# INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

**The quality of this reproduction is dependent upon the quality of the copy submitted.** Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI®

Université d'Ottawa · University of Ottawa

# MODAL AND FIXPOINT LINEAR LOGIC

By
Alan J. Martin, B.Sc.
September 2002

A Thesis
submitted to the School of Graduate Studies and Research
in partial fulfillment of the requirements
for the degree of
Master of Science in Mathematics[1]

© Copyright 2002
by Alan J. Martin, B.Sc., Ottawa, Canada

---

[1] The M.Sc. Program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-76612-8

Canada

# Abstract

This thesis provides adaptations of the algebraic and relational semantics of modal logic to model J.-Y. Girard's linear logic extended with general modalities. This work extends the work of M. D'Agostino, D. Gabbay, and A. Russo on modalities in implication systems, which include a fragment of linear logic, and the work of J.-Y. Girard on phase semantics for linear logic. We develop deductive systems based on the Gentzen-style sequent calculi of Ohnishi and Matsumoto and the indexed sequents of Mints, and prove cut-elimination properties. We show that semantics and deductive systems that are equivalent for classical modal logic become nonequivalent when adapted to linear logic. We also provide a semantics based on Girard's phase semantics for the fixpoint operators of the modal mu-calculus, developed by D. Kozen, E.A. Emerson, E. Clarke, and others, in linear logic, and consider the translation of Y. Lafont's exponentials with the Free Storage rule into linear logic with fixpoint operators.

# Acknowledgements

I would like to thank my supervisor, Richard Blute, for his advice and support. I would also like to thank the Natural Sciences and Engineering Research Council (NSERC) and the University of Ottawa for their financial support.

# Contents

# Chapter 1

# Introduction

Linear logic was introduced by Girard in 1987 [11] as a new tradition for logic comparable to intuitionistic or classical logic. Linear logic grew out of Girard's work in domain theory, in which the operations of linear logic were used as a simplification and decomposition of the operations of intuitionistic logic. This semantics has been developed into the semantics of coherent spaces, described by Girard in [12].

Linear logic can be thought of as a logic of resources, in which formulas are consumed when they are used to deduce new formulas via rules such as *modus ponens*. Whereas classically a formula can be used as many times as it is needed, in linear logic the ability to reuse a formula is controlled by connectives called the exponentials, which are a kind of modality enriched with the structural rules of contraction and weakening.

Although the exponentials are a kind of modality, little research has been done on modalities in linear logic in general. D'Agostino et al. [9] considered modalities in general implication systems that include a variant of linear logic, and some work on the exponentials by Martini and Masini [22] has involved the removal of structural rules, thus causing the exponentials to resemble ordinary modalities.

The theory of modalities in classical logic is a very old subject, going back at least as far as the work of Lewis in 1918. A good mathematical and historical introduction to the subject is Blackburn et al. [2]. Modal logic has been studied from several different perspectives. Originally it meant the logic of necessity and possibility, and it was motivated in part by a dissatisfaction with the classical notion of implication which admits such seemingly absurd statements as "$2+2=5$ implies the Axiom of Choice" which do not reflect any notion of causality. Much of the early research on modal logic was focused on the syntactic study of various deductive systems.

More recent work on modal logic has centered on the relational semantics developed by Kripke in 1959–1963. Soundness and completeness theorems for various deductive systems with respect to corresponding classes of models have been proven. The failure of certain axioms to admit soundness and completeness for a class of models has led to the development of an algebraic approach to modal logic, based on Boolean algebras for classical logic. Proof theory has also been developed for modal logic, such as the sequent systems of Ohnishi and Matsumoto [23, 24] which satisfy cut-elimination theorems.

Fixpoint operators have been used to add expressive power to modal and temporal logics since the work of Emerson and Clarke [10] and Kozen [17]. The multi-modal **K** logic with fixpoint operators is known as the modal mu-calculus, and it has been used primarily in model-checking applications (see, for example, [8]). More recently completeness of the axiomatization proposed by Kozen in [17] was proved by Walukiewicz in [29]. Proof theory of modal mu-calculus is a relatively new subject, with the work of Aldwinckle and Cockett [1] appearing to be the only work to consider cut-elimination in deductive systems for modal mu-calculus.

We are interested in considering the theory of modal logic in linear logic, and determining to what extent modalities behave similarly or differently in linear logic as compared with classical logic. We develop a variety of systems for modal linear logic, generalizing the algebraic semantics and the relational semantics of classical modal logic. The algebraic semantics for modalities in linear logic builds on the earlier work by D'Agostino et al. [9] and Martini and Masini [22], and the corresponding deductive system builds on the work of Ohnishi and Matsumoto [23, 24]. The relational semantics, on the other hand, does not appear to have been considered previously in linear logic in the form that we develop. The corresponding deductive system also appears to be new, although it is based on the technique of indexed sequents which has been used in classical modal logic, for instance by Braüner [5].

We are also interested in the possibility of adding fixpoint operators to linear logic, whether with or without modalities. This does not appear to have been considered before, although categorical semantics involving fixed points have been developed [18]. Together with modalities, fixpoint operators allow features of temporal logics to be introduced into linear logic, creating a logic of resources and time. Even without the use of modalities, fixpoint operators allow new possibilities for controlling the reuse of formulas, since fixpoint formulas can translate the system of linear logic with free storage described in Chapter 12 of Troelstra [28] and based on Lafont's work in [18].

The work is divided into the following chapters:

**Chapter 2: Linear Logic** We discuss those aspects of the semantics and proof theory of linear logic that are relevant for our development of modal and fixpoint linear logics. The main topics are the sequent calculus and phase semantics for linear logic, and the corresponding results of soundness, completeness, and cut-elimination.

**Chapter 3: Modal Logic** We review those aspects of the theory of modal logic that are to be adapted to the linear logic case. These consist of the Kripke semantics, deductive systems (especially sequent calculi), algebraic semantics, and soundness and completeness theorems. We also consider temporal logics as a special case of modal logic.

**Chapter 4: Modal Mu-Calculus** We introduce the modal mu-calculus as an extension of modal and temporal logics, and describe its semantics, deductive systems, and proof-theoretical properties of soundness, completeness, and cut-elimination.

**Chapter 5: Modal Linear Logic** We construct our algebraic and relational semantics for modal linear logic, together with corresponding deductive systems that we prove sound and complete. We then compare the resulting logics and prove that they define distinct linear logic versions of a single classical modal logic, **KD**.

**Chapter 6: Fixpoint Linear Logic** We construct a semantics based on the phase semantics for linear logic with fixpoint operators, and present a deductive system

> based on Kozen's axiomatization for the modal mu-calculus. We then consider proof-theoretical issues, and present a rewrite system that can translate the cut-elimination of linear logic, although its normal forms are not entirely cut-free and weak normalization remains an open question. Finally, we consider translations of linear logic, with and without free storage, into linear logic with fixpoint operators.

What we have achieved in this thesis is to develop in detail semantics and deductive systems for modalities in linear logic, extending the work by D'Agostino et al. [9] and Martini and Masini [22]. We have shown that the additional distinctions of linear logic allow the possibility of distinct logics that correspond to a single classical modal logic, while satisfying reasonable proof-theoretic properties.

We have also shown that the fixpoint operators of modal mu-calculus can be interpreted in the phase semantics of linear logic in such a way that a sequent calculus presentation of Kozen's axioms for the the mu-calculus [17] is sound. We have shown that it is possible to translate linear logic with the exponentials into linear logic with fixpoint operators via linear logic with the Free Storage rule [18, 28], translating formulas, proofs, and cut-elimination steps.

# Chapter 2

# Linear Logic

## 2.1 History and Motivation

Linear logic was developed by Jean-Yves Girard starting in 1986–1987 in response to results obtained during the study of a model of intuitionistic logic, a variant of *Scott domains.* It was developed as an "extension of usual logic" [12], by which it is meant that linear logic should allow finer distinctions than classical or intuitionistic logic, while allowing those logics to be recovered by translations. In this way it follows in the tradition of intuitionistic logic, which allows us to make distinctions, particularly between constructive and nonconstructive proof techniques, that are not present in classical logic.

This chapter is based on [11, 12, 28]. Girard's initial paper [11] on linear logic describes the sequent calculus, phase semantics, and proof-nets for linear logic. Some more recent developments are described in Girard's paper [12], particularly coherent spaces and an alternative formulation of the phase semantics for the exponentials. The book [28] by Troelstra is a good survey of a variety of developments in linear logic, including in particular categorical semantics.

The key feature of linear logic that distinguishes it from earlier logics is *resource-sensitivity*: A formula no longer represents a stable fact or 'situation', but instead a resource; and such a resource is consumed in an implication. That is, in linear logic, if we have $A$ together with $A$ implies $B$, then we can conclude $B$, but both of the original formulas are used up in the process and cannot be used again.

Starting with the idea of resource-sensitivity and implication as consumption of resources, we can determine how a sequent calculus for linear logic must differ from one for classical logic. Suppose, for example, that $a$ denotes a dollar and $b$ denotes a can of soda. We might have several dollars, which would be denoted by several copies of $a$. A vendor might offer to sell us a can of soda for a dollar; this would be denoted by the implication $a \multimap b$. Again, there might be several such formulas, since the vendor might have several cans of soda. Now the sequent $a, a \multimap b \vdash b$ denotes the transaction of purchasing a can of soda.

We find that some of the rules of classical sequent calculus no longer make sense in this setting. For instance, if soda cost two dollars, we might have $a, a, A \vdash b$ for some $A$; using the contraction rule, we could conclude $a, A \vdash b$—we could get for one dollar whatever we could get for two. Thus, the contraction rule clearly must be discarded in a resource-sensitive logic.

The issue of weakening is a bit less clear. Weakening essentially amounts to being able to 'throw away' resources. A logic could reasonably be considered resource-sensitive while still allowing weakening. (Indeed, there are variants of linear logic called *affine logic* that do just that.) However, another objective in developing linear logic was to have an involutive negation, with $A$ and $\neg A$ representing, perhaps, the two sides of a transaction; so if $A$ represents a resource, then $\neg A$ represents the obligation to provide it, which we certainly should not be able to throw away! So weakening must also be discarded.

The remaining structural rule, exchange, is also open to question. In usual linear logic it is retained; the order of formulas in a sequent is not meaningful. However, there are *noncommutative linear logics* that discard or restrict this rule.

Now that we have decided on the structural rules, we consider the logical rules. Here we find that some care is required. For instance, there are two traditions for the presentation of a sequent-calculus rule for conjunction in classical or intuitionistic logic:

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \wedge B}\wedge_m \qquad \text{and} \qquad \frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B}\wedge_a$$

These two rules are interderivable via weakening and contraction:

$$\dfrac{\dfrac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, \Gamma, A \wedge B}\,\wedge_m}{\vdash \Gamma, A \wedge B}\,\mathsf{C}^{\bullet} \qquad \dfrac{\dfrac{\vdash \Gamma, A}{\vdash \Gamma, \Delta, A}\,\mathsf{W}^{\bullet} \quad \dfrac{\vdash \Delta, B}{\vdash \Gamma, \Delta, B}\,\mathsf{W}^{\bullet}}{\vdash \Gamma, \Delta, A \wedge B}\,\wedge_a$$

On the other hand, in linear logic, they are not interderivable. So which should we adopt? The solution adopted by Girard was to split the connective $\wedge$ itself into two conjunctive connectives, the additive & (with) and the multiplicative $\otimes$ (tensor), corresponding to the two rules. Similarly there are two disjunctions, the additive $\oplus$ (plus) and the multiplicative $\parr$ (par). The constants $\top$ and $\bot$ of classical logic are also split into additive and multiplicative versions for similar reasons, and the implication of linear logic is written with a different symbol $\multimap$ (linear implication).

Linear logic was not the first logic to be based on the idea of dumping structural rules (such logics are called **substructural logics**). A summary of earlier such efforts can be found in Troelstra [28], section 2.8. These include logics that discard weakening only (*relevance logics*), logics that discard contraction only (*BCK-logics*), and logics that discard all three structural rules (*categorial logics*).

Linear logic has found diverse applications, some of which are only remotely connected to the idea of a resource-sensitive logic. Its *phase space* semantics, which is an ordinary semantics of formulas, much like Boolean algebras, for which the logic is sound and complete, has been useful primarily for theoretical applications such as Yves Lafont's proof of the finite model property for MALL [20].

The semantics of linear logic proofs called *coherent spaces*, on the other hand, has led to interpretations of linear logic in several well-known categorical structures, such as symmetric monoidal categories and $*$-autonomous categories, in which new category-theoretic ideas and results have developed from the linear logic approach.

Linear logic also has (at least in the intuitionistic case) a lambda-calculus-like semantics of proof terms, presented by Lafont in [18]. This semantics can in theory be used to develop new functional programming languages. In practice, however, research on programming languages based on linear logic has centered mainly on logic programming languages such as Lolli, developed by Hodas and Miller [14], and the related language Forum.

## 2.2 Syntax

There are several alternative notations in use for linear logic. We use the notation of [11].

**Definition 2.1** *The formulas of propositional linear logic are defined by the following Backus-Naur Form (BNF):*

$$\begin{array}{lcl}\textbf{formula}, A, B & ::= & \textbf{atom} \mid \textbf{atom}^{\perp} \mid A \otimes B \mid A \mathbin{\rotatebox[origin=c]{180}{\&}} B \mid A \mathbin{\&} B \mid A \oplus B \\ & & \mid \mathbf{1} \mid \perp \mid \top \mid \mathbf{0} \mid\, !A \mid\, ?A\end{array}$$

*An involutive operation of negation* $^{\perp}$ *is defined by* $a^{\perp\perp} := a$ *and de Morgan dualities between* $\otimes$ *and* $\mathbin{\rotatebox[origin=c]{180}{\&}}$, $\&$ *and* $\oplus$, $\mathbf{1}$ *and* $\perp$, $\top$ *and* $\mathbf{0}$, *and* $!$ *and* $?$. *(That is,* $(A \otimes B)^{\perp} := (A^{\perp}) \mathbin{\rotatebox[origin=c]{180}{\&}} (B^{\perp})$, $\mathbf{1}^{\perp} := \perp$, *and* $(!A)^{\perp} := ?(A^{\perp})$*; the other cases are similar.) An operation of linear implication* $\multimap$ *is defined by* $A \multimap B := A^{\perp} \mathbin{\rotatebox[origin=c]{180}{\&}} B$.

The connectives $\otimes$, $\mathbin{\rotatebox[origin=c]{180}{\&}}$, $\mathbf{1}$, and $\perp$ are called the *multiplicatives*; $\&$, $\oplus$, $\top$, and $\mathbf{0}$ are called the *additives*; and ! and ? are called the *exponentials*. Letters $a$, $b$, ... denote atoms, and letters $A$, $B$, $C$, ... denote formulas. Atoms are taken from a set Atoms, which is unspecified but sometimes assumed to be infinite.

Finite sequences of formulas, which may be empty, are denoted $\Gamma$, $\Delta$, $\Lambda$, .... Empty sequences are denoted by blank space, where it is clear that a sequence is expected (i.e., in sequents). It will frequently be useful to apply a unary operation componentwise to the formulas in a sequence, so if $\Gamma = A_1, A_2, \ldots, A_n$ (this notation will be used even when $n = 0$ and the sequence is empty), and $\diamond$ is a unary operation, then $\diamond\Gamma$ denotes $\diamond A_1, \diamond A_2, \ldots, \diamond A_n$. For instance, $\Gamma^{\perp}$ denotes the sequence consisting of the negations of the formulas in $\Gamma$.

**Convention 2.2** *Negation is considered to bind tighter than the exponentials, which in turn bind tighter than the binary connectives. Parentheses are used to override these binding priorities.*

Several fragments and extensions of propositional linear logic are also of interest:

- (Propositional) *multiplicative-additive linear logic* (MALL) is the fragment of the logic excluding the exponentials.
- *Multiplicative linear logic* (MLL) is the fragment of MALL excluding also the additives.
- *Multiplicative-exponential linear logic* (MELL) is the fragment of linear logic excluding the additives.
- Any of these logics may be augmented with first-order or higher-order quantifiers, or atoms may be excluded (*constant-only* logics), or constants may be excluded.

On the other hand, sublogics excluding the multiplicatives have been less studied. It seems likely that the reason for this is that in the sequent calculus, the commas between formulas are interpreted by implicit multiplicatives ($\otimes$ on the left, $\invamp$ on the right; and $\vdash$ is interpreted by $\multimap$), so the meaning of the structural rules is in this way dependent on the multiplicatives. The multiplicatives are also responsible for some of linear logic's most distinctive semantic features: informally, the ability to quantify resources; formally, the monoid structure of the phase semantics.

**Definition 2.3** *A* literal *is an atom (a* positive literal*) or a negated atom (a* negative literal*). The* principal connective *of a formula that is not a literal is the connective occurring in the (unique) BNF clause matching the formula.*

Letters $\alpha$, $\beta$, ... denote literals. Positive and negative literals can and will be treated uniformly, except when interpreting formulas in a semantics where a choice must be made for the base case.

**Definition 2.4** *An occurrence of a literal $\alpha$ in a formula is called a* positive occurrence *of $\alpha$ or a* negative occurrence *of $\alpha^{\perp}$. A formula $A$ is called* positive *(resp.* negative*) in a literal $\alpha$ if all occurrences of $\alpha$ in $A$ are positive (negative). The set of atoms occurring (positively or negatively) in a formula $A$ is denoted* $\mathrm{At}(A)$.

