes t} & [\Delta', \Gamma_3, \Delta', \Gamma_2] \otimes T[\Lambda_1] \\
\xrightarrow{T \circ \text{id} = T(Split \otimes id)} & T[\Delta', \Gamma_3, \Delta', \Gamma_2, \Lambda_1] \\
\xrightarrow{id \otimes (f_N; TG)} & [\Delta', \Gamma_3] \otimes T^2[\Lambda_2] \\
\xrightarrow{id \otimes \mu} & T^2[\Delta', \Gamma_3, \Lambda_2] \\
\xrightarrow{T} & T[\Delta', \Gamma_3, \Lambda_2] \end{align*} \]

This is enough to say that $h_1 = h_2$.

The case where $M$, $N$ and $P$ are extended values is similar, without the need for the equations of strong monadicity.

**Rule (let)**. We have

\[ \Delta \triangleright \text{let } \Box = V \text{ in let } \Box = W \text{ in } M \approx_{ax} \text{ let } \Box = W \text{ in } \text{let } \Box = V \text{ in } M : A, \]
where $V$ and $W$ are core values. Using Lemma 11.2.1, there exist contexts $\Delta', \Gamma_1, \Gamma_2, \Gamma_3, \Lambda_1$ and $\Lambda_2$ such that $\Lambda_1$ contains the variables in $\square$, $\Lambda_2$ the variables in $\blacksquare$ such that $\Delta = (\Delta', \Gamma_1, \Gamma_2, \Gamma_3)$ and such that

$$1 \Delta', \Gamma_3, \Lambda_1, \Lambda_2 \triangleright M : A,$$  

$$1 \Delta', \Gamma_1 \triangleright V : C,$$  

$$1 \Delta', \Gamma_2 \triangleright W : D.$$ 

Let $h_1$ and $h_2$ be

$$h_1 = \langle 1 \Delta', \Gamma_1, \Gamma_2, \Gamma_3 \triangleright \text{let } \square = V \text{ in let } \square = W \text{ in } A \rangle^c,$$  

$$h_2 = \langle 1 \Delta', \Gamma_1, \Gamma_2, \Gamma_3 \triangleright \text{let } \square = W \text{ in let } \square = V \text{ in } A \rangle^c.$$ 

Let us define the following maps:

$$f_M = \langle 1 \Delta', \Gamma_3, \Lambda_1, \Lambda_2 \triangleright M : A \rangle^c,$$  

$$f_V = \langle 1 \Delta', \Gamma_1 \triangleright V : C \rangle^w,$$  

$$f_W = \langle 1 \Delta', \Gamma_2 \triangleright W : D \rangle^w.$$ 

There exists a map $F : \llbracket C \rrbracket \rightarrow \llbracket \Lambda_1 \rrbracket$ and a map $G : \llbracket D \rrbracket \rightarrow \llbracket \Lambda_2 \rrbracket$, respectively based upon the value of $\square$ and $\blacksquare$, such that

$$g_1 = (f_V ; \eta_C ; TF) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_2} ; \sigma_{T[\Lambda_1], [\Delta', \Gamma_3, \Lambda_2] ; [\Delta', \Gamma_3, \Lambda_2]} ; t \otimes (id \otimes \sigma_{\Lambda_2, [\Lambda_1]}) ; f_M^1,$$  

$$g_2 = (f_W ; \eta_D ; TG) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_1} ; \sigma_{T[\Lambda_1], [\Delta', \Gamma_3, \Lambda_1] ; [\Delta', \Gamma_3, \Lambda_1]} ; \eta ; f_M^2,$$  

$$h_1 = \langle 1 \Delta', \Gamma_1, \Gamma_2, \Gamma_3 \triangleright \text{let } \square = V \text{ in let } \square = W \text{ in } A \rangle^c,$$  

$$h_2 = \langle 1 \Delta', \Gamma_1, \Gamma_2, \Gamma_3 \triangleright \text{let } \square = W \text{ in let } \square = V \text{ in } A \rangle^c.$$ 

We now want to show that $h_1 = h_2$. Using Equation 11.2.4.3 stating that $\eta_{A \otimes B} = (id_A \otimes \eta_B) ; t_{A, B}$, we rewrite $h_1$:

$$h_1 = ((f_V ; \eta_C ; TF) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_2}) ; \sigma_{T[\Lambda_1], [\Delta', \Gamma_3, \Lambda_2] ; [\Delta', \Gamma_3, \Lambda_2]} ; t ; g_2^2,$$  

$$h_2 = \langle 1 \Delta', \Gamma_1, \Gamma_2, \Gamma_3 \triangleright \text{let } \square = V \text{ in let } \square = W \text{ in } A \rangle^c.$$ 

Similarly one can rewrite $g_1$, $g_2$ and $h_2$:

$$g_1 = ((f_V ; F) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_2}) ; \sigma_{\Lambda_1, [\Delta', \Gamma_3, \Lambda_2] ; [\Delta', \Gamma_3, \Lambda_2]} ; f_M^1,$$  

$$g_2 = (f_W ; G) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_1} ; \sigma_{\Lambda_1, [\Delta', \Gamma_3, \Lambda_1] ; [\Delta', \Gamma_3, \Lambda_1]} ; f_M^2,$$  

$$h_2 = \text{id} \otimes \sigma_{\Lambda_1, [\Delta', \Gamma_3, \Lambda_2]} \otimes \eta ; ((f_W ; G) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_3}) ; \sigma_{\Lambda_2, [\Delta', \Gamma_3, \Lambda_3] ; [\Delta', \Gamma_3, \Lambda_3]} ; g_1^1.$$ 