Formulas are defined here in such a way that the negation symbol $^\perp$ occurs only applied to atoms. Such formulas are said to be in *positive normal form*; it is clear that formulas using negation as a connective can be translated into positive normal form using the defined operation of negation. Working with positive normal form is typical both in linear logic [11] and in modal mu-calculus [4]. It has the advantage of simplifying deductive systems, cut-elimination proofs, etc. by not having to deal with an explicit negation connective. Positive normal form can also be used for classical logic, but not for intuitionistic logic due to that logic's lack of involutive negation and de Morgan laws.

## 2.3 Deductive Systems

Just as there are a variety of deductive systems for classical logic, various deductive systems can be constructed for linear logic. Two such systems are of particular interest for linear logic: sequent calculus and proof-nets. However, most of the other traditions for deductive systems (such as Hilbert systems and natural deduction) can be transferred to linear logic; see, for example, Troelstra [28].

The sequent calculus was historically the first to be developed, and it is the easiest to compare with the corresponding system for classical logic, because the differences consist of discarding structural rules.

Proof-nets were developed by Girard [11] as a linear analogue of classical natural deduction. The intention was to obtain a confluent normalization (cut-elimination) process by eliminating unnecessary sequencing of commuting rules. Proof-nets work best for the multiplicative fragment: they have been defined for the full logic, but many nice properties hold only for the multiplicative fragment and there has been some uncertainty as to the best way to handle the rest of the logic. Proof-nets remain a major area of linear logic research.

Only the sequent calculus will be considered here, because it is simple to define and work with, it supports a notion of normalization (cut-elimination), and the advantages of the other systems are not important here.

**Definition 2.5** *Linear logic sequent calculus (LLSC) is a deductive system on sequents $\vdash \Gamma$, where $\Gamma$ is a sequence of formulas. Linear logic sequent calculus consists of the following axioms and inference rules:*

$$\frac{}{\vdash A, A^{\perp}}\,\text{Id} \qquad \frac{\vdash \Gamma, A \quad \vdash A^{\perp}, \Delta}{\vdash \Gamma, \Delta}\,\text{Cut} \qquad \frac{\vdash \Gamma}{\vdash \sigma(\Gamma)}\,\text{Ex} \quad (\sigma \textit{ a permutation})$$

$$\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \mathbin{\&} B}\,\& \qquad \frac{}{\vdash \Gamma, \top}\,\top \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\,\oplus_1 \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\,\oplus_2$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\,\otimes \qquad \frac{}{\vdash \mathbf{1}}\,\mathbf{1} \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\,\parr \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \bot}\,\bot$$

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, ?A}\,\text{D} \qquad \frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A}\,\text{S} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, ?A}\,\text{W} \qquad \frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}\,\text{C}$$

For the additive rules, the contexts match for all the premises and the conclusion; for the multiplicative rules, on the other hand, the contexts of the premises are concatenated to form the context of the conclusion. This is a reasonable way to define the terms 'additive' and 'multiplicative', although in some cases ($\parr$ vs. $\oplus$) there are other differences forced by duality.

The subscript on the $\oplus$ rules will sometimes be dropped when it is clear which rule is intended. However, the two rules are distinct.

**Definition 2.6** *An instance of the* Cut *rule as shown above is called a cut on $A$ (or on $A^{\perp}$). A premise formula of an inference rule that does not occur as a subformula of the conclusion is called a cut formula; the only cut formulas in LLSC are $A$ and $A^{\perp}$ in the* Cut *rule.*

Just as there are a number of variations on the definition of linear logic formulas, there are several variants of linear logic sequent calculus:

- Sequent calculi for fragments of the logic: MALL sequent calculus, etc.

  As a consequence of the cut-elimination theorem all provable sequents in such a fragment have proofs entirely within the fragment. So it is enough to discard the rules for connectives not occurring in the fragment.

- Two-sided sequent calculus: Here sequents are of the form $\Gamma \vdash \Delta$ where $\Gamma$ and $\Delta$ are both sequences of formulas. Negation is treated as a connective with its own introduction rules:

  $$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash A^{\perp}, \Delta}\,{\scriptstyle \perp_{R}} \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma, A^{\perp} \vdash \Delta}\,{\scriptstyle \perp_{L}}$$

  Each connective rule is split into a right rule, which is the same as the one-sided rule except for the possibility of contexts on both sides, and a left rule, which behaves like the one-sided rule for the de Morgan dual connective. For instance, the rules for $\otimes$ are:

  $$\frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \otimes B, \Delta, \Delta'}\,{\scriptstyle \otimes_{R}} \qquad \frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \otimes B \vdash \Delta}\,{\scriptstyle \otimes_{L}}$$

  The identity axiom and cut rule are also written differently in the two-sided sequent calculus:

  $$\frac{}{A \vdash A}\,{\scriptstyle \mathrm{Id}} \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,{\scriptstyle \mathrm{Cut}}$$

  The exchange rule applies separate permutations on the left and the right.

  Sequent calculi were originally developed by Gentzen in this two-sided form. The one-sided sequent calculus is used as a notational convenience, together with positive normal form. However, the one-sided calculus has the disadvantage of sometimes obscuring the structure or significance of a derivation. (The Identity and Cut rules are good examples.) This problem can often be avoided, without sacrificing the convenience of one-sided sequents, by using $\Gamma \vdash \Delta$ simply as an alternate notation for $\vdash \Gamma^{\perp}, \Delta$. We will take this approach in the following sections except where otherwise noted.

- Sequent calculi on multisets of formulas: A sequent $\vdash \Gamma$ can be treated as a multiset of formulas, rather than a sequence. This gives an equivalent deductive system as a result of the Exchange rule, and that rule is no longer needed. This approach is useful in the proof of completeness for phase semantics. It does have disadvantages, however, notably the fact that it erases distinctions between nonequivalent proofs when certain semantics of proofs are considered.

In the following sections, the exchange rule will often be ignored, even when a multiset formulation is not explicitly used.

- *Noncommutative linear logic*: There are several variants of linear logic that restrict or eliminate the exchange rule. This requires some care in writing the rules, as equivalent ways of writing the LLSC rules become nonequivalent without Exchange, much the same as equivalent ways of writing the classical sequent calculus rules become nonequivalent without Weakening and Contraction. In some cases this can lead to further splitting of connectives such as by having two negations.

- *Intuitionistic linear logic*: The intuitionistic linear logic sequent calculus is a two-sided sequent calculus in which at most one formula is permitted on the right side of a sequent. The definition of formulas is also different: the connectives of intuitionistic linear logic are $\otimes$, $\&$, $\oplus$, $\mathbf{1}$, $\top$, $\mathbf{0}$, $!$, and linear implication $\multimap$; negation is not built in even for atoms. The constant $\bot$ may also be included, in which case negation can be defined by $A^{\bot} := A \multimap \bot$, which is not involutive. The connectives $⅋$ and $?$, whose sequent rules depend critically on the use of multiple formulas on the right, are omitted. The rules are the usual two-sided rules plus the following rules for $\multimap$:

  $$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B}\,{\scriptstyle \multimap\mathrm{R}} \qquad \frac{\Gamma \vdash A \quad \Delta, B \vdash C}{\Gamma, \Delta, A \multimap B \vdash C}\,{\scriptstyle \multimap\mathrm{L}}$$

  Unlike ordinary intuitionistic logic, intuitionistic linear logic does not gain in constructiveness over classical linear logic, as the latter is already constructive; but it does have some interesting semantics that do not extend to semantics for classical linear logic [28]. It also collapses to intuitionistic rather than classical logic if $A$, $!A$, and $?A$ are identified.

The choice of notation $\vdash$ for sequents is somewhat unfortunate. This symbol is traditionally used in the meta-language to denote provability. However, there is no universally accepted alternative symbol to separate the left and right sides of a sequent (or to mark the start of a one-sided sequent): for instance, Troelstra [28] uses

$\Rightarrow$, while Blackburn et al. [2] use $\longrightarrow$. Instead of using one of these notations, we will use $\vdash$ for sequents and no special notation for provability.

## 2.4 Linear Logic as a Resource Logic

In this section we consider an informal semantics of linear logic, which illustrates in what way it is a logic of resources. Most of these ideas are found in Girard [12]; many others have used similar informal semantics in describing linear logic.

In classical and intuitionistic logics, a formula represents a *proposition*, a statement that is in principle true or false. Deductive systems for these logics are concerned with what propositions are necessarily true. The connective $\rightarrow$ allows us to consider preservation of truth, i.e., truth under assumptions.

In linear logic, on the other hand, a formula represents a *resource*. This means, in particular, that a formula cannot automatically be duplicated, as indicated by the lack of an unrestricted Contraction rule. Linear logic also does not assume that resources can be thrown away, which would correspond to unrestricted Weakening. (That this can be the case in the real world is evident from such examples of 'resources' as garbage, debts, etc.) Deductive systems for linear logic are concerned with what resources can be constructed 'out of thin air'; for instance, a coupon to exchange a resource for itself (we consider idealized coupons that require no resources except to back up the offer). The connective $\multimap$, or its implicit sequent version $\vdash$, allows us to consider how resources can be transformed into other resources.

The roles of the intuitionistic linear logic connectives can be described in these terms:

- $A \otimes B$ is the pair of resources $A$ and $B$.
- $A \,\&\, B$ is the choice of resource $A$ or resource $B$.
- $A \oplus B$ is one of $A$ or $B$, which one not being specified.
- $A \multimap B$ is the ability (and obligation) to exchange one $A$ for a $B$.
- $\mathbf{1}$ is nothing (the empty tuple of resources).

- $\top$ is some unspecified collection of resources.
- $\mathbf{0}$ is a choice of any resources at all.
- $!A$ is an unlimited supply of $A$.

Atomic formulas represent arbitrary resources, the structure of which is not to be modeled in linear logic. The interpretation of $\top$ is from its phase semantics interpretation as the $\oplus$ of everything, not from its role as the unit for $\&$ (although it clearly does fulfill the latter role); $\mathbf{0}$ is treated similarly. $A \multimap B$ can be thought of as an idealized coupon in the sense mentioned above, although it can also represent a debt (as in $a \multimap 1$ where $a$ represents a dollar) since it cannot be thrown away unused. An 'unlimited supply' is understood to be divisible, so that $!A \multimap !A \otimes !A$ is valid. Then all of the rules of intuitionistic linear logic are clearly sound for this informal semantics.

Classical linear logic is trickier. There are two problems: the constant $\bot$, which has no obvious meaning, and the assumption of involutivity of negation $((A \multimap \bot) \multimap \bot) \multimap A$. One way to describe classical linear logic is to replace resources with contracts, with rights and obligations for two parties, and to have negation represent *exchange of roles*. This approach is similar to the one used in game semantics, and it explains involutivity of negation quite nicely. It works best, for informal semantics at least, if we require $\mathbf{1} = \bot$. This is a stronger variant of the MIX rule $A \otimes B \vdash A \parr B$; linear logic with MIX and its variants has been studied extensively. Now we can describe the classical linear logic connectives informally:

- $A^\perp$ is $A$ with roles reversed
- $A \otimes B$ is the pair of independent contracts $A$ and $B$.
- $A \parr B$ is the pair of possibly interdependent contracts $A$ and $B$.
- $A \& B$ is the choice of contract $A$ or contract $B$.
- $A \oplus B$ is one of $A$ or $B$, which one not being specified.
- $\mathbf{1}$ is nothing (a contract with no rights or obligations).

- $\mathbf{0}$ is a 'blank cheque', a contract with an arbitrary choice of terms.
- $\top$ is a contract where the other party chooses arbitrary terms.
- $!A$ is a contract allowing the options to terminate it (Weakening), duplicate it (Contraction), or convert it to $A$ (Dereliction).
- $?A$ is a contract allowing the other party the options listed for ! above.

The notion of independent versus dependent contracts is key. We may obtain $A^\perp \parr A$, but not $A^\perp \otimes A$, by asking another party to act as an intermediary, satisfying our rights under $A$ (which are the intermediary's obligations) from our corresponding obligations under $A^\perp$ and vice versa; this is what is meant by dependence of contracts. The validity of the MIX rule represents the fact that we never insist that two contracts are *dependent*, only that they are independent. The invalidity of its converse ensures that circular dependencies cannot be created.

As for classical linear logic without MIX, it is difficult to give it an informal semantics. The additional distinctions that this logic allows can be understood in terms of the correctness conditions for proof-nets due to Danos and Regnier: switchings of proof-nets must always be acyclic, which corresponds to prevention of circular dependencies, but without MIX, they must also be connected. Unfortunately, connectedness of switchings does not seem to have any simple informal meaning.

## 2.5 Syntactic Results

In this section we consider several results concerning the LLSC deductive system: classical collapse, the substitution theorem, cut-elimination, and invertibility of rules.

**Definition 2.7** *The classical collapse of (an extension of) linear logic is obtained by adding the following axiom to the sequent calculus:*

$$\frac{}{\vdash !A^\perp, !A}\,\mathrm{CC}$$

*The classical collapse* $A^C$ *of a formula* $A$ *is defined inductively by* $a^C := a$, $(a^\perp)^C := \neg a$, $\top^C = \mathbf{1}^C := \top$, $\mathbf{0}^C = \perp^C := \perp$, $(A \,\&\, B)^C = (A \otimes B)^C := A^C \wedge B^C$, $(A \oplus B)^C = (A \parr B)^C := A^C \vee B^C$, *and* $(!A)^C = (?A)^C := A^C$.

The CC axiom does not allow Cut to be eliminated, but if the original sequent calculus satisfies cut-elimination, then usually it is possible to axiomatize the resulting logic by a sequent calculus that also satisfies cut-elimination.

As for classical collapse of formulas, it is clearly a surjective map.

**Proposition 2.8** *The following sequents are provable in the classical collapse of linear logic:*

$$!A \dashv\vdash A \dashv\vdash ?A$$

$$A \,\&\, B \dashv\vdash A \otimes B$$

$$A \oplus B \dashv\vdash A \parr B$$

*Furthermore, the classical collapse of linear logic induces, by classical collapse of formulas, a well-defined logic on classical formulas which is equivalent to a version (without implication or negation as connectives) of classical propositional logic.*

**Proof.** The sequents for the exponentials follow from $!A \vdash A$ and $A \vdash ?A$ (proved by Dereliction) and the CC axiom, using Cut. The remaining sequents follow from $!(A \,\&\, B) \dashv\vdash !A \otimes !B$ which is proved as follows [11]:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathrm{Id}}{A \,\&\, B \vdash A}\,\&\mathrm{L}}{!(A \,\&\, B) \vdash A}\,\mathrm{D}}{!(A \,\&\, B) \vdash !A}\,\mathrm{S} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{B \vdash B}\,\mathrm{Id}}{A \,\&\, B \vdash B}\,\&\mathrm{L}}{!(A \,\&\, B) \vdash B}\,\mathrm{D}}{!(A \,\&\, B) \vdash !B}\,\mathrm{S}}{!(A \,\&\, B), !(A \,\&\, B) \vdash !A \otimes !B}\,\otimes\mathrm{R}}{!(A \,\&\, B) \vdash !A \otimes !B}\,\mathrm{C} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathrm{Id}}{!A \vdash A}\,\mathrm{D}}{!A, !B \vdash A}\,\mathrm{W} \qquad \dfrac{\dfrac{\dfrac{}{B \vdash B}\,\mathrm{Id}}{!B \vdash B}\,\mathrm{D}}{!A, !B \vdash B}\,\mathrm{W}}{!A, !B \vdash A \,\&\, B}\,\&\mathrm{R}}{!A, !B \vdash !(A \,\&\, B)}\,\mathrm{S}}{!A \otimes !B \vdash !(A \,\&\, B)}\,\otimes\mathrm{L}$$

Now we define $A^L$ for classical formulas $A$ in such a way that $(A^L)^C = A$, by $(\neg A)^L := (A^L)^\perp$, $(A \wedge B)^L := A^L \,\&\, B^L$, and $(A \vee B)^L := A^L \oplus B^L$. A proof in LLSC with CC corresponds under classical collapse $(-)^C$ to a proof in a variant of classical sequent calculus, whose rules are the rules of LLSC with all formulas classically collapsed. On the other hand, a proof in this variant of classical sequent calculus corresponds under $(-)^L$ to a proof using rules that are derivable in LLSC with CC using the above equivalences. So LLSC with CC induces classical logic via classical collapse of formulas, as was to be proven. □

Another way to collapse linear logic into a classical logic is to add unrestricted Contraction and Weakening. This approach leaves the exponentials as classical modalities. It is also possible to translate classical or intuitionistic logic into linear logic without added axioms; see [12, 28].