The term $h_1$ becomes:

$$h_1 = ((f_V ; F) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_2}) ; \sigma_{\Lambda_1, [\Delta', \Gamma_3, \Lambda_2] ; [\Delta', \Gamma_3, \Lambda_2]} ; g_2^2$$  

$$= ((f_V ; F) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_2}) ; \sigma_{\Lambda_1, [\Delta', \Gamma_3, \Lambda_2] ; [\Delta', \Gamma_3, \Lambda_2]} ; \sigma_{\Lambda_2, [\Delta', \Gamma_3, \Lambda_2] ; [\Delta', \Gamma_3, \Lambda_2]} ; f_M^1.$$ 

The term $h_2$ becomes:

$$h_2 = (f_W ; G) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_1} ; \sigma_{\Lambda_1, [\Delta', \Gamma_3, \Lambda_1] ; [\Delta', \Gamma_3, \Lambda_1]} ; \sigma_{\Lambda_2, [\Delta', \Gamma_3, \Lambda_1] ; [\Delta', \Gamma_3, \Lambda_1]} ; (id_A \otimes (f_W ; G) \otimes_{\Delta'} \text{id}_{\Delta', \Gamma_3, \Lambda_1}) ; f_M^2.$$
11.2. Soundness of the Denotation

= ((f_V; F) \otimes_{\Delta'} ((f_W; G) \otimes_{\Delta'} id_{\Delta'; \Gamma_3})); \sigma_{[\Lambda_1; \Lambda_2; \Psi_{\Delta'}; \Gamma_3]; \Psi_M} \cdot f_M.

A similar computation shows that \( h_2 \) also yields this term.

In the case where \( M \) is an extended value, the only computation needed is the last one.

Rules \((let^{\text{app}})\) and \((let^\otimes)\). We have

\[\Delta \vdash \text{let } x^{A \rightarrow B} = M \text{ in } y^A = N \text{ in } x^{A \rightarrow B}y^A \equiv_{\text{ax}} MN : B,\]

\[\Delta \vdash \text{let } x^{nA} = M \text{ in } y^{nB} = N \text{ in } (x^{nA}, y^{nB})^n \equiv_{\text{ax}} (M, N)^n : !n(A \otimes B).\]

Note that both of these equations are of the form

\[\Delta \vdash \text{let } x^C = M \text{ in } y^D = N \text{ in } P \equiv_{\text{ax}} P(M, N) : E,\]

for some types \( C, D \) and \( E \) and some term construct \( P(-, -) \).

We can compute the computational interpretation in both cases. The value interpretation can be done only in the second case. However, the proof being a subset of the one required for the computational interpretation, we omit it.

Using \( \alpha \)-equivalence, one can assume that \( x \) and \( y \) do not occur in \( M \) nor in \( N \). Using Lemma 9.1.19, there exist contexts \( !\Delta', \Gamma_1 \) and \( \Gamma_2 \) such that \( \Delta = (\Delta', \Gamma_1; \Gamma_2) \) and such that

\[!\Delta', \Gamma_1 \triangleright M : C, \quad !\Delta', \Gamma_2 \triangleright N : D.\]

Let \( h_1 \) and \( h_2 \) be

\[h_1 = [!\Delta', \Gamma_1; \Gamma_2 \triangleright \text{let } x^C = M \text{ in } y^D = N \text{ in } P(x, y) : B]^c,\]

\[h_2 = [!\Delta', \Gamma_1; \Gamma_2 \triangleright P(M, N) : B]^c.\]

Let us define the following maps:

\[f_M = [!\Delta', \Gamma_1 \triangleright M : C]^c,\]

\[f_N = [!\Delta', \Gamma_2 \triangleright N : D]^c,\]

\[g = [!\Delta', \Gamma_1; \Gamma_2 \triangleright \text{let } x^D = N \text{ in } P(x, y) : B]^c,\]

\[k = [x : C, y : D \triangleright P(x, y) : B]^c.\]

By definition and from Lemma 9.1.19, there exists a map \( F : [C \otimes D] \to T(B) \) such that

\[k = (\eta_C \otimes \eta_D); \Psi_1; F^*,\]

\[g = (f_N \otimes id_C); \sigma_{T[D];C}; t; k^*,\]

\[h_1 = (f_M \otimes id_{\Delta'}; \sigma_{T[C];\Delta'; \Gamma_2}); \sigma_{T[C];\Delta'; \Gamma_3}; T_{[C];D}; \mu; F^*,\]

\[h_2 = (f_M \otimes id_{\Delta'}; f_N); \Psi_1; F^*;\]

Using Equation 5.4.4 of the tensorial strength, let us rewrite \( k \):

\[k = (\eta_C \otimes \eta_D); \Psi_1; F^*\]

\[= (\eta_C \otimes \eta_D); \sigma_{T[C];T[D];T_{[C];D};T_{[C];D}; T_{[C];D}; \mu; F^*\]

\[= (\eta_D \otimes \eta_C); \sigma_{T[D];T[C]; T_{[D];C}; T_{[C];D}; \mu; F^*\]

\[= (\eta_D \otimes id_C); \sigma_{T[D];T[C]; T_{[D];C}; T_{[C];D}; \mu; F^*.\]
11.2. Soundness of the Denotation 195

Rule \( n \) definition, we have \( n \). There are four cases:

Let us define the following maps:

\[
\begin{align*}
\Gamma_1' &= (\eta_D \otimes \text{id}_C); \sigma_{T[D], [C]}; t[C], [D]; F^* \\
\eta[C], [D]; F^* \\
\eta[C], [D]; F^* \\
F.
\end{align*}
\]

Let us rewrite \( g \):

\[
g = (f_N \otimes \text{id}_C); \sigma_{T[D], [C]}; t; k^* = (f_N \otimes \text{id}_C); \sigma_{T[D], [C]}; t; F^*
\]

Let us rewrite \( h_1 \):

\[
\begin{align*}
h_1 &= (f_M \otimes \Delta'). \text{id}_{\Delta', \Gamma_2}; \sigma_{T[C], [\Delta', \Gamma_2]}; t; g^* \\
&= (f_M \otimes \Delta'. \text{id}_{\Delta', \Gamma_2}); \sigma_{T[C], [\Delta', \Gamma_2]}; t; T(f_N \otimes \text{id}_C); T; F^* \\
&= (f_M \otimes \Delta'. \text{id}_{\Delta', \Gamma_2}); \sigma_{T[C], [\Delta', \Gamma_2]}; t; T(id_{T[D]} \otimes \text{id}_C); T; F^* \\
&= (f_M \otimes \Delta'. \text{id}_{\Delta', \Gamma_2}); \sigma_{T[C], [\Delta', \Gamma_2]}; t; T; F^* \\
&= (f_M \otimes \Delta'. \text{id}_{\Delta', \Gamma_2}); \Psi; F^* \\
&= h_2.
\end{align*}
\]

Rule (let\(^\lambda\)). We have

\[
\Delta \triangleright \text{let } x^D = V \text{ in } \lambda^n y^A M \equiv_{ax} \lambda^n y^A, \text{ let } x^D = V \text{ in } M : !^n (A \rightarrow B),
\]

where \( V \) is a core value. Using \( \alpha \)-equivalence, one can assume that \( \Delta \) does not occur in \( M \) nor in \( V \), and that \( y \neq x \). Using Lemma \([9.1.10]\), there exist contexts \( !\Delta', \Gamma_1 \) and \( \Gamma_2 \) such that \( \Delta = (!\Delta', \Gamma_1, \Gamma_2) \) and such that

\[
!\Delta', \Gamma_2, \lambda : D, y : A \triangleright M : B, \quad !\Delta', \Gamma_1 \triangleright V : D,
\]

Let \( h_1 \) and \( h_2 \) be

\[
\begin{align*}
h_1 &= \llbracket !\Delta', \Gamma_1, \Gamma_2 \triangleright \text{let } x^D = V \text{ in } \lambda^n y^A M : !^n (A \rightarrow B) \rrbracket^c, \\
h_2 &= \llbracket !\Delta', \Gamma_1, \Gamma_2 \triangleright \lambda^n y^A \text{, let } x^D = V \text{ in } M : !^n (A \rightarrow B) \rrbracket^c.
\end{align*}
\]

Let us define the following maps:

\[
\begin{align*}
f_M &= \llbracket !\Delta', \Gamma_2, x : D, y : A \triangleright M : B \rrbracket^c \\
f_V &= \llbracket !\Delta', \Gamma_1 \triangleright V : D \rrbracket^v \\
g_1 &= \llbracket !\Delta', \Gamma_2, x : D \triangleright \lambda^n y^A M : !^n (A \rightarrow B) \rrbracket^c \\
g_2 &= \llbracket !\Delta', \Gamma_1, \Gamma_2, y : A \triangleright \text{let } x^D = V \text{ in } M : B \rrbracket^c
\end{align*}
\]

There are four cases: \( n \) can be null or not, and \( M \) can be an extended value or not (allowing us to compute the value interpretation). We fully develop the computational interpretation of the case \( n = 0 \) since the other three cases are done using similar calculations.

From Lemma \([9.1.10]\), \( \Gamma_1 \) and \( \Gamma_2 \) are respectively of the form \( !\Gamma_1' \) and \( !\Gamma_2' \), and \( D = !D' \). By definition, we have

\[
\begin{align*}
g_1 &= \delta_{1\Delta', !\Gamma_1'; x : !D'; !\Delta'; !\Gamma_2'; x : !D'; L\Phi^{-1}(f_M); h(A \rightarrow B); !^n (A \rightarrow B); \eta(A \rightarrow B) \\
g_2 &= ((f_V; \eta_D) \otimes \Delta'. \text{id}_{\Delta', \Gamma_2, y: A}); \sigma_{T[D], [\Delta', \Gamma_2, y: A]}; t; T(id \otimes \sigma_{A, D}); f_M',
\end{align*}
\]
We are considering the relation $\Delta = (|\Delta', \Gamma_1, \Gamma_2|)$.