**Definition 2.9** *The substitution of* $A_i$ *for* $\alpha_i$ $(1 \leqslant i \leqslant n)$ *in a formula* $B$*, denoted* $B[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n]$*, is defined inductively by*

$$\alpha_i[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n] := A_i,$$
$$\alpha_i^{\perp}[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n] := A_i^{\perp},$$

*preservation of all other literals, and distributivity over all the connectives. No atom may be duplicated among the* $\alpha_i$*. Substitution extends to sequences of formulas in the obvious way.*

*The substitution of* $A_i$ *for* $\alpha_i$ $(1 \leqslant i \leqslant n)$ *in a proof* $\pi$*, denoted* $\pi[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n]$*, is obtained by performing the indicated substitution on each formula occurring in the proof. That the result is a well-formed LLSC proof is clear by inspection of the rules: they are all closed under substitution instances.*

**Theorem 2.10 (Substitution)** *The following is a derivable rule in LLSC with the Identity rule restricted to atomic formulas:*

$$\dfrac{\vdash A_1^{\perp}, A_1' \quad \vdash A_2^{\perp}, A_2' \quad \cdots \quad \vdash A_n^{\perp}, A_n'}{\vdash B^{\perp}[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n], B[A_1'/\alpha_1, A_2'/\alpha_2, \ldots, A_n'/\alpha_n]}\,\mathrm{ST} \qquad (B \textit{ positive in } \alpha_i)$$

**Proof.** The substitution theorem follows by an easy induction using the following derivations:

$$\dfrac{\dfrac{\vdash A^{\perp}, A' \quad \vdash B^{\perp}, B'}{\vdash A^{\perp}, B^{\perp}, A' \otimes B'}\,{\scriptstyle\otimes}}{\vdash A^{\perp} \parr B^{\perp}, A' \otimes B'}\,{\scriptstyle\parr} \qquad \dfrac{\dfrac{\vdash A^{\perp}, A'}{\vdash A^{\perp}, A' \oplus B'}\,{\scriptstyle\oplus} \quad \dfrac{\vdash B^{\perp}, B'}{\vdash B^{\perp}, A' \oplus B'}\,{\scriptstyle\oplus}}{\vdash A^{\perp} \mathbin{\&} B^{\perp}, A' \oplus B'}\,{\scriptstyle\&} \qquad \dfrac{\dfrac{\vdash A^{\perp}, A'}{\vdash A^{\perp}, ?A'}\,{\scriptstyle ?}}{\vdash !A^{\perp}, ?A'}\,{\scriptstyle !}$$

$$\dfrac{\dfrac{}{\vdash \mathbf{1}}\,{\scriptstyle\mathbf{1}}}{\vdash \perp, \mathbf{1}}\,{\scriptstyle\perp} \qquad \dfrac{}{\vdash \top, \mathbf{0}}\,{\scriptstyle\top}$$

These derivations may be treated as derivable rules, denoted $\mathrm{ST}_{\otimes,\parr}$ etc. (or collectively $\mathrm{ST}_*$), from which the general rule ST can be derived.

The base case is when $B$ is a literal; then the ST rule can be derived by its $i^{\text{th}}$ premise if $B = \alpha_i$ for some $i$, or by the Identity rule on atoms otherwise; we cannot have $B = \alpha_i^{\perp}$ by the positivity side condition. Otherwise one of the derived rules above suffices to derive the ST rule from other ST rules on smaller formulas than $B$. ☐

**Corollary 2.11** *The Identity rule on arbitrary formulas is derivable in LLSC with the Identity rule restricted to atomic formulas.*

**Proof.** This is just the case $n = 0$ of the Substitution Theorem. ☐

**Theorem 2.12 (Cut-Elimination)** *Every sequent that is provable in linear logic sequent calculus is provable in LLSC without the Cut rule.*

The proof of this theorem, for any logic, usually takes the form of a construction of a weakly normalizing rewrite system on proofs having the property that normal forms are cut-free. This is not the only way to prove cut-elimination: a semantic proof is given by Okada [25] by proving completeness of the cut-free sequent calculus. However, via the Curry-Howard isomorphism, the cut-elimination rewrite system corresponds to evaluation of terms, so the process itself is important as well as the actual cut-elimination theorem. Further evidence for this comes from categorical semantics of proofs, in which the cut-elimination rewrite rules are semantically sound (i.e., they transform proofs into semantically equivalent proofs).

The proof of normalization has been well treated in the literature. A clear and detailed treatment of cut-elimination in LLSC can be found in [21], and a treatment using a strongly normalizing rewrite system is given in [26] (see also [28]). Girard [11] gives a proof of cut-elimination for proof nets from which cut-elimination for LLSC can be derived. The treatment followed here is based on [21].

The normalization procedure is simplified through the use of an extended version of the Cut rule called Cut!:

$$\frac{\vdash \Gamma, !A \quad \vdash (?A^{\perp})^n, \Delta}{\vdash \Gamma, \Delta}\,\text{Cut!}$$

By convention, this rule will be used only for $n > 1$. This is a derivable rule using Cut and Contraction:

$$\dfrac{\vdash \Gamma, !A \qquad \dfrac{\vdash (?A^{\perp})^n, \Delta}{\vdash ?A^{\perp}, \Delta}\,\mathrm{C}^{*}}{\vdash \Gamma, \Delta}\,\mathrm{Cut}$$

Some rewrite rules will introduce the Cut! rule where it did not occur in the original proof, but the cut-elimination procedure will ultimately eliminate this rule as well as the original Cut rule. This extended Cut rule, which is related to Gentzen's Mix rule, is widely used: three proofs of LLSC cut-elimination in [21, 26, 28] all make use of it.

**Definition 2.13** *A principal formula of a rule is a formula introduced by the rule (i.e., not occurring as a subformula of the premises). By convention, we consider the contracted formula in a Contraction rule to be principal, and we consider the formulas other than $\top$ in the $\top$ rule to be non-principal. Thus, each non-principal formula occurs exactly once in each premise (additive rules) or in one premise (multiplicative rules).*

The definition of principal formula used here is different from the one in [21]. This definition is more usual, except that the ? formulas in the conclusion of the Storage rule are often considered principal as well.

**Definition 2.14** *The degree of an instance of* Cut *or* Cut! *is the number of atoms, negated atoms, and connectives in the cut formulas. Since negation is not a connective, this number is the same for both cut formulas.*

*The degree of a proof is the maximum degree of its* Cut *and* Cut! *rules, or zero if there are none.*

**Definition 2.15** *The cut-elimination rewrite rules are presented in several groups of related rules. The notation* Cut* *is used to denote either* Cut *or* Cut!, *and the notation $A^*$ is used to denote one or more occurrences of $A$, with multiple occurrences permitted only if the principal connective of $A$ is ?.*

*Rewrite rules which apply to cuts on non-principal formulas:*

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \qquad \dfrac{{}^{\pi_2}\dfrac{}{\vdash \Delta, B^*} \quad {}^{\pi_3}\dfrac{}{\vdash A^{\perp*}, B^{\perp*}, \Lambda}}{\vdash A^{\perp*}, \Delta, \Lambda}\,\text{Cut}*}{\vdash \Gamma, \Delta, \Lambda}\,\text{Cut}*$$

$$\Downarrow$$

$$\dfrac{{}^{\pi_2}\dfrac{}{\vdash \Delta, B^*} \qquad \dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad {}^{\pi_3}\dfrac{}{\vdash A^{\perp}, B^{\perp*}, \Lambda}}{\vdash \Gamma, B^{\perp*}, \Lambda}\,\text{Cut}*}{\vdash \Gamma, \Delta, \Lambda}\,\text{Cut}*$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \qquad \dfrac{{}^{\pi_2}\dfrac{}{\vdash A^{\perp}, \Delta, B} \quad {}^{\pi_3}\dfrac{}{\vdash A^{\perp}, \Delta, C}}{\vdash A^{\perp*}, \Delta, B \mathbin{\&} C}\,\&}{\vdash \Gamma, \Delta, B \mathbin{\&} C}\,\text{Cut}*$$

$$\Downarrow$$

$$\dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad {}^{\pi_2}\dfrac{}{\vdash A^{\perp*}, \Delta, B}}{\vdash \Gamma, \Delta, B}\,\text{Cut}* \qquad \dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad {}^{\pi_3}\dfrac{}{\vdash A^{\perp*}, \Delta, C}}{\vdash \Gamma, \Delta, C}\,\text{Cut}*}{\vdash \Gamma, \Delta, B \mathbin{\&} C}\,\&$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad \dfrac{}{\vdash A^{\perp*}, \Delta, \top}\,\top}{\vdash \Gamma, \Delta, \top}\,\text{Cut}* \quad \Longrightarrow \quad \dfrac{}{\vdash \Gamma, \Delta, \top}\,\top$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad \dfrac{{}^{\pi_2}\dfrac{}{\vdash A^{\perp*}, \Delta, B}}{\vdash A^{\perp*}, \Delta, B \oplus C}\,\oplus_1}{\vdash \Gamma, \Delta, B \oplus C}\,\text{Cut}* \quad \Longrightarrow \quad \dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad {}^{\pi_2}\dfrac{}{\vdash A^{\perp*}, \Delta, B}}{\vdash \Gamma, \Delta, B}\,\text{Cut}*}{\vdash \Gamma, \Delta, B \oplus C}\,\oplus_1$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad \dfrac{{}^{\pi_2}\dfrac{}{\vdash A^{\perp*}, \Delta, C}}{\vdash A^{\perp*}, \Delta, B \oplus C}\,\oplus_2}{\vdash \Gamma, \Delta, B \oplus C}\,\text{Cut}* \quad \Longrightarrow \quad \dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad {}^{\pi_2}\dfrac{}{\vdash A^{\perp*}, \Delta, C}}{\vdash \Gamma, \Delta, C}\,\text{Cut}*}{\vdash \Gamma, \Delta, B \oplus C}\,\oplus_2$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad \dfrac{{}^{\pi_2}\dfrac{}{\vdash A^{\perp*}, \Delta, B} \quad {}^{\pi_3}\dfrac{}{\vdash \Lambda, C}}{\vdash A^{\perp*}, \Delta, \Lambda, B \otimes C}\,\otimes}{\vdash \Gamma, \Delta, \Lambda, B \otimes C}\,\text{Cut}* \quad \Longrightarrow \quad \dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad {}^{\pi_2}\dfrac{}{\vdash A^{\perp*}, \Delta, B}}{\vdash \Gamma, \Delta, B}\,\text{Cut}* \quad {}^{\pi_3}\dfrac{}{\vdash \Lambda, C}}{\vdash \Gamma, \Delta, \Lambda, B \otimes C}\,\otimes$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad \dfrac{{}^{\pi_2}\dfrac{}{\vdash A^{\perp *}, \Delta, B, C}}{\vdash A^{\perp *}, \Delta, B \parr C}\parr}{\vdash \Gamma, \Delta, A \parr B}\text{Cut}* \quad\Longrightarrow\quad \dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad {}^{\pi_2}\dfrac{}{\vdash A^{\perp *}, \Delta, B, C}}{\vdash \Gamma, \Delta, B, C}\text{Cut}*}{\vdash \Gamma, \Delta, B \parr C}\parr$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad \dfrac{{}^{\pi_2}\dfrac{}{\vdash A^{\perp *}, \Delta}}{\vdash A^{\perp *}, \Delta, \perp}\perp}{\vdash \Gamma, \Delta, \perp}\text{Cut}* \quad\Longrightarrow\quad \dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Gamma, A^*} \quad {}^{\pi_2}\dfrac{}{\vdash A^{\perp *}, \Delta}}{\vdash \Gamma, \Delta}\text{Cut}*}{\vdash \Gamma, \Delta, \perp}\perp$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash ?\Gamma, !A} \quad \dfrac{{}^{\pi_2}\dfrac{}{\vdash (?A^{\perp})^n, ?\Delta, B}}{\vdash (?A^{\perp})^n, ?\Delta, !B}\text{S}}{\vdash ?\Gamma, ?\Delta, !B}\text{Cut}* \quad\Longrightarrow\quad \dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash ?\Gamma, !A} \quad {}^{\pi_2}\dfrac{}{\vdash (?A^{\perp})^n, ?\Delta, B}}{\vdash ?\Gamma, ?\Delta, B}\text{Cut}*}{\vdash ?\Gamma, ?\Delta, !B}\text{S}$$

*Rewrite rules which apply to* Cut! *on non-principal formulas from more than one premise of a multiplicative rule:*

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash ?\Gamma, !A} \quad \dfrac{{}^{\pi_2}\dfrac{}{\vdash (?A^{\perp})^m, \Delta, B^*} \quad {}^{\pi_3}\dfrac{}{\vdash (?A^{\perp})^n, B^{\perp *}, \Lambda}}{\vdash (?A^{\perp})^{m+n}, \Delta, \Lambda}\text{Cut}*}{\vdash ?\Gamma, \Delta, \Lambda}\text{Cut!}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash ?\Gamma, !A} \quad {}^{\pi_2}\dfrac{}{\vdash (?A^{\perp})^m, \Delta, B^*}}{\vdash ?\Gamma, \Delta, B^*}\text{Cut!} \quad \dfrac{{}^{\pi_1}\dfrac{}{\vdash ?\Gamma, !A} \quad {}^{\pi_3}\dfrac{}{\vdash (?A^{\perp})^n, B^{\perp *}, \Lambda}}{\vdash ?\Gamma, B^{\perp *}, \Lambda}\text{Cut!}}{\vdash ?\Gamma, ?\Gamma, \Delta, \Lambda}\text{Cut}*}{\vdash ?\Gamma, \Delta, \Lambda}\text{C}^{*}$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash ?\Gamma, !A} \quad \dfrac{{}^{\pi_2}\dfrac{}{\vdash (?A^{\perp})^m, \Delta, B} \quad {}^{\pi_3}\dfrac{}{\vdash (?A^{\perp})^n, \Lambda, C}}{\vdash (?A^{\perp})^{m+n}, \Delta, \Lambda, B \otimes C}\otimes}{\vdash ?\Gamma, \Delta, \Lambda, B \otimes C}\text{Cut!}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash ?\Gamma, !A} \quad {}^{\pi_2}\dfrac{}{\vdash (?A^{\perp})^m, \Delta, B}}{\vdash ?\Gamma, \Delta, B}\text{Cut!} \quad \dfrac{{}^{\pi_1}\dfrac{}{\vdash ?\Gamma, !A} \quad {}^{\pi_3}\dfrac{}{\vdash (?A^{\perp})^n, \Lambda, C}}{\vdash ?\Gamma, \Lambda, C}\text{Cut!}}{\vdash ?\Gamma, ?\Gamma, \Delta, \Lambda, B \otimes C}\otimes}{\vdash ?\Gamma, \Delta, \Lambda, B \otimes C}\text{C}^{*}$$

*Rewrite rules which apply to cuts on principal formulas:*

$$\dfrac{\dfrac{}{\vdash A^{\perp}, A}\text{Id} \quad {}^{\pi_1}\dfrac{}{\vdash A^{\perp}, \Gamma}}{\vdash A^{\perp}, \Gamma}\text{Cut} \quad\Longrightarrow\quad {}^{\pi_1}\dfrac{}{\vdash A^{\perp}, \Gamma}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A} \quad \dfrac{\pi_2}{\vdash \Delta, B}}{\vdash \Gamma, \Delta, A \otimes B}\otimes \quad \dfrac{\dfrac{\pi_3}{\vdash A^\perp, B^\perp, \Lambda}}{\vdash A^\perp \parr B^\perp, \Lambda}\parr}{\vdash \Gamma, \Delta, \Lambda}\text{Cut} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_1}{\vdash \Gamma, A} \quad \dfrac{\dfrac{\pi_2}{\vdash \Delta, B} \quad \dfrac{\pi_3}{\vdash A^\perp, B^\perp, \Lambda}}{\vdash A^\perp, \Delta, \Lambda}\text{Cut}}{\vdash \Gamma, \Delta, \Lambda}\text{Cut}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A} \quad \dfrac{\pi_2}{\vdash \Gamma, B}}{\vdash \Gamma, A \mathbin{\&} B}\& \quad \dfrac{\dfrac{\pi_3}{\vdash A^\perp, \Delta}}{\vdash A^\perp \oplus B^\perp, \Delta}\oplus_1}{\vdash \Gamma, \Delta}\text{Cut} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_1}{\vdash \Gamma, A} \quad \dfrac{\pi_3}{\vdash A^\perp, \Delta}}{\vdash \Gamma, \Delta}\text{Cut}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A} \quad \dfrac{\pi_2}{\vdash \Gamma, B}}{\vdash \Gamma, A \mathbin{\&} B}\& \quad \dfrac{\dfrac{\pi_3}{\vdash B^\perp, \Delta}}{\vdash A^\perp \oplus B^\perp, \Delta}\oplus_2}{\vdash \Gamma, \Delta}\text{Cut} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_2}{\vdash \Gamma, B} \quad \dfrac{\pi_3}{\vdash B^\perp, \Delta}}{\vdash \Gamma, \Delta}\text{Cut}$$

$$\dfrac{\dfrac{}{\vdash \mathbf{1}}\mathbf{1} \quad \dfrac{\dfrac{\pi_1}{\vdash \Gamma}}{\vdash \perp, \Gamma}\perp}{\vdash \Gamma}\text{Cut} \quad \Longrightarrow \quad \dfrac{\pi_1}{\vdash \Gamma}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\text{S} \quad \dfrac{\dfrac{\pi_2}{\vdash \Delta}}{\vdash ?A^\perp, \Delta}\text{W}}{\vdash ?\Gamma, \Delta}\text{Cut} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_2}{\vdash \Delta}}{\vdash ?\Gamma, \Delta}\text{W}^*$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\text{S} \quad \dfrac{\dfrac{\pi_2}{\vdash (?A^\perp)^n, \Delta}}{\vdash (?A^\perp)^{n+1}, \Delta}\text{W}}{\vdash ?\Gamma, \Delta}\text{Cut!} \quad \Longrightarrow \quad \dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\text{S} \quad \dfrac{\pi_2}{\vdash (?A^\perp)^n, \Delta}}{\vdash ?\Gamma, \Delta}\text{Cut}*$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\text{S} \quad \dfrac{\dfrac{\pi_2}{\vdash (?A^\perp)^{n+1}, \Delta}}{\vdash (?A^\perp)^n, \Delta}\text{C}}{\vdash ?\Gamma, \Delta}\text{Cut}* \quad \Longrightarrow \quad \dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\text{S} \quad \dfrac{\pi_2}{\vdash (?A^\perp)^{n+1}, \Delta}}{\vdash ?\Gamma, \Delta}\text{Cut!}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\text{S} \quad \dfrac{\dfrac{\pi_2}{\vdash A^\perp, \Delta}}{\vdash ?A^\perp, \Delta}\text{D}}{\vdash ?\Gamma, \Delta}\text{Cut} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A} \quad \dfrac{\pi_2}{\vdash A^\perp, \Delta}}{\vdash ?\Gamma, \Delta}\text{Cut}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\,\text{S} \qquad \dfrac{\dfrac{\pi_2}{\vdash A^\perp, (?A^\perp)^n, \Delta}}{\vdash (?A^\perp)^{n+1}, \Delta}\,\text{D}}{\vdash ?\Gamma, \Delta}\,\text{Cut!} \quad \Longrightarrow \quad \dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{\vdash ?\Gamma, A}}{\vdash ?\Gamma, !A}\,\text{S} \qquad \dfrac{\pi_2}{\vdash A^\perp, (?A^\perp)^n, \Delta}}{\vdash A^\perp, ?\Gamma, \Delta}\,\text{Cut*}}{}}{\vdash ?\Gamma, ?\Gamma, \Delta}\,\text{Cut}}{\vdash ?\Gamma, \Delta}\,\text{C*}$$