The setting is the following:

$$h_1 = ((f_V; \eta_D) \otimes |\Delta'; \Gamma_1, \Gamma_2|; \sigma_{T[D],|\Delta', \Gamma_2|}; t; g_1^*),$$

$$h_2 = \delta|\Delta', |\Gamma_1', |\Gamma_2'|; d^h|\Delta', |\Gamma_1', |\Gamma_2'|; L\Phi^{-1}(g_2); I((A \rightarrow B), \eta_n(A \rightarrow B)).$$

We want to show that $h_1 = h_2$. Let us rewrite $g_2$, using Equation 5.4.4 of strong monadicity of $T$:

$$g_2 = ((f_V; \eta_D) \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{T[D],|\Delta', \Gamma_2|}; t; \sigma_{A,D}; f_M^*$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*)$$

By naturality of $\Phi$,

$$\Phi^{-1}(g_2) = (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \Phi^{-1}(f_M)).$$

The map $h_2$ is reformatted using the naturality of $d^L$ and of $\delta$:

$$h_2 = \delta|\Delta', |\Gamma_1', |\Gamma_2'|; d^h|\Delta', |\Gamma_1', |\Gamma_2'|; L\Phi^{-1}(g_2); I((A \rightarrow B), \eta_n(A \rightarrow B))$$

$$= \delta|\Delta', |\Gamma_1', |\Gamma_2'|; d^h|\Delta', |\Gamma_1', |\Gamma_2'|; L(f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*$$

$$= \delta|\Delta', |\Gamma_1', |\Gamma_2'|; d^h|\Delta', |\Gamma_1', |\Gamma_2'|; L(f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*)$$

Note that $g_1$ is of the form $g_1^*; \eta_n(A \rightarrow B)$. Again using Equation 5.4.4:

$$h_1 = ((f_V; \eta_D) \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{T[D],|\Delta', \Gamma_2|}; t; g_1^*,$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*)$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*)$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*)$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*)$$

$$= (f_V \otimes |\Delta' \otimes \text{id}_{|\Delta', \Gamma_2|}; \sigma_{D[D],|\Delta', |\Delta', \Gamma_2|}; \eta_n(A \rightarrow B); f_M^*)$$

$$I((A \rightarrow B), \eta_n(A \rightarrow B); \eta_n(A \rightarrow B))$$

$$= h_2.$$
then, since \(I_{B \to C, A \to C} = (I_{A,B}) \to C\), we have

\[
\Delta \triangleright N\{P <: B\} : B\] = \( (f \otimes I_{A,B}; \Psi_1; \varepsilon_{B,C}^*) \),
\[
= (f \otimes I_{A,B}; (\text{id} \otimes I_{A,B}) \circ \text{id}; \Psi_1; \varepsilon_{B,C}^*) \varepsilon_{A,C}^*
\]
and

\[
\Delta \triangleright \{N <: A \to C\} P : C\] = \( (f; T I_{B \to C, A \to C} \otimes I_{\Delta'} g) \circ \text{id}; \Psi_1; \varepsilon_{A,C}^* \),
\[
= (f; (I_{B \to C, A \to C} \otimes \text{id}) \circ \text{id}; \Psi_1; \varepsilon_{A,C}^*)^* \varepsilon_{A,C}^*.
\]

The two denotations are equal by naturality of \(\Phi\). Indeed, since

\[
\Phi(A \to C, A \to C) : (I_{A,B} \to C) \triangleright C(A \to C) \otimes A, TC)
\]

we have \(\Phi(I_{A,B} \to C) = ((I_{A,B} \to C) \otimes A); \varepsilon_{A,C}\). Since

\[
\Phi(B \to C, B \to C) : (I_{A,B} \to C) \triangleright C(B \to C) \otimes B, TC)
\]

we have \(\Phi(I_{A,B} \to C) = ((B \to C) \otimes I_{A,B}); \varepsilon_{B,C}\). Thus,

\[
((B \to C) \otimes I_{A,B}); \varepsilon_{B,C} = ((I_{A,B} \to C) \otimes A); \varepsilon_{A,C}.
\]

**Rule (let\(^2\)).** In this case, \(A <: A'\), \(B <: B'\), and \(n' = 0\) if \(n = 0\). We have \(\Delta = (!\Delta', \Gamma_1, \Gamma_2)\) with

\[
!\Delta', \Gamma_1 \triangleright N : !n'(A \otimes B), \quad !\Delta', \Gamma_2, x : !n' A', y : !n' B' \triangleright P : E,
\]

and we consider the following relation:

\[
\Delta \triangleright \left(\text{let} \,(x^A, y^B)^{n'} = \{N <: !n'(A' \otimes B')\} \text{ in } P\right) \approx (\text{let} \,(x^A, y^B)^{n'} = N \text{ in } P) : E.
\]

By \(\alpha\)-equivalence, one can assume that \(x, y\) do not occur in \(N\).