*Trivial variations, such as those obtained by exchanging the order of premises, are also included. Exchange of formulas is not considered at all: sequents are treated as multisets.*

*We distinguish three relations on proofs. The* Cut-reduction relation $\Longrightarrow$ *is defined by the rewrite rules shown above, and thus applies only to proofs ending in Cut. The* single-step reduction relation $\longrightarrow$ *relates proofs which are identical except for one pair of corresponding subproofs related by the Cut-reduction relation. The* multi-step reduction relation $\twoheadrightarrow$ *is the reflexive-transitive closure of the single-step reduction relation.*

**Lemma 2.16** *The single-step reduction relation is weakly normalizing, or equivalently, for every proof $\pi$ there is a proof in normal form $\pi'$ such that $\pi \twoheadrightarrow \pi'$.*

**Proof.** First we claim that any proof ending with a Cut$*$ of degree $d$, with the proofs of its premises having degree less than $d$, may be reduced to a proof of degree less than $d$. This claim is proved by induction on the number of axioms and inference rules in the proof. That some rewrite rule must apply is easily checked, by considering cases for reductions on non-principal formulas and on principal formulas; the one tricky case is the non-principal ? formulas of the Storage rule, but it is not possible for both cut formulas to be of this form, and if the other cut formula is principal then it is from another Storage rule and a rewrite rule applies for the non-principal cut formula. Every rewrite rule replaces a proof ending in a Cut$*$ of degree $d$ with a proof containing only Cut$*$ rules of degree less than $d$, and Cut$*$ rules of degree $d$ that conclude subproofs smaller than the original proof and containing no other cuts of degree $d$ or more. (In the case of the rewrite rule with two Cut$*$ rules, the upper one must have degree less than $d$ by assumption.) Thus the claim follows by induction.

Now by induction on the derivation, any proof of degree $d > 0$ may be reduced to a proof of lower degree. By the induction hypothesis, we may assume that the proofs of the premises of the last rule are so reduced, and then either the resulting proof is of degree less than $d$, or it ends in a Cut$*$ of degree $d$ and the hypotheses of the claim above are satisfied.

Finally, by induction on the degree, any proof may be reduced to a proof of degree 0, which by definition is cut-free and thus a normal form. □

**Proof of Theorem 2.12** The theorem follows immediately from Lemma 2.16 since the reduction relations preserve the conclusion of a proof, and any normal form is cut-free. □

Lemma 2.16 was stated separately because it is an important result on its own, for the reasons mentioned earlier.

**Corollary 2.17** *Provability is equivalent to cut-free provability for MALL, MLL, and MELL.*

**Corollary 2.18 (Subformula Property)** *Every provable sequent in LLSC has a proof in which all the formulas that appear are subformulas of the conclusion.*

**Proof.** Using Theorem 2.12, this is clear from a consideration of the rules excluding Cut: every formula appearing in a premise of a rule is a subformula of the conclusion, and the subformula relation is transitive. □

**Corollary 2.19** *Provability in MALL sequent calculus is decidable.*

**Proof.** Each premise of a rule other than Cut or Contraction contains strictly fewer connectives and atoms than the conclusion, so the maximum depth of a cut-free MALL proof is limited by the number of connectives and atoms in its conclusion. The subformula property ensures that the set of atoms occurring in a cut-free proof is the set of atoms occurring in its conclusion. Together, these facts imply that a cut-free proof of a given sequent, if one exists, can certainly be found among a finite set of pseudo-proofs (i.e., trees of sequents and rules, without regard for whether or not the rules are correctly applied), and the enumeration of this set and testing for a valid proof are clearly (by Church's thesis) effective. Since provability is equivalent to cut-free provability by Corollary 2.17, provability is decidable. □

On the other hand, provability in full LLSC is undecidable [21]. The decidability argument above fails because the premise of the Contraction rule contains a strictly larger number of connectives and atoms than the conclusion. Although the subformula property limits the set of possible formulas in a cut-free proof to the finite set of subformulas of the conclusion, the number of occurrences of a ? formula in a sequent can become arbitrarily large in a cut-free proof using the Contraction rule. This allows an undecidable problem to be encoded in terms of LL provability, as in [21].

**Proposition 2.20** *The introduction rules for* $\parr$*,* $\&$*,* $\top$*, and* $\bot$ *are invertible; that is, any provable sequent containing a formula with principal connective among these four has a proof whose last rule is the introduction rule for that connective.*

**Proof.** Indeed, the case of $\top$ is trivial since its introduction rule is actually an axiom, and the introduction rules for the other three connectives have inverses derivable using Cut:

$$\dfrac{\vdash \Gamma, A \parr B \qquad \dfrac{\dfrac{}{\vdash A^{\perp}, A}\,\text{Id} \qquad \dfrac{}{\vdash B^{\perp}, B}\,\text{Id}}{\vdash A^{\perp} \otimes B^{\perp}, A, B}\,\otimes}{\vdash \Gamma, A, B}\,\text{Cut} \qquad\qquad \dfrac{\vdash \Gamma, \bot \qquad \dfrac{}{\vdash \mathbf{1}}\,1}{\vdash \Gamma}\,\text{Cut}$$

$$\dfrac{\vdash \Gamma, A \& B \qquad \dfrac{\dfrac{}{\vdash A^{\perp}, A}\,\text{Id}}{\vdash A^{\perp} \oplus B^{\perp}, A}\,\oplus_1}{\vdash \Gamma, A}\,\text{Cut} \qquad\qquad \dfrac{\vdash \Gamma, A \& B \qquad \dfrac{\dfrac{}{\vdash B^{\perp}, B}\,\text{Id}}{\vdash A^{\perp} \oplus B^{\perp}, B}\,\oplus_2}{\vdash \Gamma, B}\,\text{Cut}$$

□

**Proposition 2.21** *None of the connective rules for* $\otimes$*,* $\oplus$*,* $1$*, and* $0$ *are invertible, that is, for each of these connectives there is a provable sequent containing a formula with that principal connective and for which there is no proof ending with the introduction rule for that connective.*

**Proof.** For $\oplus$, consider the sequent $\vdash a^{\perp} \& b^{\perp}, a \oplus b$, which is provable by the identity rule. A proof ending with an introduction rule for $\oplus$ must necessarily contain a proof of $\vdash a^{\perp} \& b^{\perp}, a$ or $\vdash a^{\perp} \& b^{\perp}, b$, neither of which is provable. (This is easily checked by assuming a cut-free proof and considering cases. Semantic counterexamples can also be used.) The other cases are similar, 0 being trivial since it has no introduction rule. □

The connectives ? and ! are trickier. The Dereliction rule, which is the modal introduction rule for ?, is certainly not invertible by the argument above. The Weakening rule is likewise not invertible, but the inverse of Contraction is a special case of Weakening. The Storage rule, which is the modal introduction rule for !, is not invertible, although the identity argument above fails: the sequent $\vdash ?a^\perp, a$ is provable, but the sequent $\vdash ?a^\perp \,\&\, ?a^\perp, !a$ is provable and does not have a proof ending with the Storage rule.

## 2.6 Phase Semantics

This section describes the algebraic semantics for linear logic, called phase spaces (for MALL) or topolinear spaces (for full linear logic). The results are primarily from Girard's initial paper [11], while the notation is closer to [28].

**Definition 2.22** *A phase space $\mathcal{X} = (X, \perp, \times, 1)$ consists of:*

- *a set $X$ whose elements are called phases;*
- *a commutative and associative operation $\times$ on $X$, with unit $1$;*
- *a set $\perp \subset X$ of antiphases or orthogonal phases.*

As in [11], the monoid $(X, \times, 1)$ is written multiplicatively despite its commutativity, for notational consistency with noncommutative variants of linear logic.

**Definition 2.23** *Given $F \subset X$, its dual $F^\perp$ is defined by $F^\perp := \{\, p \in X \mid pF \subset \perp \,\}$.*

**Definition 2.24** *A fact is a set $F$ of phases such that $F^{\perp\perp} = F$. A fact $F$ is called valid if $1 \in F$.*

*The set of facts of a phase space $\mathcal{X}$ is also denoted $\mathcal{X}$.*

**Lemma 2.25** *The dual $F^\perp$ of a set of phases $F$ satisfies*

$$F^\perp = \max\{\, G \subset X \mid FG \subset \perp \,\}$$

*where the maximum is simply the union with the side condition that it is already an element of the set.*

**Proposition 2.26** *The following properties are true of sets of phases $F$ and $G$:*

1. $F \subset F^{\perp\perp}$
2. $F \subset G \rightarrow G^{\perp} \subset F^{\perp}$
3. $F$ *is a fact iff* $F = H^{\perp}$ *for some* $H \subset X$

**Definition 2.27** *In addition to $\perp$, we define three additional constants* $\top = X$, $\mathbf{0} := \top^{\perp}$, $\mathbf{1} := \perp^{\perp}$.

All of these are facts: $\top = \varnothing^{\perp}$ and $\perp = \{1\}^{\perp}$. $\top$ is the greatest fact and $\mathbf{0}$ is the least fact.

**Example 2.28** There are some small phase spaces in which the only facts are constants. The *three-constant phase space* has $X = \{1, 0\}$, $\perp = \{1\}$, with integer multiplication and unit. There are only three facts $\mathbf{0} \subset \perp = \mathbf{1} \subset \top$.

The *four-constant phase space* has $X = \{1, 0\}$, $\perp = \{0\}$, with $p \times q := p + q + 1$ (mod 2) and unit 1. There are four facts $\mathbf{0} = \varnothing$, $\perp = \{0\}$, $\mathbf{1} = \{1\}$, and $\top = \{1, 0\}$.

**Proposition 2.29** *The following properties hold for sets of phases $F$, $G$, and $F_i$:*

- $\bigcap_{i \in I} F_i^{\perp} = \left(\bigcup_{i \in I} F_i\right)^{\perp}$; *thus, facts are closed under arbitrary intersections.*
- $F^{\perp\perp} = \min \{ H \in \mathcal{X} \mid F \subset H \}$
- $F \multimap G = \max \{ H \subset X \mid FH \subset G \}$
- $(F^{\perp\perp} G)^{\perp} = (FG)^{\perp}$ *and* $(F^{\perp\perp} \cup G)^{\perp} = (F \cup G)^{\perp}$

Now we are ready to define the connectives of linear logic on phase spaces. Connectives will be operations on facts.

**Definition 2.30** *The connectives of linear logic on phase spaces are:*

- $F^{\perp}$ *(nil or linear negation) as defined earlier (duality on facts)*
- $F \otimes G := (FG)^{\perp\perp}$ *(tensor)*

- $F \parr G := (F^{\perp}G^{\perp})^{\perp}$ *(par)*
- $F \multimap G := (FG^{\perp})^{\perp}$ *(entails or linear implication)*
- $F \,\&\, G := F \cap G$ *(with)*
- $F \oplus G := (F \cup G)^{\perp\perp}$ *(plus)*

**Proposition 2.31** *The connectives and constants satisfy the following properties:*

- *de Morgan duality and alternate definition of* $\multimap$*:*

$$\begin{array}{ll}
F \otimes G = (F^{\perp} \parr G^{\perp})^{\perp} & F \parr G = (F^{\perp} \otimes G^{\perp})^{\perp} \\
F \,\&\, G = (F^{\perp} \oplus G^{\perp})^{\perp} & F \oplus G = (F^{\perp} \,\&\, G^{\perp})^{\perp} \\
F \otimes G = (F \multimap G^{\perp})^{\perp} & F \parr G = F^{\perp} \multimap G \\
F \multimap G = F^{\perp} \parr G & F \multimap G = (F \otimes G^{\perp})^{\perp}
\end{array}$$

- *Associativity, commutativity, and neutral elements:*

$$\begin{array}{ll}
\mathbf{1} \otimes F = F & \perp \parr F = F \\
\top \,\&\, F = F & \mathbf{0} \oplus F = F \\
(F \otimes G) \otimes H = F \otimes (G \otimes H) & (F \parr G) \parr H = F \parr (G \parr H) \\
(F \,\&\, G) \,\&\, H = F \,\&\, (G \,\&\, H) & (F \oplus G) \oplus H = F \oplus (G \oplus H) \\
F \otimes G = G \otimes F & F \parr G = G \parr F \\
F \,\&\, G = G \,\&\, F & F \oplus G = G \oplus F
\end{array}$$

- *Distributivity:*

$$\begin{array}{ll}
F \otimes (G \oplus H) = (F \otimes G) \oplus (F \otimes H) & F \otimes \mathbf{0} = \mathbf{0} \\
F \parr (G \,\&\, H) = (F \parr G) \,\&\, (F \parr H) & F \parr \top = \top \\
(F \oplus G) \multimap H = (F \multimap H) \,\&\, (G \multimap H) & \mathbf{0} \multimap F = \top \\
F \multimap (G \,\&\, H) = (F \multimap G) \,\&\, (F \multimap H) & F \multimap \top = \top
\end{array}$$

- *Half-distributivity:*

$$F \otimes (G \mathbin{\&} H) \subset (F \otimes G) \mathbin{\&} (F \otimes H)$$

$$(F \parr G) \oplus (F \parr H) \subset F \parr (G \oplus H)$$

$$(F \multimap H) \oplus (G \multimap H) \subset (F \mathbin{\&} G) \multimap H$$

$$(F \multimap G) \oplus (F \multimap H) \subset F \multimap (G \oplus H)$$

**Example 2.32** A *power set algebra* is $\mathcal{P}(X)$ for some set $X$, with the classical connectives interpreted in the usual way by set operations (viewing $\mathcal{P}(X)$ as a Boolean algebra). We can construct a corresponding phase space $\mathcal{X} = (X', \perp, \times, 1)$ as follows:

- $X' = X \cup \{0, 1\}$ (we assume $X \cap \{0, 1\} = \varnothing$)
- $\perp = \{0\}$
- $p \times q = \begin{cases} p & \text{if } p = q \text{ or } q = 1 \\ q & \text{if } p = q \text{ or } p = 1 \\ 0 & \text{otherwise} \end{cases}$
- 1 as shown

We can now show a bijection between $\mathcal{X}$ and $\mathcal{P}(X)$ under which the interpretation of the linear connectives corresponds to the interpretation of the corresponding classical connectives. First, we claim that for any fact $F \in \mathcal{X}$, $0 \in F$, and $1 \in F$ iff $X \subset F$. That $0 \in F$ is clear since $0 \in \mathbf{0} = X'^{\perp}$ and $\mathbf{0}$ is the least fact. If $1 \in F$, then $\{1\}^{\perp\perp} = \mathbf{1} \subset F$; but $\mathbf{1} = \top$ since $\perp \times X' \subset \perp$. On the other hand, if $X \subset F$, then no element of $X$ can be in $F^{\perp}$ since they are all idempotent and not in $\perp$; so $F^{\perp} = \mathbf{0}$ and $1 \in \top = F^{\perp\perp} = F$.

Thus the facts of $\mathcal{X}$ are simply $F \cup \{0\}$ for $F \in \mathcal{P}(X)$ not equal to $X$, together with $X \cup \{0, 1\}$. The necessary bijection $\Phi : \mathcal{P}(X) \to \mathcal{X}$ is given by $\Phi(F) = F^{\perp\perp}$, with $\Phi^{-1}(F) = F \cap X$.

An element of $\mathcal{P}(X)$ is considered valid if it is $X$, while an element of $\mathcal{X}$ is considered valid if it contains 1; so validity is preserved by $\Phi$. $F^{\perp} = (X \setminus F)^{\perp\perp}$ so classical and linear negation correspond. The product and the intersection coincide for subsets of $X'$ containing 0 because of the definition of the product, so & and $\otimes$ correspond under $\Phi$ to classical conjunction; dually, $\oplus$ and $⅋$ correspond to classical disjunction.

There are several ways to interpret the exponentials in phase semantics. Here we consider Girard's original approach from [11], topolinear spaces. The main alternative is Girard's more recent approach from [12], which amounts to defining one specific topolinear structure on any phase space, in a way that still admits a completeness theorem. That approach has the advantage of not requiring extra structure, but on the other hand it is inconsistent with the treatment of the exponentials as modal operators: it fails to extend to a model of LL with an additional pair of exponential connectives $!'$ and $?'$, with the same rules as the usual exponentials.

**Definition 2.33** *A topolinear space* $\mathcal{X} = (X, \perp, \times, 1, \mathcal{K})$ *is a phase space* $\mathcal{X} = (X, \perp, \times, 1)$ *together with a set* $\mathcal{K} \subset \mathcal{X}$ *called the closed facts, satisfying, for* $F$, $G$, *and* $F_i$ *in* $\mathcal{K}$:

- $\bigcap_{i \in I} F_i \in \mathcal{K}$
- $\perp \in \mathcal{K}$
- $\perp \subset F$
- $F ⅋ G \in \mathcal{K}$
- $F ⅋ F = F$

*The set* $\mathcal{K}^\perp := \left\{ F^\perp \mid F \in \mathcal{K} \right\}$ *is called the set of open facts.*

The properties listed are chosen to allow sound and complete interpretation of the exponentials.

**Definition 2.34** *The exponential connectives on topolinear spaces are:*

- $!F := \left(\bigcup \left\{ G \in \mathcal{K}^\perp \mid G \subset F \right\}\right)^{\perp\perp}$ *(of course)*
- $?F := \bigcap \left\{ G \in \mathcal{K} \mid F \subset G \right\}$ *(why not)*

Since the closed facts are closed under arbitrary intersections, $!F \in \mathcal{K}^\perp$ and $?F \in \mathcal{K}$.

**Example 2.35** Given an arbitrary phase space $\mathcal{X}$, we define the set of idempotents of $\mathcal{X}$, which need not be a fact, by $I := \{ p \in X \mid p \times p = p \}$. Now we can define a set of closed facts by

$$\mathcal{K} := \{ F^\perp \mid F \subset I \cap \mathbf{1} \}.$$

This defines a topolinear space based on $\mathcal{X}$. It is easier to check the duals of the conditions of Definition 2.33. $\mathcal{K}^\perp$ is closed under arbitrary $\oplus$ by Proposition 2.29 extended to arbitrary unions. $\mathbf{1} \in \mathcal{K}^\perp$ since $1 \in I \cap \mathbf{1}$ and $\mathbf{1} = \{1\}^{\perp\perp}$. $F \subset \mathbf{1}$ for $F \in \mathcal{K}^\perp$ since $F = G^{\perp\perp}$ for some $G \subset \mathbf{1}$. For $F, G \in \mathcal{K}^\perp$, $F \otimes G = (FG)^{\perp\perp} = (F'^{\perp\perp} G'^{\perp\perp})^{\perp\perp}$ for some $F', G' \subset I \cap \mathbf{1}$; but this is equal to $(F'G')^{\perp\perp}$ by Proposition 2.29, and $F'G' \subset I \cap \mathbf{1}$ since $\mathbf{1}$ is closed under product and the product of idempotents is idempotent in a commutative monoid. Finally, for $F \in \mathcal{K}^\perp$, $F \subset \mathbf{1}$, so $\perp \subset F^\perp$. Thus, given $p \in F$, $pF^\perp \subset \perp \subset F^\perp$; but then for $p, q \in F$, $pqF^\perp \subset pF^\perp \subset \perp$, so $pq \in F^{\perp\perp} = F$. Thus, $F$ is closed under product, and since each element of $F$ is idempotent, $F \otimes F = F$.

Girard's more recent work on the phase semantics [12] interprets the exponentials in arbitrary phase spaces using this construction, and proves completeness for this interpretation.

If we apply this construction to the phase space corresponding to a power set algebra, we have $\mathbf{1} = \top$ as shown before, and $I = \top$ since every phase is idempotent by construction; so all facts are both open and closed, and $!F = ?F = F$ for any fact $F$. This means that all of the connectives including the exponentials are interpreted classically.

## 2.7 Soundness and Completeness

The link between syntax and semantics, as is usual in logic, begins with soundness and completeness theorems.

The possibilities do not end here: other links between syntax and semantics are possible, particularly those theorems called *full completeness* theorems (such as that of Blute and Scott [3] for noncommutative linear logic), which are for semantics of proofs what completeness theorems are for semantics of formulas.

We begin by interpreting sequents in the phase semantics.

**Definition 2.36** *A topolinear model* $\mathcal{M} = (\mathcal{X}, f)$ *for linear logic consists of a topolinear space* $\mathcal{X}$ *and a function* $f : \mathrm{Atoms} \to \mathcal{X}$ *assigning facts to atoms.*

**Definition 2.37** *The interpretation* $\llbracket A \rrbracket$ *of a formula* $A$ *is defined inductively in the obvious way, i.e., interpreting each connective of linear logic (including the constants) by the corresponding connective on topolinear spaces. The base case is* $\llbracket a \rrbracket := f(a)$.

*The interpretation* $\llbracket \Gamma \rrbracket$ *of a nonempty sequence of formulas* $\Gamma = A_1, A_2, \ldots, A_n$ *is the par of the interpretations of the formulas,* $\left(\llbracket A_1 \rrbracket^{\perp} \llbracket A_2 \rrbracket^{\perp} \cdots \llbracket A_n \rrbracket^{\perp}\right)^{\perp}$. *The empty sequence is interpreted by* $\perp$.

**Proposition 2.38** *For any formula* $A$, $\llbracket A^{\perp} \rrbracket = \llbracket A \rrbracket^{\perp}$.

**Proof.** The result is clear from the fact that the negation of a formula is defined by de Morgan dualities that hold in topolinear spaces. □

This result provides retrospective justification for the use of positive normal form as a notational convenience.

**Definition 2.39** *We say* $\Gamma$ *is valid in* $\mathcal{M}$ *if* $1 \in \llbracket \Gamma \rrbracket$. *We say* $\Gamma$ *is a linear tautology if it is valid in every topolinear model.*

These definitions have obvious analogues for phase spaces; a *phase model* interprets MALL formulas.

For the remainder of this section, we treat sequents as multisets. This causes no trouble semantically because of the commutativity and associativity of $\parr$.

**Theorem 2.40 (Soundness)** *Linear logic sequent calculus is sound with respect to validity in topolinear models. That is, if* $\vdash \Gamma$ *is provable, then* $\Gamma$ *is a linear tautology.*

Soundness is proved by induction on a derivation of $\vdash \Gamma$. The soundness of the MALL rules follows from the properties of phase spaces, particularly those stated in Propositions 2.29 and 2.31. The soundness of the exponential rules follows from the properties imposed in Definition 2.33 for topolinear spaces.

In fact, a stronger result is usually proved: each rule of LLSC is sound in the sense that validity of the premises implies validity of the conclusion, regardless of provability.

**Theorem 2.41 (Completeness)** *Linear logic sequent calculus is complete with respect to validity in topolinear models. That is, if* $\Gamma$ *is a linear tautology, then* $\vdash \Gamma$ *is provable.*

Whereas soundness (in the stronger form mentioned above) is essentially a property of one rule and one model, and extends to a set of rules (a deductive system) and a set of models by universal quantification, completeness involves existential quantification and thus it cannot be reduced to the case of one rule (or proof) or one model. However, completeness for a set of models implies completeness for any larger set of models. Here we prove completeness of LLSC for one model, the syntactic model, and obtain completeness for the class of all topolinear models as a corollary. The proof closely follows Girard [11].

Where the proof of soundness uses the definition of the sequent calculus and the proof techniques of topolinear spaces, the proof of completeness does the reverse: it uses the definition of topolinear spaces and the proof techniques of linear logic sequent calculus.

**Definition 2.42** *For any formula* $A$*, we define* $\mathrm{Pr}(A)$*, the set of contexts proving* $A$*, by:*

$$\mathrm{Pr}(A) := \left\{ \Gamma \;\middle|\; \Gamma \vdash A \textit{ is provable} \right\}$$

**Definition 2.43** *The syntactic model* $\mathcal{M}_{\mathrm{syn}}$ *for linear logic is defined as follows:*

- $X$ *is the set of all multisets of formulas;*

- $\perp := \mathrm{Pr}(\perp)$ *is the set of those multisets of formulas* $\Gamma$ *such that* $\Gamma \vdash \perp$, *or equivalently (by Proposition 2.20)* $\Gamma \vdash$, *is provable;*
- $\times$ *is concatenation of multisets;*
- $1$ *is the empty multiset;*
- $\mathcal{K}$ *is the set of arbitrary intersections of facts of the form* $\mathrm{Pr}(?A)$*;*
- $f(a) := \mathrm{Pr}(a)$ *for atoms* $a$.

In the syntactic model, it is clear that $\mathrm{Pr}(A) = \{A^\perp\}^\perp$.

The syntactic model is certainly a phase model, but to show that it is a topolinear model, the conditions of Definition 2.33 must be verified.

**Lemma 2.44** $\mathrm{Pr}(A^\perp)^\perp = \mathrm{Pr}(A)$ *for all formulas* $A$*, and thus* $\mathrm{Pr}(A)$ *is a fact.*

**Proof.** Suppose $\Gamma \in \mathrm{Pr}(A)$, i.e., $\Gamma \vdash A$ is provable. Now for any sequence of formulas $\Delta$ such that $\Delta \vdash A^\perp$ is provable, by the Cut rule $\Gamma, \Delta \vdash$ is provable. Thus $\Gamma \in \mathrm{Pr}(A^\perp)^\perp$, so $\mathrm{Pr}(A) \subset \mathrm{Pr}(A^\perp)^\perp$.

Conversely, suppose $\Gamma \in \mathrm{Pr}(A^\perp)^\perp$. Then by the Identity rule, $A^\perp \in \mathrm{Pr}(A^\perp)$, so $\Gamma, A^\perp \vdash$ is provable. But this is the same as $\Gamma \vdash A$, so $\Gamma \in \mathrm{Pr}(A)$. Thus $\mathrm{Pr}(A^\perp)^\perp \subset \mathrm{Pr}(A)$, and combining the two inclusions gives the equality that was to be proven. □

We would like to conclude that $\mathrm{Pr}(A) = [\![A]\!]$ for all formulas $A$, and to do so it is enough to show that $\mathrm{Pr}(A)$ satisfies the inductive definition of $[\![A]\!]$. The base case where $A$ is a literal follows from the definition of $\mathcal{M}_{\mathrm{syn}}$ and Lemma 2.44.

**Lemma 2.45** $\mathrm{Pr}(\perp) = \perp$, $\mathrm{Pr}(A \otimes B) = \mathrm{Pr}(A) \otimes \mathrm{Pr}(B)$, *and similarly for all the other connectives of MALL.*

**Proof.** The cases $\perp$ and $\top$ follow from the definition of $\mathcal{M}_{\mathrm{syn}}$ and the corresponding rule and axiom. The case $\&$ follows from the fact that $\Gamma \vdash A \& B$ is provable iff $\Gamma \vdash A$ and $\Gamma \vdash B$ are both provable. The case $\otimes$ follows from the rules $\otimes$, $\invamp$, and Cut and properties of phase spaces. The other cases follow by duality using Lemma 2.44. □

**Lemma 2.46** *$\mathcal{M}_{\mathrm{syn}}$ is a topolinear model, i.e., it satisfies the conditions of Definition 2.33.*

**Proof.** Consider the set $K$ of facts of the form $\mathrm{Pr}(?A)$. By the Cut rule, if $A \vdash B$ then $\mathrm{Pr}(A) \subset \mathrm{Pr}(B)$. Now since $\bot \dashv\vdash ?\bot$, $\bot = \mathrm{Pr}(\bot) \in K$. Since $\bot \vdash ?A$, $\bot = \mathrm{Pr}(\bot) \subset \mathrm{Pr}(?A)$ so $\bot$ is the least element of $K$. Since $?A \mathbin{⅋} ?B \dashv\vdash ?(A \oplus B)$, $\mathrm{Pr}(?A) \mathbin{⅋} \mathrm{Pr}(?B) = \mathrm{Pr}(?A \mathbin{⅋} ?B) = \mathrm{Pr}(?(A \oplus B)) \in K$. Finally, since $?(A \oplus A) \dashv\vdash ?A$, $\mathrm{Pr}(?A) \mathbin{⅋} \mathrm{Pr}(?A) = \mathrm{Pr}(?A)$. So $K$ satisfies all of the conditions except closure under arbitrary intersections.

Now $\mathcal{K}$ consists of arbitrary intersections of elements of $K$, so it is closed under arbitrary intersections by construction. That $\bot$ is the least element of $\mathcal{K}$ follows from this property for $K$. The other two conditions for $\mathcal{K}$ are obtained from the conditions for $K$ by properties of phase spaces, notably distributivity of $⅋$ over arbitrary intersections (i.e., $\&$). □

It remains only to extend Lemma 2.45 to the exponentials:

**Lemma 2.47** $\mathrm{Pr}(!A) = !\,\mathrm{Pr}(A)$ *and* $\mathrm{Pr}(?A) = ?\,\mathrm{Pr}(A)$.

**Proof.** Indeed,

$$?\,\mathrm{Pr}(A) = \bigcap \{\, \mathrm{Pr}(?B) \mid \mathrm{Pr}(A) \subset \mathrm{Pr}(?B) \,\} = \bigcap \{\, \mathrm{Pr}(?B) \mid A \vdash ?B \text{ is provable} \,\}$$

and by the Storage and Dereliction rules, $A \vdash ?B$ is provable iff $?A \vdash ?B$ is provable, in which case $\mathrm{Pr}(?A) \subset \mathrm{Pr}(?B)$. Thus $?\,\mathrm{Pr}(A) = \mathrm{Pr}(?A)$, and the other equality follows by duality (Lemma 2.44). □

**Proof of Theorem 2.41 (Completeness).** An easy induction using Lemmas 2.45 and 2.47 shows that $[\![A]\!]_{\mathcal{M}_{\mathrm{syn}}} = \mathrm{Pr}(A)$ for any formula $A$. Suppose $A$ is a linear tautology; then $A$ is valid in $\mathcal{M}_{\mathrm{syn}}$, which means $\varnothing \in [\![A]\!]_{\mathcal{M}_{\mathrm{syn}}} = \mathrm{Pr}(A)$, and thus $\vdash A$ is provable.

Now if $\Gamma$ is a linear tautology, then so is $⅋\,\Gamma$, since $[\![\Gamma]\!] = [\![⅋\,\Gamma]\!]$ holds in topolinear models; then $\vdash ⅋\,\Gamma$ is provable, or equivalently (by Proposition 2.20) $\vdash \Gamma$ is provable. Thus every linear tautology is provable, as was to be proven. □

## 2.8 Free Storage

From the point of view of the informal semantics, the linear logic sequent calculus is somewhat unsatisfactory. The problem is that the meaning of the exponentials is too restricted. Certainly the storage rule is intuitively sound: if we can obtain one copy of a resource, using only unlimited resources to do so, then we can obtain as many as we want from the same resources.

On the other hand, suppose we assume that a particular resource, say $a$, can be thrown away or duplicated as often as necessary, i.e., we assume $!(a \multimap \mathbf{1})$ and $!(a \multimap a \otimes a)$. Then we should be able to obtain an unlimited supply of this resource from one copy of it. That is, we should be able to prove $!(a \multimap \mathbf{1}), !(a \multimap a \otimes a), a \vdash !a$. However, it is easily checked that no matter what rules we apply, we will never be in a position to apply the Storage rule to the right-hand formula unless we have already thrown away the copy of $a$ we started with, in which case we will never be able to obtain another one. So this sequent, while intuitively valid, is not provable in LLSC. In effect, this means that completeness fails for the informal semantics.

There is another, related potential flaw in the sequent rules for the exponentials. If we add a second dual pair of connectives $!'$ and $?'$ with the same rules as for the usual exponentials, then we find that we are unable to prove $!A \vdash !'A$. The problem is that the Storage$'$ rule does not apply because its premise would have to contain the alternate exponential $!'$ in place of the $!$ on the left. Thus, in the sense described in [22], the rules for $!$ are not universal.

Although we expect such non-universality for modal connectives (indeed, it is necessary for the construction of multi-modal logics), universality is generally considered a good property of axiomatizations of *logical* connectives. Indeed, universality holds for all of the connectives of classical, intuitionistic, and linear logic (even predicate logic) in the usual sequent calculi, excluding the linear exponentials. The term 'logical' here is intended as a generalization of 'truth-functional' in the classical case; in linear logic, it refers to connectives that represent ways to build new resources from existing ones without any assumptions about the nature of those resources.