Let \(f, g, h_1\) and \(h_2\) be the following maps:

\[
f = [[\Delta', \Gamma_1 \triangleright N : !n'(A \otimes B)]]^*,
\]

\[
g = [[\Delta', \Gamma_2, x : !n' A', y : !n' B' \triangleright P : E]^*],
\]

\[
h_1 = [[\Delta', \Gamma_1, \Gamma_2 \triangleright \text{let} \,(x^A, y^B)^{n'} = \{N <: !n'(A' \otimes B')\} \text{ in } P : E]^*],
\]

\[
h_2 = [[\Delta', \Gamma_1, \Gamma_2 \triangleright \text{let} \,(x^A, y^B)^{n'} = N \text{ in } P : E]^*].
\]
By definition, we have
\[ h_1 = \left( (f; I^n_{(A \otimes B),!^{n'}(A' \otimes B')}) \right) \otimes \Delta; \text{id}(\Delta; \Gamma_2); (T(d_{A',B'}^{!n'})^{-1} \otimes \text{id}); \]
\[ \sigma_{T(x^{!n'}A',y^{!n'}B')} \cdot \{ \Delta; \Gamma_2; t; g^* \}; \]
\[ h_2 = (f \otimes \Delta; \text{id}(\Delta; \Gamma_2); (T(d_{A,B}^{!n})^{-1} \otimes \text{id}); \]
\[ \sigma_{T(x^{!n}A,y^{!n}B)} \cdot \{ \Delta; \Gamma_2; t; (I(\Delta', \Gamma_2, x^{!n}A,y^{!n}B), (\Delta', \Gamma_2, x^{!n'}A',y^{!n'}B'); g)^* \}. \]

These two maps are the same since
\[ I^n_{(A \otimes B),!^{n'}(A' \otimes B')} = L^n I_{A,A'} \otimes L^{!n'} I_{B,B'}. \]

and
\[ I_{(\Delta', \Gamma_2, x^{!n}A,y^{!n}B), (\Delta', \Gamma_2, x^{!n'}A',y^{!n'}B')} = \text{id}(\Delta', \Gamma_2) \otimes L^n I_{A,A'} \otimes L^{!n'} I_{B,B'}. \]

For the same reasons the value interpretation of the two terms in relation are the same.

This ends the list of possible cases. Theorem 11.2.5 is then verified.

**Corollary 11.2.6.** If Erase(M) = Erase(M') and if \( \Delta \triangleright M, M' : A \) are valid typing judgements, then \([M]^c = [M']^c\) (and \([M]^v = [M']^v\) if \(M \) and \(M' \) are values).

**Proof.** Corollary of Theorems 11.2.5 and 11.3.1.

### 11.3 Completeness

Recall the category \( \mathcal{C}_\lambda \) from Section 11.2. Since the category \( \mathcal{C}_\lambda \) is a linear category for duplication, one can interpret the language in it. This section states that the defined lambda calculus is an internal language of linear categories for duplication.

Since the category \( \mathcal{C}_\lambda \) is a monoidal category, one can w.l.o.g. generalize the notion of pairing to finite tensor products of terms.

**Definition 11.3.1.** We define the following shortcut notations for terms:

\[ \langle \rangle^n = \ast^n, \quad \langle x^A \rangle^n = x^{nA}, \quad \langle x_1, x_2 \ldots \rangle^n = \langle x_1, (x_2 \ldots)^0 \rangle^n, \]

(\(\text{let } \langle \rangle^n = M \quad \text{in } N\)),

(\(\text{let } \langle x^A \rangle^n = M \quad \text{in } N\)),

(\(\text{let } \langle x_1, x_2 \ldots \rangle^n = M \quad \text{in } N\)),

and for types:

\[ A_1 \otimes A_2 \otimes \cdots \otimes A_n = A_1 \otimes (A_2 \otimes (\cdots \otimes A_n) \cdots). \]

**Lemma 11.3.2.** The following derived typing rules are correct:

\[
\begin{align*}
\frac{!\Delta, \Gamma_1 \triangleright M : !^n(A_1 \otimes \cdots \otimes A_k)}{
!\Delta, \Gamma_1, I_1 \triangleright \langle x_1, \ldots, x_k \rangle^n = M \quad \text{in } N : B}
\end{align*}
\] (11.3.1)

\[
\frac{!\Delta, \Gamma_2, x_1 : !^n A_1, \ldots, x_k : !^n A_k \triangleright N : B}{
!\Delta, \Gamma_1, I_2 \triangleright \langle x_1, \ldots, x_k \rangle^n = M \quad \text{in } N : B}
\]
and

\begin{align*}
\Gamma_1 \triangleright M_1 &: \!^n A_1 \\
\Gamma_2 \triangleright M_2 &: \!^n A_2 \\
\vdots \\
\Gamma_k \triangleright M_k &: \!^n A_k \\
\Gamma_1, \ldots, \Gamma_k &\triangleright (M_1, \ldots, M_k)^n : \!^n (A_1 \otimes \cdots \otimes A_k).
\end{align*}

(11.3.2)

Proof. Proof by induction on \(k\).