These considerations suggest that the Storage rule may not be appropriate for some applications of linear logic. There is an alternative rule called Free Storage, described by Troelstra [28] based on semantical developments by Yves Lafont [18], which avoids these problems. One presentation of this rule is the following:

$$\dfrac{A \vdash \mathbf{1} \quad A \vdash A \otimes A \quad A \vdash B}{A \vdash !B}\;{\scriptstyle \mathrm{FS}}$$

We can now check that the problems mentioned above are not present in linear logic with free storage (denoted $\mathrm{LL_{FS}}$; the ordinary Storage rule is discarded):

$$\dfrac{\dfrac{\dfrac{}{\vdash \mathbf{1}}\;{\scriptstyle \mathbf{1}_{\mathrm{R}}}}{!A \vdash \mathbf{1}}\;{\scriptstyle \mathrm{W_L}} \qquad \dfrac{\dfrac{\dfrac{}{!A \vdash !A}\;{\scriptstyle \mathrm{Id}} \quad \dfrac{}{!A \vdash !A}\;{\scriptstyle \mathrm{Id}}}{!A, !A \vdash !A \otimes !A}\;{\scriptstyle \otimes_{\mathrm{R}}}}{!A \vdash !A \otimes !A}\;{\scriptstyle \mathrm{C_L}} \qquad \dfrac{\dfrac{}{A \vdash A}\;{\scriptstyle \mathrm{Id}}}{!A \vdash A}\;{\scriptstyle \mathrm{D_L}}}{!A \vdash !'A}\;{\scriptstyle \mathrm{FS'}}$$

For the proof of $!(a \multimap \mathbf{1}), !(a \multimap a \otimes a), a \vdash !a$ we use some abbreviations: $A_{\mathrm{W}} = a \multimap \mathbf{1}$, $A_{\mathrm{C}} = a \multimap a \otimes a$, $\Gamma = !A_{\mathrm{W}}, !A_{\mathrm{C}}, a$, and $A = !A_{\mathrm{W}} \otimes !A_{\mathrm{C}} \otimes a$. We also indicate multiple uses of a rule by *, and combine the Identity rule into the rules following it.

$$\dfrac{\dfrac{}{\Gamma \vdash A}\;{\scriptstyle \otimes_{\mathrm{R}}^{*},\mathrm{Id}^{*}} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a \multimap \mathbf{1}, a \vdash \mathbf{1}}\;{\scriptstyle \text{⅋}_{\mathrm{L}},\mathrm{Id}^{*}}}{!A_{\mathrm{W}}, a \vdash \mathbf{1}}\;{\scriptstyle \mathrm{D}}}{\Gamma \vdash \mathbf{1}}\;{\scriptstyle \mathrm{W}}}{A \vdash \mathbf{1}}\;{\scriptstyle \otimes_{\mathrm{L}}^{*}} \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A}\;{\scriptstyle \otimes_{\mathrm{R}}^{*},\mathrm{Id}^{*}} \quad \dfrac{}{\Gamma \vdash A}\;{\scriptstyle \otimes_{\mathrm{R}}^{*},\mathrm{Id}^{*}}}{\Gamma, \Gamma \vdash A \otimes A}\;{\scriptstyle \otimes_{\mathrm{R}}}}{!A_{\mathrm{W}}, !A_{\mathrm{W}}, !A_{\mathrm{C}}, !A_{\mathrm{C}}, a \otimes a \vdash A \otimes A}\;{\scriptstyle \otimes_{\mathrm{L}}}}{!A_{\mathrm{W}}, !A_{\mathrm{W}}, !A_{\mathrm{C}}, !A_{\mathrm{C}}, a \multimap a \otimes a, a \vdash A \otimes A}\;{\scriptstyle \text{⅋}_{\mathrm{L}},\mathrm{Id}}}{!A_{\mathrm{W}}, !A_{\mathrm{W}}, !A_{\mathrm{C}}, !A_{\mathrm{C}}, !A_{\mathrm{C}}, a \vdash A \otimes A}\;{\scriptstyle \mathrm{D}}}{\Gamma \vdash A \otimes A}\;{\scriptstyle \mathrm{C}^{*}}}{A \vdash A \otimes A}\;{\scriptstyle \otimes_{\mathrm{L}}^{*}} \quad \dfrac{\dfrac{}{\Gamma \vdash a}\;{\scriptstyle \mathrm{W}^{*},\mathrm{Id}}}{A \vdash a}\;{\scriptstyle \otimes_{\mathrm{L}}^{*}}}{A \vdash !a}\;{\scriptstyle \mathrm{FS}}}{!(a \multimap \mathbf{1}), !(a \multimap a \otimes a), a \vdash !a}\;{\scriptstyle \mathrm{Cut}}$$

We can also check that the usual Storage rule is derivable:

$$\dfrac{\dfrac{}{!\Gamma \vdash \otimes !\Gamma}\;{\scriptstyle \otimes_{\mathrm{R}}^{*},\mathrm{Id}^{*}} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \mathbf{1}}\;{\scriptstyle \mathbf{1}_{\mathrm{R}}}}{!\Gamma \vdash \mathbf{1}}\;{\scriptstyle \mathrm{W}_{\mathrm{L}}^{*}}}{\otimes !\Gamma \vdash \mathbf{1}}\;{\scriptstyle \otimes_{\mathrm{L}}^{*}} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{!\Gamma \vdash \otimes !\Gamma}\;{\scriptstyle \otimes_{\mathrm{R}}^{*},\mathrm{Id}^{*}} \quad \dfrac{}{!\Gamma \vdash \otimes !\Gamma}\;{\scriptstyle \otimes_{\mathrm{R}}^{*},\mathrm{Id}^{*}}}{!\Gamma, !\Gamma \vdash (\otimes !\Gamma) \otimes (\otimes !\Gamma)}\;{\scriptstyle \otimes_{\mathrm{R}}}}{!\Gamma \vdash (\otimes !\Gamma) \otimes (\otimes !\Gamma)}\;{\scriptstyle \mathrm{C}_{\mathrm{L}}^{*}}}{\otimes !\Gamma \vdash (\otimes !\Gamma) \otimes (\otimes !\Gamma)}\;{\scriptstyle \otimes_{\mathrm{L}}^{*}} \quad !\Gamma \vdash A}{\otimes !\Gamma \vdash !A}\;{\scriptstyle \mathrm{FS'}}}{!\Gamma \vdash !A}\;{\scriptstyle \mathrm{Cut}}$$

On the other hand, free storage has its own disadvantages. One major disadvantage is that cut-elimination fails, as is illustrated by the derivations above. The substitution theorem also fails if the identity rule is not allowed for exponential formulas.

An important result is that whichever rule we choose for !, the set of provable MALL sequents is not affected.

**Proposition 2.48** (Troelstra [28], corollary to Proposition 12.12) *$LL_{FS}$ is conservative over MALL.*

The linear logic sequent calculus with free storage will be useful because it allows a natural translation of the exponentials into fixpoint linear logic. The free storage exponentials can be interpreted in phase spaces using this translation. Free storage also has a categorical interpretation using fixed points [18, 28].

# Chapter 3

# Modal Logic

## 3.1 Motivation

Traditionally, modal logic has meant 'the logic of necessity and possibility'. However, the subject has grown in so many different directions that it is difficult to find a universally accepted definition. This section will attempt to present a reasonably inclusive definition and describe what kinds of modal logic are of interest here.

Modal logics are extensions of classical logic (or some other logic, such as intuitionistic) to consider *modes of truth.* What is a mode of truth? In the most general sense, it is a connective that is not *truth-functional*, i.e., for which the truth of a formula with that principal connective is not simply a function of the truth values of its immediate subformulas. Modes of truth are often used to express in logic fragments of natural language that are themselves not truth-functional. Examples include 'necessarily true', 'true in the future', 'known by agent $A$ to be true', etc.

However, much of the study of modal logics focuses on particular kinds of modal connectives. The most commonly used simplification is to consider only those modal logics that can be interpreted in terms of *relational structures*, which are also known as *Kripke structures.* These logics, called *normal modal logics*, all satisfy a particular axiom scheme called K, as well as several closure conditions. This ensures in particular that it is possible to *reason* within a mode of truth: such modal connectives are positive in all their arguments. Modal connectives are also often assumed to be unary; most of the traditional applications (temporal logic, deontic logic, etc.) involve unary connectives. Dual pairs of unary modal connectives are traditionally denoted $\Box$ and $\Diamond$, or $[x]$ and $\langle x \rangle$ when several are present simultaneously.

Modal logics are usually based on propositional logic, which means that they have no variable binding whatsoever. In fact, this is sometimes considered a key property of modal logics, and it can be a good reason to use them in preference to the first- and second-order predicate logics into which they can be translated. However, much research has been done on the subject of combining modal logics with first-order quantification. A survey of this work can be found in Hughes and Cresswell [15].

In this chapter we will consider the formulas of *basic modal logic*, with one dual pair of modal connectives $\Box$ and $\Diamond$, and the semantics and deductive systems of normal modal logics. This chapter is based on Chellas [6], Huth and Ryan [16], and especially Blackburn, de Rijke, and Venema [2]. [6] is a well-known book on modal logic, while the others are more modern treatments; [2] in particular is quite comprehensive and inclusive.

## 3.2 Syntax

**Definition 3.1** *The formulas of basic modal logic are defined by the following BNF:*

$$\mathbf{formula}, A, B \quad ::= \quad \mathbf{atom} \mid \neg A \mid A \wedge B \mid A \vee B \mid A \to B \mid \Box A \mid \Diamond A$$

Letters $a$, $b$, ... denote atoms, and letters $A$, $B$, $C$, ... denote formulas. The set of all formulas (with atoms from a set Atoms) is denoted $\Phi(\text{Atoms})$.

**Convention 3.2** *The modal connectives $\Box$ and $\Diamond$ have the same binding priority as negation, i.e., bind tighter than the binary connectives.*

Traditionally, $\Box$ denotes necessity and $\Diamond$ denotes possibility.

Generalized modal connectives of arity greater than one are sometimes denoted $\nabla$ and $\Delta$, corresponding to $\Box$ and $\Diamond$ respectively. They will not be considered here, but [2] describes most aspects of the theory of modal logics in this generality.

## 3.3 Semantics

**Definition 3.3** *A frame (or Kripke structure) $\mathcal{F} = (W, R)$ consists of a nonempty set $W$ of worlds (or states; other terms are also used) and a relation $R \subset W \times W$.*

For basic modal logic, frames are simply directed graphs. When more complicated modal languages are considered, frames are generalized to include relations corresponding to each of the modal connectives, each with arity one greater than that of the corresponding connective.

**Example 3.4** A *labeled transition system* $\mathcal{F} = (W, X, R)$ consists of a nonempty set $W$ and a relation $R \subset W \times X \times W$, for some set $X$ of *labels*.

A labeled transition system may be viewed as a set $W$ together with relations $R_x$ for $x \in X$ defined by $w \; R_x \; w'$ iff $(w, x, w') \in R$. Labeled transition systems can be used to interpret multi-modal logic with modalities $[x]$ and $\langle x \rangle$ for each $x \in X$.

**Definition 3.5** *A model (or Kripke model) $\mathcal{M} = (W, R, L)$ consists of a frame $\mathcal{F} = (W, R)$ together with a labeling $L \subset W \times \mathrm{Atoms}$. The model $\mathcal{M}$ is said to be based on the frame $\mathcal{F}$.*

**Definition 3.6** *The satisfaction relation $\Vdash \; \subset W \times \Phi(\mathrm{Atoms})$ is defined inductively by:*

- *$w \Vdash a$ iff $(w, a) \in L$;*
- *$w \Vdash A \wedge B$ iff $w \Vdash A$ and $w \Vdash B$, and similarly for the other classical connectives;*
- *$w \Vdash \Box A$ iff $w' \Vdash A$ for all $w'$ such that $w \; R \; w'$;*
- *$w \Vdash \Diamond A$ iff $w' \Vdash A$ for some $w'$ such that $w \; R \; w'$.*

*If the model is not clear from context, we may write $w \Vdash_{\mathcal{M}} A$ or $\mathcal{M}, w \Vdash A$. We may also write $[\![A]\!]_w = \mathbf{T}$ for $w \Vdash A$, and $[\![A]\!]_w = \mathbf{F}$ for $w \nVdash A$, and say that a formula is true or false at a world.*

**Definition 3.7** *A formula $A$ is* globally true *or* valid *in a model $\mathcal{M}$, denoted $\mathcal{M} \vDash A$, if $\mathcal{M}, w \Vdash A$ for all worlds $w$. $A$ is* satisfiable *in $\mathcal{M}$ if $\mathcal{M}, w \Vdash A$ for some world $w$.*

*A formula $A$ is* valid in a class of models *$\mathbb{M}$, written $\mathbb{M} \vDash A$, if it is globally true in every model of $\mathbb{M}$.*

Instead of interpreting a formula at a particular world, we may also interpret a formula by the set of worlds satisfying it.

**Definition 3.8** *The* interpretation *$[\![A]\!]$ of a formula $A$ in a model $\mathcal{M}$ is*

$$[\![A]\!] := \{\, w \in W \mid w \Vdash A \,\}.$$

This way of describing the semantics is sometimes more convenient than the satisfaction relation, particularly for the modal mu-calculus to be described later.

## 3.4 Deductive Systems

Deductive systems for modal logic are traditionally presented in Hilbert style, although sequent calculi and natural deduction systems exist; those systems unfortunately do not satisfy all of the nice properties of such systems for propositional and predicate logics.

**Definition 3.9** *A* normal modal logic *$\Lambda$ is a set of formulas satisfying the following conditions for all formulas $A$ and $B$ and atoms $a$:*

- *$\Box/\Diamond$ duality: $\neg\Box A \leftrightarrow \Diamond\neg A \in \Lambda$*
- *Axiom K: $\Box(A \to B) \to (\Box A \to \Box B) \in \Lambda$*
- *If $A$ is a propositional tautology, then $A \in \Lambda$*
- *Modus ponens: if $A \in \Lambda$ and $A \to B \in \Lambda$, then $B \in \Lambda$*
- *Rule of necessitation, or generalization: if $A \in \Lambda$, then $\Box A \in \Lambda$*
- *Substitution closure: if $A \in \Lambda$, then $A[B/a] \in \Lambda$*

A Hilbert-style axiomatization of classical propositional logic together with the rule of necessitation, axiom K, the duality axiom, and arbitrary other axioms clearly defines a normal modal logic, called the normal modal logic *generated by* the additional axioms. With no additional axioms we obtain the modal logic **K**, which is the smallest normal modal logic. This logic has some applications, but in many applications a logic that validates additional principles is desired. Thus, additional axioms are often added. Some of the best-known ones are (see [6, 16]):

- Axiom D: $\Box A \to \Diamond A$
- Axiom T: $\Box A \to A$
- Axiom B: $A \to \Box\Diamond A$
- Axiom 4: $\Box A \to \Box\Box A$
- Axiom 5: $\Diamond A \to \Box\Diamond A$

Not all of these axioms are independent. For instance, axiom D is derivable from axiom T. According to [6], there are exactly 15 distinct normal modal logics among those generated by the 32 possible choices of a subset of these five axioms. Some of the best-known ones are **K** (K), **KD** (KD), **T** (KT), **B** (KB), **S4** (KT4), and **S5** (KT45 or KTB4).

For later sections which will combine modal logic and linear logic, it is useful to have sequent calculus presentations for certain normal modal logics. These can be found in Ohnishi and Matsumoto [23, 24]. They are all obtained by augmenting classical sequent calculus with rules for the modalities. We will use the version of classical sequent calculus obtained by classical collapse from LLSC, omitting the redundant Dereliction and Storage rules. The rules for the modalities are:

$$\mathbf{K}: \qquad \frac{\vdash \Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box\Diamond_{\mathbf{K}}$$

$$\mathbf{KD}: \qquad \frac{\vdash \Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box\Diamond_{\mathbf{KD}} \qquad \frac{\vdash \Gamma}{\vdash \Diamond\Gamma}\,\Diamond_{\mathbf{KD}}$$

$$\mathbf{T}: \qquad \frac{\vdash \Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box\Diamond_{\mathbf{T}} \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, \Diamond A}\,\Diamond_{\mathbf{T}}$$

$$\mathbf{S4}: \qquad \frac{\vdash \Diamond\Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box_{\mathbf{S4}} \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, \Diamond A}\,\Diamond_{\mathbf{S4}}$$

The $\Box\Diamond_{\mathbf{K}}$ rule is perhaps clearer in two-sided form:

$$\frac{\Gamma \vdash A}{\Box\Gamma \vdash \Box A}\,\Box\Diamond_{\mathbf{K}}$$

Cut-elimination theorems for these sequent calculi were proved by Ohnishi and Matsumoto. On the other hand, the modal logic **S5** has an equally simple sequent presentation, but it does not satisfy cut-elimination (a counterexample can be found in [5]):

$$\mathbf{S5}: \qquad \frac{\vdash \Diamond\Gamma, \Box\Delta, A}{\vdash \Diamond\Gamma, \Box\Delta, \Box A}\,\Box_{\mathbf{S5}} \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, \Diamond A}\,\Diamond_{\mathbf{S5}}$$

It is possible to use various technical devices to obtain a sequent calculus for **S5** that satisfies cut-elimination. One such approach, using a notion of dependency between formulas in a sequent proof, is given by Braüner [5]. Braüner defines a sequent calculus with the rule

$$\frac{\vdash \Gamma, A}{\vdash \Gamma, \Box A}\,\Box'_{\mathbf{S5}}$$

in place of $\Box_{\mathbf{S5}}$. This sequent calculus has an obvious cut-elimination procedure, but it is not sound for **S5**. Soundness is restored by a global correctness criterion on sequent proofs, which is preserved by cut-elimination steps. This approach has the advantage that the sequent rules cleanly introduce the modal connectives, without conditions on non-principal formulas, multiple principal formulas, or use of both $\Box$ and $\Diamond$ in the conclusion.

The sequent rules for **S4** are identical to the Storage and Dereliction rules for linear logic. Adding unrestricted Contraction and Weakening to linear logic recovers, under a translation similar to classical collapse, the classical **S4** sequent calculus. It is for this reason that ! and ? of linear logic are sometimes called modalities.

## 3.5 Soundness

The presentation of the well-known results in the following three sections closely follows Blackburn et al. [2], chapters 3–5, in which the theory of modal logic is presented in considerable detail and with historical information.

To obtain sound and complete semantics for the various normal modal logics, the relational semantics on particular classes of models will be used. The particular classes of models that are of interest are those that are defined by properties of frames.

**Definition 3.10** *A formula $A$ is* valid *at a world $w$ in a frame $\mathcal{F} = (W, R)$, written $\mathcal{F}, w \Vdash A$, if $\mathcal{M}, w \Vdash A$ for every model $\mathcal{M}$ based on $\mathcal{F}$. $A$ is* valid *on $\mathcal{F}$, written $\mathcal{F} \vDash A$, if it is valid at every world in $\mathcal{F}$, or equivalently, if it is globally true in every model based on $\mathcal{F}$. $A$ is* valid *on a class of frames $\mathbb{F}$, denoted $\mathbb{F} \vDash A$, if it is valid on each frame in $\mathbb{F}$.*

By convention, a class of frames may be viewed also as a class of models, specifically those models based on frames from that class.

**Definition 3.11** *A formula $A$* defines *a class of frames $\mathbb{F}$ if for any frame $\mathcal{F}$, we have $\mathcal{F} \in \mathbb{F}$ iff $\mathcal{F} \vDash A$.*

The notion of a formula defining a class of frames can be used to characterize the axioms D, T, B, 4, and 5 semantically.

**Proposition 3.12** *The axioms D, T, B, 4, and 5 (on particular atoms) define the following classes of frames:*

- *Axiom D ($\Box a \to \Diamond a$):* serial *frames*

- *Axiom T ($\Box a \to a$): reflexive frames*
- *Axiom B ($a \to \Box\Diamond a$): symmetric frames*
- *Axiom 4 ($\Box a \to \Box\Box a$): transitive frames*
- *Axiom 5 ($\Diamond a \to \Box\Diamond a$):* Euclidean *frames*

*The classes of reflexive, symmetric and transitive frames consist of those frames whose relation $R$ has the corresponding property. A frame is called* serial *(or* right-unbounded*) if for every world $w$, there is a world $w'$ such that $w \ R \ w'$. A frame is called* Euclidean *if, for worlds $w_1$, $w_2$, and $w_3$, $w_1 \ R \ w_2$ and $w_1 \ R \ w_3$ imply $w_2 \ R \ w_3$. (See [16], section 5.3.2.)*

**Proof.** The proofs are similar for each of these cases. We consider Axiom B and symmetric frames. If a given frame $\mathcal{F}$ is symmetric, then we consider any model $\mathcal{M}$ based on $\mathcal{F}$. Suppose for some world $w$, we have $w \Vdash a$, and consider any world $w'$ such that $w \ R \ w'$. Then by symmetry, $w' \ R \ w$, so $w' \Vdash \Diamond a$. Since $w'$ was arbitrary, $w \Vdash \Box\Diamond a$. Now we have shown that $w \Vdash a$ implies $w \Vdash \Box\Diamond a$, i.e., that $w \Vdash a \to \Box\Diamond a$. So $a \to \Box\Diamond a$ is globally true in $\mathcal{M}$, and it is valid in $\mathcal{F}$.

Conversely, if a given frame $\mathcal{F}$ is not symmetric, then there exist worlds $w_1$ and $w_2$ such that $w_1 \ R \ w_2$ but not $w_2 \ R \ w_1$. We define a model $\mathcal{M}$ based on $\mathcal{F}$ by $L = \{(w_1, a)\}$. We have $\mathcal{M}, w \Vdash a$ iff $w = w_1$, and thus $\mathcal{M}, w \Vdash \Diamond a$ iff $w \ R \ w_1$; so $\mathcal{M}, w_2 \nVdash \Diamond a$. But since $w_1 \ R \ w_2$, we have $\mathcal{M}, w_1 \nVdash \Box\Diamond a$; and finally, we conclude $\mathcal{M}, w_1 \nVdash a \to \Box\Diamond a$. So $\mathcal{F} \nvDash a \to \Box\Diamond a$. Thus, Axiom B defines the class of symmetric frames, as was to be proven. $\Box$

**Corollary 3.13 (Soundness)** *Each of the axioms D, T, B, 4, and 5 is sound with respect to the class of frames that it defines (or any smaller class). Furthermore, the normal modal logic generated by any subset of these axioms is sound with respect to the intersection of the classes of frames corresponding to those axioms.*

**Proof.** The soundness of the axioms is an immediate consequence of Proposition 3.12. The soundness of the generated normal modal logics follows from the soundness of axiom K, propositional tautologies, and the rules of inference specified for normal modal logics, on any frame. $\Box$

On the other hand, completeness does not follow at once. The fact that a formula $A$ defines a class of frames is not enough to conclude that every formula validated by that class of frames is derivable in the normal modal logic generated by $A$. In fact there exist formulas for which there is no sound and complete class of frames (see [2], section 4.4). However, completeness for the usual normal modal logics can be proven using *canonical models.*

## 3.6 Completeness

**Definition 3.14** *Given a logic $\Lambda$, we say that a formula $A$ is $\Lambda$-deducible from a set of formulas $\Gamma$ if $B_1 \wedge B_2 \wedge \cdots \wedge B_n \to A \in \Lambda$ for some finite subset $\{B_1, B_2, \ldots, B_n\}$ of $\Gamma$.*

*A set of formulas $\Gamma$ is called $\Lambda$-consistent if $\bot$ is not $\Lambda$-deducible from $\Gamma$.*

**Definition 3.15** *A logic $\Lambda$ is strongly complete with respect to a class of models $\mathbb{M}$ if for any set of formulas $\Gamma$ and formula $A$, if $\Gamma \models_{\mathbb{M}} A$, then $A$ is $\Lambda$-deducible from $\Gamma$. (The notation $\Gamma \models_{\mathbb{M}} A$, called the semantic consequence relation, means $\mathbb{M}' \models A$ where $\mathbb{M}' := \{\mathcal{M} \in \mathbb{M} \mid \mathcal{M} \models B$ for all $B \in \Gamma\}$.) $\Lambda$ is weakly complete with respect to $\mathbb{M}$ if for any formula $A$ such that $\mathbb{M} \models A$, $A \in \Lambda$.*

Strong completeness implies weak completeness by taking $\Gamma = \varnothing$. Weak completeness does not in general imply strong completeness. However, in a logic such as S4 (or linear logic), which includes a modality $\Box$ (! in linear logic) such that $\Box A \to B$ holds iff $B$ is a global semantic consequence of $A$, weak completeness does imply *finite* strong completeness, i.e., strong completeness for finite sets of formulas $\Gamma$. In other sections, particularly those that discuss linear logic, the term 'completeness' always refers to weak completeness.

**Definition 3.16** *A set of formulas $\Gamma$ is called maximal $\Lambda$-consistent if it is $\Lambda$-consistent and no proper superset is $\Lambda$-consistent. Such a set is called an $\Lambda$-MCS.*

**Lemma 3.17 (Lindenbaum's Lemma)** *Every $\Lambda$-consistent set of formulas is a subset of some $\Lambda$-MCS.*

**Proof.** [2], Lemma 4.17. Essentially, we can enumerate the set of all formulas, and starting with an $\Lambda$-consistent set $\Gamma$, add $A$ or $\neg A$ for each formula $A$, whichever preserves $\Lambda$-consistency; by the Law of the Excluded Middle, at least one of these formulas can be added to any $\Lambda$-consistent set while preserving consistency. □

**Definition 3.18** *The canonical model for a normal modal logic $\Lambda$ is the model $\mathcal{M}_\Lambda = (W_\Lambda, R_\Lambda, L_\Lambda)$ where $W_\Lambda$ is the set of all $\Lambda$-MCSs, $w \; R_\Lambda \; w'$ iff $\Box A \in w$ implies $A \in w'$ for all formulas $A$, and $L_\Lambda = \left\{ (w, a) \in W_\Lambda \times \text{Atoms} \;\middle|\; a \in w \right\}$.*

**Lemma 3.19** *In the canonical model for $\Lambda$, $w \; R_\Lambda \; w'$ iff $A \in w'$ implies $\Diamond A \in w$ for all formulas $A$.*

**Proof.** [2], Lemma 4.19 (we have exchanged definition and lemma). □

**Theorem 3.20 (Canonical Model Theorem)** *Any normal modal logic is strongly complete with respect to its canonical model.*

**Proof.** [2], Theorem 4.22. □

This theorem is what is needed to prove completeness for the usual normal modal logics.

**Definition 3.21** *A formula $A$ is canonical for a property $P$ of frames if the canonical frame for any normal modal logic containing $A$ has property $P$, and $A$ is sound for frames with property $P$.*

Clearly, by the Canonical Model Theorem, a normal modal logic generated by a set of formulas $A_i$ that are canonical for properties $P_i$ respectively is sound and complete for the class of frames satisfying all the properties $P_i$.

**Proposition 3.22** *The axioms D, T, B, 4, and 5 are canonical for seriality, reflexivity, symmetry, transitivity, and the Euclidean property of frames respectively.*

**Proof.** By Proposition 3.12 these axioms are sound for frames with the corresponding properties. It remains to prove that the presence of these axioms forces canonical frames to satisfy the corresponding properties. We consider the axiom 5; the other cases are similar and are proved in [2], Theorems 4.27 and 4.28.

Suppose $w_1$, $w_2$, and $w_3$ are $\Lambda$-MCSs for some normal modal logic $\Lambda$ containing Axiom 5, and $w_1 \; R_\Lambda \; w_2$ and $w_1 \; R_\Lambda \; w_3$. We must show that $w_2 \; R_\Lambda \; w_3$. Suppose $A \in w_3$. Then by Lemma 3.19, $\Diamond A \in w_1$. Since $w_1$ is an $\Lambda$-MCS, and $\Box\Diamond A$ is $\Lambda$-deducible from $\Diamond A$ using the axiom 5, $\Box\Diamond A \in w_1$. Thus by the definition of $R_\Lambda$, $\Diamond A \in w_2$. Using Lemma 3.19 again, we have shown that $w_2 \; R_\Lambda \; w_3$. So the canonical frame for $\Lambda$ is Euclidean, as was to be proven. □

**Corollary 3.23 (Completeness)** *The normal modal logic generated by any subset of the axioms D, T, B, 4, and 5 is complete with respect to the class of frames with the corresponding properties as in Proposition 3.22.*

On the other hand, there are some axioms that are not canonical for any property of frames. A good discussion of this, with examples of such axioms, can be found in [2], section 4.4.

## 3.7 Algebraic Semantics

**Definition 3.24** *A Boolean algebra $\mathcal{X} = (\mathcal{X}, \neg, \wedge, \top)$ consists of a set $\mathcal{X}$ together with a function $\wedge : \mathcal{X} \times \mathcal{X} \to \mathcal{X}$, a function $\neg : \mathcal{X} \to \mathcal{X}$, and an element $\top \in \mathcal{X}$, satisfying the following properties for $p, q, r \in \mathcal{X}$ (we write $p \vee q$ for $\neg(\neg p \wedge \neg q)$, and $\bot$ for $\neg\top$):*

- *Involutivity of negation:* $\neg\neg p = p$
- *Commutativity and associativity of* $\wedge$ *(and dually* $\vee$*)*
- *Unit laws:* $p \wedge \top = p$, $p \vee \bot = p$
- *Absorption laws:* $p \wedge \bot = \bot$, $p \vee \top = \top$
- *Distributivity:* $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$, $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$

- *Law of the Excluded Middle:* $p \vee \neg p = \top$

*A* *Boolean algebra with operator (BAO)* $\mathcal{X} = (\mathcal{X}, \neg, \wedge, \top, g)$ *consists of a Boolean algebra* $(\mathcal{X}, \neg, \wedge, \top)$ *together with a function* $g : \mathcal{X} \rightarrow \mathcal{X}$ *satisfying the following additional property:*

- *Distributivity of g over finite conjunctions:* $g(\top) = \top$, $g(p \wedge q) = g(p) \wedge g(q)$

As is usual with definitions of algebraic structures, there are some arbitrary choices to be made in the definition which have no effect on the structure defined, such as whether to make $\wedge$, $\vee$, or both primitive, and which of a set of redundant conditions to impose.

**Definition 3.25** *A* *homomorphism* *of Boolean algebras, or Boolean algebras with operators, is defined in the usual way: a function preserving the operations. An* *isomorphism* *is a bijective homomorphism.*

Boolean algebras with operators can be defined with several operators like $g$, as well as with operators of arity greater than one. Such algebras are used to model more complicated modal logics.

**Definition 3.26** *A* *power set algebra* $\mathcal{P}(X)$, *for a set* $X$, *is the Boolean algebra with* $\mathcal{X} = \mathcal{P}(X)$ *the set of subsets of* $X$, $p \wedge q = p \cap q$, $\neg p = X \setminus p$, *and* $\top = X$. *(All of the properties required for a Boolean algebra are familiar properties of the set operations.)*

*A* *set algebra* *is a subalgebra of a power set algebra, i.e., a subset of a power set algebra closed under the Boolean algebra operations* $\wedge$, $\neg$, *and* $\top$.

The simplest nontrivial power set algebra is $\mathcal{P}(\{*\})$, which is isomorphic to $\{\mathbf{T}, \mathbf{F}\}$ with the usual truth tables.

An important result is the *Stone Representation Theorem* ([2], Theorem 5.16) which states that any Boolean algebra is isomorphic to a set algebra. The proof of this theorem is nonconstructive, using Zorn's Lemma.

**Definition 3.27** *An assignment on a BAO $\mathcal{X}$ is a function $f : \text{Atoms} \to \mathcal{X}$.*

*The interpretation $[\![A]\!]$ of a basic modal logic formula $A$ under an assignment $f$ is defined by interpreting each connective by the corresponding operation, where $p \to q = \neg p \vee q$, $\Box p = g(p)$, and $\Diamond p = \neg g(\neg p)$, and interpreting atoms by $[\![a]\!] = f(a)$.*

**Definition 3.28** *The (full) complex algebra of a frame $(W, R)$ is the power set algebra $\mathcal{P}(W)$ with operator*

$$g(p) = \{\, w \in W \mid w\, R\, w' \text{ implies } w' \in p \,\}.$$

**Proposition 3.29** *The interpretation of a formula $A$ in a model $\mathcal{M} = (W, R, L)$ is equal to the interpretation of $A$ in the full complex algebra of $(W, R)$ under the assignment $f(a) := \{\, w \in W \mid (w, a) \in L \,\}$.*

**Proof.** The result follows immediately from the definitions of the interpretations. □

Thus frames and models may be viewed as special cases of boolean algebras with operators and assignments.

**Theorem 3.30** *Every normal modal logic $\Lambda$ is sound and complete for the class of BAOs validating its formulas.*

**Proof.** Soundness is immediate; completeness follows from completeness for the *Lindenbaum-Tarski algebra* ([2], Theorem 5.32). This algebra is the Boolean algebra with operators on the set of equivalence classes of formulas under provable equivalence in $\Lambda$, with the operations defined by the corresponding connectives on representatives. It must be checked that the Lindenbaum-Tarski algebra is in fact a member of the specified class of BAOs ([2], Theorem 5.33). □

It can be shown that a BAO validating a set of axioms validates the normal modal logic generated by those axioms; indeed, the conditions on a BAO validate the axioms and inference rules from the definition of a normal modal logic. Thus, the normal modal logic generated by a set of axioms is sound and complete for the class of BAOs validating the axioms.

The algebraic semantics is used in studying the problem of completeness for classes of frames, via the *Jónsson-Tarski Theorem* ([2], Theorem 5.43) which is the equivalent of the Stone Representation Theorem for BAOs: it states that every BAO is isomorphic to a subalgebra of the full complex algebra of some frame (called a *complex algebra*).

## 3.8 Temporal Logic

Temporal logics are a special case of modal logics in which formulas are considered to represent time-dependent properties, and modalities to represent the temporal relationships among such properties. The basic temporal modalities are F ('true at some time in the future') and P ('true at some time in the past'); these have de Morgan duals G ('always true in the future') and H ('always true in the past') respectively. From here there are a number of variations in use (see, for instance, [2, 4, 16]):

**Unidirectional vs. bidirectional.** Unidirectional temporal logics contain only modalities that refer to the future; a property at a given time cannot depend on things that occurred in the past. (The modalities could equivalently be considered to refer only to the past.) Bidirectional temporal logics contain both past and future connectives. Most of the other variations are independent of this choice, so we will discuss them only for unidirectional temporal logics.

**Linear time vs. branching time.** Linear time temporal logics refer to a single timeline: they can be modeled by assigning valuations to elements of a linear order. Branching time temporal logics refer to many possible futures; in this way they incorporate both temporal modalities and the traditional modalities of necessity and possibility. These two kinds of modalities may be represented by separate connectives, as in CTL* (which is sometimes called a *mixed branching-time/linear-time logic*), or by connectives combining both temporal and traditional modal features ('necessarily always true in the future', etc.), as in CTL.

**Discrete time vs. continuous time.** Discrete time temporal logics refer to time as a sequence of discrete points, like the clock cycles of a computer. Continuous time temporal logics refer to time as a real-valued (or sometimes rational-valued) quantity. Discrete-time temporal logics normally provide an additional modality X, 'true in the next time step'. Continuous-time temporal logics do not have such a modality, or have a modality $\mathrm{X}_t$, 'true $t$ units of time from now', where $t$ is continuous-valued. Such logics are sometimes called *timed logics*.