Lemma 11.3.3. In the setting of Equation \(\text{11.3.2}\) in Lemma \(\text{11.3.2}\) if for all \(i\) we have \(f_i = [\!^n \Gamma_i \triangleright M_i : \!^n A_i]^c\), then

\[ [\Gamma_1, \ldots, \Gamma_k \triangleright (M_1, \ldots, M_k)^n : \!^n (A_1 \otimes \cdots \otimes A_k)]^c = (f_1 \otimes \cdots \otimes f_k)^T d^{L^n}_{A_1, \ldots, A_k}. \]

In the case where all the \(M_i\) are extended values, if \(f_i' = [\!^n \Gamma_i \triangleright M_i : \!^n A_i]^c\), then

\[ [\Gamma_1, \ldots, \Gamma_k \triangleright (M_1, \ldots, M_k)^n : \!^n (A_1 \otimes \cdots \otimes A_k)]^c = (f_1 \otimes \cdots \otimes f_k)^T d^{L^n}_{A_1, \ldots, A_k}. \]

Proof. Proof by induction on \(k\).

Lemma 11.3.4. In the setting of Equation \(\text{11.3.2}\) in Lemma \(\text{11.3.2}\) if

\[ f = [\!^n \Gamma_1 \triangleright M : \!^n (A_1 \otimes \cdots \otimes A_k)]^c, \]

\[ g = [\!^n \Gamma_2, x_1 : \!^n A_1, \ldots, x_k : \!^n A_k \triangleright N : B]^c, \]

then

\[ [\!^n \Gamma_1, \Gamma_2 \triangleright \text{let } (x_1, \ldots, x_k)^n = M \text{ in } N : B]^c = (f \otimes_\Delta id); (T(d^{L^n}_{A_1, \ldots, A_k})^{-1} \otimes id); \sigma; t; g^*. \]

In the case where \(M\) and \(N\) are extended values, if

\[ f = [\!^n \Gamma_1 \triangleright M : \!^n (A_1 \otimes \cdots \otimes A_k)]^v, \]

\[ g = [\!^n \Gamma_2, x_1 : \!^n A_1, \ldots, x_k : \!^n A_k \triangleright N : B]^v, \]

then

\[ [\!^n \Gamma_1, \Gamma_2 \triangleright \text{let } (x_1, \ldots, x_k)^n = M \text{ in } N : B]^v = (f \otimes_\Delta id); (T(d^{L^n}_{A_1, \ldots, A_k})^{-1} \otimes id); \sigma; g. \]

Proof. Proof by induction on \(n\).

Lemma 11.3.5. In \(C_\lambda\), a valid typing judgement \(x_1 : A_1, \ldots, x_n : A_n \triangleright M : B\) has for computational denotation \((t : A_1 \otimes \cdots \otimes A_n \triangleright \text{let } (x_1, \ldots, x_n) = t \text{ in } \lambda \sigma.M : \top \rightarrow B)\). If \(M = V\) is a value, the value interpretation is \((t : A_1 \otimes \cdots \otimes A_n \triangleright \text{let } (x_1, \ldots, x_n) = t \text{ in } V : B)\).

Proof. Proof by structural induction on \(M\), using Lemmas \(\text{11.3.3}\) and \(\text{11.3.4}\). For each case, one writes the categorical morphism corresponding to the term and one interprets it in \(C_\lambda\).

Theorem 11.3.6 (Completeness). In \(C_\lambda\), \(\Theta\) being the identity, one has \([x : A \triangleright M : B]^c_\Theta \approx_{ax} (x : A \triangleright \lambda \sigma.M : \top \rightarrow B)\) and \([x : A \triangleright V : B]^v_\Theta \approx_{ax} (x : A \triangleright V : B)\).

Proof. Corollary of Lemma \(\text{11.3.5}\).
11.4 Towards a Denotational Model

In Chapters 8-11, we developed the categorical requirements for modeling a generic call-by-value linear lambda calculus, i.e., its type system (which includes subtyping) and equational laws. We have not yet specialized the language to a particular set of built-in operators, for example, those that are required for quantum computation.

However, since the quantum lambda calculus of Chapter 6 is the main motivation behind our work, we will comment very briefly on what additional properties would be required to interpret its primitives. The quantum lambda calculus of Chapter 6 is obtained by instantiating and extending the call-by-value language of Chapter 9 with the following primitive types, constants, and operations:

Types: \( \text{bit}, \text{qbit} \)

Constants: \( 0 : !\text{bit}, 1 : !\text{bit} \)  
\( \text{new} : !(\text{bit} \rightarrow \text{qbit}), U : !((\text{qbit}^n \rightarrow \text{qbit}^n)), \text{meas} : !(\text{qbit} \rightarrow !\text{bit}) \)

Operations:  
\[
\Gamma_1, \Delta \triangleright P : \text{bit} \quad \Gamma_2, \Delta \triangleright M : A \quad \Gamma_2, \Delta \triangleright N : A \quad (\text{if})
\]

In the intended semantics, \( !\text{bit} \cong \text{bit} \), while \( !\text{qbit} \) is empty. \text{new} creates a new qubit, and \text{meas} measures a qubit.

The denotational semantics of these operations is already well-understood (see Section 4.3) in the absence of higher-order types. They can all be interpreted in the category \( \mathcal{Q} \) of superoperators described in Section 4.3. The part that is not yet well-understood is how these features interact with higher-order types.

In light of our present work, we can conclude that a model of the quantum lambda calculus consists of a linear category for duplication \( (\mathcal{C}, L, T, \rightarrow) \), such that the associated category of computations \( \mathcal{C}_T \) contains the category \( \mathcal{Q} \) as a full monoidal subcategory. To construct an actual instance of such a model is still an open problem.
Bibliography


---

1http://www.theory.caltech.edu/people/preskill/ph229/


\[^{2}\text{http://www.mathstat.dal.ca/~selinger/qpl2006/proceedings.html}\]
## Index

<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma^A_{x,y}$</td>
<td>91</td>
</tr>
<tr>
<td>$\gamma^A_{x,y}$</td>
<td>91</td>
</tr>
<tr>
<td>adjunction</td>
<td>8</td>
</tr>
<tr>
<td>composition</td>
<td>9</td>
</tr>
<tr>
<td>left/right adjoint</td>
<td>8</td>
</tr>
<tr>
<td>unit, counit</td>
<td>8</td>
</tr>
<tr>
<td>alpha-equivalence</td>
<td>42</td>
</tr>
<tr>
<td>arrow</td>
<td>6</td>
</tr>
<tr>
<td>axiomatic equivalence</td>
<td>45, 94, 123</td>
</tr>
<tr>
<td>$B_\sigma$</td>
<td>37</td>
</tr>
<tr>
<td>basis along $x,y,z$</td>
<td>25</td>
</tr>
<tr>
<td>Bell's algorithm</td>
<td>27</td>
</tr>
<tr>
<td>Bell's inequalities</td>
<td>27</td>
</tr>
<tr>
<td>Bloch sphere</td>
<td>22, 27</td>
</tr>
<tr>
<td>BNF</td>
<td>37</td>
</tr>
<tr>
<td>bound variable</td>
<td>42, 55</td>
</tr>
<tr>
<td>bra</td>
<td>24</td>
</tr>
<tr>
<td>$C_\lambda$</td>
<td>128</td>
</tr>
<tr>
<td>call-by-name</td>
<td>45</td>
</tr>
<tr>
<td>call-by-value</td>
<td>49</td>
</tr>
<tr>
<td>canonical first-order representation</td>
<td>111</td>
</tr>
<tr>
<td>Cat</td>
<td>4</td>
</tr>
<tr>
<td>categorical semantics</td>
<td>171</td>
</tr>
<tr>
<td>category</td>
<td>6</td>
</tr>
<tr>
<td>cartesian category</td>
<td>111</td>
</tr>
<tr>
<td>cartesian closed</td>
<td>57</td>
</tr>
<tr>
<td>equivalence</td>
<td>8</td>
</tr>
<tr>
<td>functor category</td>
<td>8</td>
</tr>
<tr>
<td>linear</td>
<td>53</td>
</tr>
<tr>
<td>linear-non-linear</td>
<td>55</td>
</tr>
<tr>
<td>opposite category</td>
<td>6</td>
</tr>
<tr>
<td>product category</td>
<td>8</td>
</tr>
<tr>
<td>small, locally small</td>
<td>8</td>
</tr>
<tr>
<td>trivial category</td>
<td>8</td>
</tr>
<tr>
<td>characteristic matrix</td>
<td>20, 38</td>
</tr>
<tr>
<td>Church-Rosser theorem</td>
<td>101</td>
</tr>
<tr>
<td>Church-style</td>
<td>36</td>
</tr>
<tr>
<td>classical object</td>
<td>57</td>
</tr>
<tr>
<td>classical objects</td>
<td>57</td>
</tr>
<tr>
<td>co-Eilenberg-Moore category</td>
<td>12</td>
</tr>
<tr>
<td>co-Kleisli category</td>
<td>11</td>
</tr>
<tr>
<td>coalgebra</td>
<td>12</td>
</tr>
<tr>
<td>coherence map</td>
<td>14</td>
</tr>
<tr>
<td>commutation of diagrams</td>
<td>8</td>
</tr>
<tr>
<td>commutative comonoid</td>
<td>14</td>
</tr>
<tr>
<td>comonad</td>
<td>111</td>
</tr>
<tr>
<td>idempotent</td>
<td>140</td>
</tr>
<tr>
<td>coherence properties</td>
<td>101</td>
</tr>
<tr>
<td>completely positive map</td>
<td>20</td>
</tr>
<tr>
<td>completeness</td>
<td>48, 199</td>
</tr>
<tr>
<td>composition</td>
<td>5</td>
</tr>
<tr>
<td>computation</td>
<td>50</td>
</tr>
<tr>
<td>category of</td>
<td>37</td>
</tr>
<tr>
<td>concurrent quantum computation</td>
<td>34</td>
</tr>
<tr>
<td>consistency</td>
<td>59</td>
</tr>
<tr>
<td>context</td>
<td>43</td>
</tr>
<tr>
<td>contraction</td>
<td>26</td>
</tr>
<tr>
<td>controlled gate</td>
<td>24</td>
</tr>
<tr>
<td>controlled-not gate</td>
<td>24</td>
</tr>
<tr>
<td>coproduct</td>
<td>47</td>
</tr>
<tr>
<td>binary</td>
<td>106</td>
</tr>
<tr>
<td>copying</td>
<td>26</td>
</tr>
<tr>
<td>CPM</td>
<td>37</td>
</tr>
<tr>
<td>Curry-Howard isomorphism</td>
<td>16</td>
</tr>
<tr>
<td>Curry-style</td>
<td>36</td>
</tr>
<tr>
<td>dagger category</td>
<td>36</td>
</tr>
<tr>
<td>compact-closed</td>
<td>56</td>
</tr>
<tr>
<td>degree of a term</td>
<td>101</td>
</tr>
<tr>
<td>a type</td>
<td>161</td>
</tr>
<tr>
<td>denotation</td>
<td>88, 86</td>
</tr>
<tr>
<td>denotational equivalence</td>
<td>90</td>
</tr>
<tr>
<td>denotational semantics</td>
<td>88</td>
</tr>
<tr>
<td>dense-coding algorithm</td>
<td>30</td>
</tr>
<tr>
<td>density matrix</td>
<td>18</td>
</tr>
<tr>
<td>Deutsch Algorithm</td>
<td>31</td>
</tr>
<tr>
<td>Deutsch algorithm</td>
<td>31</td>
</tr>
<tr>
<td>diagonal structure</td>
<td>12</td>
</tr>
<tr>
<td>207</td>
<td></td>
</tr>
</tbody>
</table>
Dirac convention, 23
dummy variable, 115

Einstein locality criterion, 26
entanglement, 26
equational logic, 126
erasure operation, 111
error state, 59
evaluation strategy, 56
exchange gate, 24
faithful, 4
fixed point, 76
free coalgebra, 12
free variable, 72
full, 4
full abstraction, 96
full embedding, 7
fullness, 78
functional, 18
functor
  diagonal functor, 4
  identity functor, 4
  terminal functor, 7
H
  Hadamard gate, 24
  height of a term, 160
  hermitian form, 17
  hidden variable theory, 26
  Hilbert space, 18
  homset, 4
identity, 4
induced tensor, 116
initial object, 4
intermediate neutral value, 159
interpretation, 174
intuitionistic Linear Logic, 51
intuitionistic logic, 46
isomorphism, 6
ket, 23
Kleisli category, 10
Kleisli exponential, 50
Kleisli triple, 10
Kraus Representation Theorem, 20
lambda calculus, 81
lambda-term
  closed, 12
  combinator, 14
  indexed, 110
  open, 12
  operator, 13
  variables, 11
length, 79
linear category, 51
linear category for duplication, 107
linear exponential comonad, 52
linear lambda calculus, 70
linear logic, 51
Löwner order, 20
map, 4
measure of a term, 160
measurement operator, 80
measurements, 28
mixed state, 26
mixed strategy, 57
monad, 10
  commutative strong, 30
  computational, 80
  strong, 30
monoidal category, 13
  strict, 13
  symmetric, 13
monoidal comonad, 16
  symmetric, 16
monoidal functor
  lax, symmetric, strong, 14
morphism, 6
Naimark Theorem, 24
natural isomorphism, 4
natural transformation, 4
  composition, 5
  identity, 5
  monoidal, 10
NC
  neutral term, 149
no-cloning, 20
norm, 17
  induced norm, 18
  normal form, 18
  normalization, 79
  Theorem, 84
  normed vector space, 18
not gate, 24
i-th number of a term, 163
objects, 6
observable, 23
operational context, 95
    formal, 95
    typed, 95
operational equivalence, 95
operational semantics, 75
    operator, 18
        adjoint, 18
        hermitian, 18
        positive, 18
        self adjoint, 18
partial trace, 21, 39
Pauli matrices, 21
phase-shift gate, 24
Φ, 38
placeholder, 110
positive definite, 17
positive map, 19
probabilistic reduction system, 95
    product, 95
        binary, 10
        product category, 7
program, 62
    progress, 45, 63, 78
Q, 38
QML, 38
QRAM model, 35
quantum array, 56
quantum bit, 23
quantum circuit, 25, 32
quantum closure, 56
    closed, 92
    well-typed, 92
quantum computation, 17
    measurement based, 34
    models of, 34
quantum flow-chart language, 57
quantum Turing machine, 35
quantum value state, 59
qubit, 23
ray, 21
reachability, 93
reduction rules, 13
    β-reduction, 13
    η-reduction, 13
    reduction strategy, 19
rewrite system
number one, 159
number two, 165
safety properties, 76, 77
scalar product, 17
sesquilinear form, 74
Set, 8
    side effect, 48
    signature, 57
    §-size, 91
    small step semantics, 75
Solovay-Kitaev Theorem, 24
soundness, 158, 165, 188
Spectral Theorem, 18
subject reduction, 110, 111
substitution, 18, 52, 118
subtyping Lemma, 181, 182, 183
    subtyping relation, 181, 182
    superoperator, 201, 206
T-exponential, 50
    teleportation algorithm, 28, 64
    tensor product of vector spaces, 181
    tensorial strength, 49
    terminal object, 9
    tr_k, 21
    tr_n, 21
trace characteristic matrix tuple, 59
    type casting, 116
    type inference algorithm, 63
    type system, 44, 60, 108, 109
    typing context, 13, 110
    typing derivation, 14
    typing judgement, 13, 111
        valid, 14
    typing rules, 13, 111
    typing tree, 13
U_C, 24
    unitary, 18
unitary gates, 24
value, 50
    category of, 50
van Tonder’s lambda calculus, 33
weakening, 51