**Untils.** In addition to the usual temporal modalities, connectives with the meaning "$A$ remains true *until* some time when $B$ is true" are often considered. These connectives have little additional cost in model-checking applications, and they are very useful in practice to express meaningful properties. They also admit some expressive completeness results (see [2], section 7.2).

**Fixpoints.** Fixpoint operators are the characteristic feature of modal mu-calculi, which will be discussed in the next section. They allow recovery of the usual temporal operators including untils, as well as considerable additional expressive power, starting with just a next-time modality.

There are also more trivial variations, such as whether the future includes the present and whether we accept the D axiom $\mathrm{G}\,A \to \mathrm{F}\,A$ in branching-time logics.

Many temporal logics do not have good deductive systems, and the applications of temporal logic consist primarily of *model-checking* techniques, in which a system is modeled by a (usually finite) relational model for a suitable temporal logic, and desired properties are checked by evaluating the interpretations of corresponding formulas. In this way temporal logics are used quite differently from usual modal logics. The study of proof theory of temporal logics is largely confined to the modal mu-calculus, which will be described in the next chapter.

We consider here an example of a logic that is widely used in applications [8], and that can be characterized as a discrete unidirectional branching-time temporal logic with untils. This is the logic CTL developed by Clarke and Emerson [7]; we use the formulation from Huth and Ryan [16]. This choice of properties is well-adapted to modeling of computer systems: synchronous computers are inherently discrete time systems; the properties of interest describe what a program *will do* after some initial state, so a unidirectional logic is sufficient; and nondeterminism can be modeled by branching.

**Definition 3.31** *The formulas of Computation Tree Logic (CTL) are defined by the following BNF:*

$$\begin{array}{lcl} \textbf{formula}, A, B & ::= & \textbf{atom} \mid \neg A \mid A \wedge B \mid A \vee B \mid A \rightarrow B \\ & & \mid \mathrm{AX}\, A \mid \mathrm{AG}\, A \mid \mathrm{AF}\, A \mid \mathrm{A}[A \,\mathrm{U}\, B] \\ & & \mid \mathrm{EX}\, A \mid \mathrm{EF}\, A \mid \mathrm{EG}\, A \mid \mathrm{E}[A \,\mathrm{U}\, B] \end{array}$$

**Definition 3.32** *We interpret CTL in a right-unbounded Kripke model, with the notation* AX *for* $\Box$ *and* EX *for* $\Diamond$*, and extend the definition of the satisfaction relation with the following clauses:*

- $\mathcal{M}, w \Vdash \mathrm{AG}\, A$ *if we have* $\mathcal{M}, w' \Vdash A$ *for every world* $w'$ *reachable by finitely many steps of* $R$ *from* $w$*;*
- $\mathcal{M}, w \Vdash \mathrm{AF}\, A$ *if on every infinite path* $w = w_0\ R\ w_1\ R\ w_2 \cdots$*, we have* $\mathcal{M}, w_i \Vdash A$ *for some* $i \in \mathbb{N}$*;*
- $\mathcal{M}, w \Vdash \mathrm{A}[A \,\mathrm{U}\, B]$ *if on every infinite path* $w = w_0\ R\ w_1\ R\ w_2 \cdots$*, we have* $\mathcal{M}, w_i \Vdash B$ *for some* $i \in \mathbb{N}$*, and* $\mathcal{M}, w_j \Vdash A$ *for* $0 \leqslant j < i$*;*
- $\mathcal{M}, w \Vdash \mathrm{EF}\, A$ *if we have* $\mathcal{M}, w' \Vdash A$ *for some world* $w'$ *reachable by finitely many steps of* $R$ *from* $w$*;*
- $\mathcal{M}, w \Vdash \mathrm{EG}\, A$ *if there is an infinite path* $w = w_0\ R\ w_1\ R\ w_2 \cdots$*, such that* $\mathcal{M}, w_i \Vdash A$ *for all* $i \in \mathbb{N}$*;*
- $\mathcal{M}, w \Vdash \mathrm{E}[A \,\mathrm{U}\, B]$ *if there is an infinite path* $w = w_0\ R\ w_1\ R\ w_2 \cdots$*, such that* $\mathcal{M}, w_i \Vdash B$ *for some* $i \in \mathbb{N}$*, and* $\mathcal{M}, w_j \Vdash A$ *for* $0 \leqslant j < i$*.*

Thus A represents 'necessarily true', in the sense of 'true in every possible future', and E represents 'possibly true'. These must be combined with one of the temporal modalities X ('true in the next time'), F ('true at some time in the future'), G ('always true in the future') or the binary modality $A \, \mathrm{U} \, B$ ('$A$ remains true until some future time when $B$ is true'). In CTL, the future is taken to include the present. The term 'states' is usually used instead of 'worlds', reflecting the main application area in verification of computer-based systems.

Other related systems (see, for example, [16]) include LTL, which is a linear-time logic with connectives X, G, F, and U, and CTL*, which is a two-sorted logic that allows the temporal modalities to be separated from necessity/possibility modalities.

**Example 3.33** Some typical properties that can be expressed in CTL:

- It is not possible for a request to remain continuously asserted indefinitely without being granted:

  $$\mathrm{AG} \neg \mathrm{EG}(a \wedge \neg b)$$

  where $a$ denotes assertion of the request and $b$ granting of the request.

- After a piece of data is written to a queue (of length one), the data is read before any more data is written:

  $$\mathrm{AG}(a \rightarrow \mathrm{A}[\neg a \, \mathrm{U} \, b \wedge \neg a])$$

  where $a$ denotes writing of data and $b$ denotes reading of data.

On the other hand, a typical property that cannot be expressed in CTL is "It is possible for a system to stop processing transactions indefinitely", i.e., some formula is true only *finitely often* along some path. (For a proof see [7].)

# Chapter 4

# Modal Mu-Calculus

## 4.1 Motivation

The modal mu-calculus is a logic that combines many of the best features of basic modal logic and temporal logics such as CTL. It includes most of the usual temporal logics as sublogics, while remaining finitary and having a reasonable semantics and a sound and complete deductive system satisfying a cut-elimination property. Although model-checking for modal mu-calculus is harder than for usual temporal logics in the worst case, in practice model checking is efficient for the kinds of formulas that arise in practice, including, in particular, translations of usual temporal logic formulas [4, 8].

The modal mu-calculus was introduced by Kozen [17], who also proposed an axiomatization but did not prove its completeness. Fixpoint operators had been previously used in temporal logics, such as by Emerson and Clarke [10]. Completeness remained an open problem until Walukiewicz proved it more than ten years later [29]. Other (mostly more complicated) complete axiomatizations exist, for some of which completeness was known earlier than for Kozen's axiomatization.

Cut-elimination has only recently been considered; Aldwinckle and Cockett [1] introduced a new deductive system that is equivalent to Kozen's axiomatization and satisfies a cut-elimination property. This result is much better than anything that is available from a proof-theoretical point of view for usual temporal logics such as CTL.

This chapter follows primarily Stirling and Bradfield [4], which is an excellent introduction to the modal mu-calculus. Model checking in the modal mu-calculus and many other temporal logics is discussed in Clarke, Grumberg, and Peled [8]. Huth and Ryan [16] discuss fixed point interpretations for CTL.

The main idea of modal mu-calculus is that formulas such as $\mathrm{EG}\,A$ of CTL, "it is possible that $A$ always holds in the future", can be interpreted in terms of pre-fixed points and post-fixed points. If $\mathrm{EG}\,A$ is true at some state, then $A$ is true at that state and $\mathrm{EG}\,A$ is true at some successor state. This can be written as $\mathrm{EG}\,A \rightarrow A \wedge \mathrm{EX}\,\mathrm{EG}\,A$. Now suppose we replace $\mathrm{EG}\,A$ with an atom $a$. We get $a \rightarrow A \wedge \mathrm{EX}\,a$. In a given model, a set of states that can be assigned to $a$ (replacing the previous interpretation of $a$) and validate this formula is called a *post-fixed point* of $\lambda\alpha.\,A \wedge \mathrm{EX}\,\alpha$. In the modal mu-calculus, we can *define* $\mathrm{EG}\,A$ to be the greatest post-fixed point of $\lambda\alpha.\,A \wedge \mathrm{EX}\,\alpha$, denoted $\nu\alpha.\,A \wedge \mathrm{EX}\,\alpha$. That it is indeed the *greatest* post-fixed point that is needed can be seen from the fact that if $a$ is interpreted by any post-fixed point, then $a \rightarrow \mathrm{EG}\,A$ should hold.

Dually, for a formula $\mathrm{AF}\,A$, meaning "it is necessary that $A$ holds at some time in the future", we have $A \vee \mathrm{AX}\,\mathrm{AF}\,A \rightarrow \mathrm{AF}\,A$. A set of worlds that can be assigned to $a$ and satisfy the corresponding formula $A \vee \mathrm{AX}\,a \rightarrow a$ with $\mathrm{AF}\,A$ replaced by $a$ is called a *pre-fixed point* of $\lambda\alpha.\,A \vee \mathrm{AX}\,\alpha$. The modal mu-calculus allows the least such pre-fixed point to be specified by a formula $\mu\alpha.\,A \vee \mathrm{AX}\,\alpha$. It turns out that the modal mu-calculus can translate all of CTL using just the modalities AX and EX. (See [4, 8] and section 3.9 of [16].)

The least pre-fixed point and greatest post-fixed point are often called the least fixed point and greatest fixed point, respectively, since they are in fact fixed points. Determining which fixpoint operator to use to express a particular property can be difficult; Stirling and Bradfield [4] describe some techniques that can be used for this purpose.

In the modal mu-calculus, it is usual to work with multiple modalities, often infinitely many. That is, modal mu-calculus is defined as *Hennessy-Milner logic*, with modal operators $[x]$ and $\langle x\rangle$ for $x$ in some set $X$, augmented with fixpoint operators. A typical use for such a logic is to use the modalities to represent *actions* of a process; so $\langle x\rangle\top$ would mean 'the process can do an $x$ action' and $\nu\alpha.\langle x\rangle\alpha$ means 'the process can do infinitely many successive $x$-actions'. The subject of such *process logics* has been extensively studied.

## 4.2 Syntax

**Definition 4.1** *The formulas of modal mu-calculus are defined by the following BNF:*

$$\begin{array}{lll} \mathbf{formula}, A, B & ::= & \mathbf{atom} \mid \neg A \mid A \wedge B \mid A \vee B \mid A \to B \\ & & \mid [\,\mathbf{label}\,]A \mid \langle\,\mathbf{label}\,\rangle A \mid \mu\,\mathbf{atom}\,.A \mid \nu\,\mathbf{atom}\,.A \end{array}$$

*We additionally require that in formulas of the form $\mu\alpha. A$ or $\nu\alpha. A$, the atom $\alpha$ occurs only positively in $A$.*

Letters $a$, $b$, ...denote atoms, and letters $A$, $B$, $C$, ...denote formulas. Letters $\alpha$, $\beta$, ...are used to denote bound atoms. Letters $x$, $y$, ...denote labels. It is not always assumed that there is an infinite set of labels; if there is only one label, then the modal connectives may be denoted $\Box$ and $\Diamond$.

The quantifiers $\mu\alpha.$ and $\nu\alpha.$ are called *fixpoint operators.*

**Convention 4.2** *The unary connectives excluding fixpoint operators have the highest binding priority, followed by the binary connectives and finally the fixpoint operators. (In general, unary quantifiers are suffixed with a dot as a notational convention to indicate that they have low precedence.)*

A convention is also required for bound atoms. We would like to regard formulas that differ only in the names of bound atoms as identical. More precisely, given a formula such as $\mu\alpha.\,\mu\beta.\,a \wedge \alpha \wedge (\nu\beta.\,\alpha \vee \beta)$, we may replace each bound occurrence of an atom $\alpha$ by an integer specifying the number of quantifiers whose scopes contain the occurrence of $\alpha$ and are strictly contained in the scope of the quantifier binding $\alpha$. In this example, we obtain $\mu\alpha.\,\mu\beta.\,a \wedge 1 \wedge (\nu\beta.\,2 \vee 0)$. We then remove the atoms from the quantifiers to obtain $\mu.\,\mu.\,a \wedge 1 \wedge (\nu.\,2 \vee 0)$, and regard two formulas as equal if their translations are identical. Such translations can be used as an alternate representation for formulas, and integers used in this way are known as *de Bruijn indices.* Replacement of one formula by an equivalent formula with bound variables renamed is known as *alpha-conversion.*

**Convention 4.3** *Formulas are always considered up to alpha-conversion, although representatives are chosen for notational purposes. When induction on formulas is used, representatives are chosen in such a way that bound atoms are all distinct and do not occur freely in any formula under consideration.*

The latter convention is known as *Barendregt's convention.* It ensures, for instance, that in the usual definition of the substitution $A[B/a]$ by distributivity over all connectives including quantifiers, free variables in $B$ do not become bound by quantifiers in $A$.

To use Barendregt's convention, we must ensure that we will always be able to choose a fresh atom. We will never consider infinitely many formulas at once, so it is enough to assume that the set Atoms is infinite.

## 4.3 Semantics

We consider here only the interpretation of modal mu-calculus with a single pair of modal connectives; interpretation of multi-modal mu-calculus is similar.

The modal mu-calculus is most easily interpreted using the set-of-worlds interpretation of formulas in the relational semantics. First it is necessary to define an operation of substitution on models:

**Definition 4.4** *If $\mathcal{M} = (W, R, L)$ is a Kripke model and $X \subset W$, then $\mathcal{M}[X/\alpha]$ is the model based on the frame $(W, R)$, with labeling $L'$ defined by*

$$L' := \Big(L \setminus (W \times \{\alpha\})\Big) \cup (X \times \{\alpha\})$$

**Definition 4.5** *A lambda-abstraction or context is of the form $\lambda\alpha.\, A$ where $\alpha$ is an atom and $A$ is a formula.*

**Definition 4.6** *The interpretation of formulas $A$ by sets of worlds $[\![A]\!]$, and of contexts $\lambda\alpha.\, A$ by functions $[\![\lambda\alpha.\, A]\!]$ from sets of worlds to sets of worlds, in a model $\mathcal{M}$ is defined inductively by:*

- $[\![a]\!] := \{\, w \mid (w, a) \in L \,\}$

- $[\![\neg A]\!] := W \setminus [\![A]\!]$
- $[\![A \wedge B]\!] := [\![A]\!] \cap [\![B]\!]$
- $[\![A \vee B]\!] := [\![A]\!] \cup [\![B]\!]$
- $[\![A \to B]\!] := (W \setminus [\![A]\!]) \cup [\![B]\!]$
- $[\![\Box A]\!] := \{\, w \mid \textit{for all } w' \textit{ such that } w \, R \, w',\ w \in [\![A]\!] \,\}$
- $[\![\Diamond A]\!] := \{\, w \mid \textit{there exists } w' \textit{ such that } w \, R \, w' \textit{ and } w \in [\![A]\!] \,\}$
- $[\![\lambda\alpha.\, A]\!](X) := [\![A]\!]_{\mathcal{M}[X/\alpha]}$
- $[\![\mu\alpha.\, A]\!] := \bigcap \{\, X \subset W \mid [\![\lambda\alpha.\, A]\!](X) \subset X \,\}$
- $[\![\nu\alpha.\, A]\!] := \bigcup \{\, X \subset W \mid X \subset [\![\lambda\alpha.\, A]\!](X) \,\}$

Note that because of the presence of bound variables, the inductive definition does not stay within one model.

**Definition 4.7** *A set $X \subset W$ is called a pre-fixed point of $\lambda\alpha.\, A$ in a model $\mathcal{M}$ if $[\![\lambda\alpha.\, A]\!](X) \subset X$, a post-fixed point if $[\![\lambda\alpha.\, A]\!](X) \supset X$, and a fixed point if $[\![\lambda\alpha.\, A]\!](X) = X$.*

**Proposition 4.8** *$[\![\mu\alpha.\, A]\!]$ and $[\![\nu\alpha.\, A]\!]$ are fixed points of $\lambda\alpha.\, A$.*

**Proof.** It is easily checked that the function $[\![\lambda\alpha.\, A]\!]$ is monotone (increasing) in $X$ for $A$ positive in $\alpha$. Thus, the property of being a pre-fixed point (resp. post-fixed point) of $\lambda\alpha.\, A$ is preserved by intersections (unions), so the interpretation of a $\mu$-formula ($\nu$-formula) is indeed the least pre-fixed point (greatest post-fixed point).

Now suppose $X$ is the least pre-fixed point of $\lambda\alpha.\, A$. By monotonicity, $[\![\lambda\alpha.\, A]\!](X)$ is also a pre-fixed point of $\lambda\alpha.\, A$; and if it were strictly smaller than $X$, that would contradict minimality of $X$, so it must be equal to $X$ and $X$ is a fixed point. Similarly the greatest post-fixed point must be a fixed point to avoid contradicting maximality. □

Because of this property, the least pre-fixed point is often called the least fixed point, and similarly the greatest post-fixed point is called the greatest fixed point.

## 4.4 Deductive Systems

There is a simple axiomatization of the modal mu-calculus, called *Kozen's axiomatization* [17] (see also [4]). It adds to multi-modal **K** logic one axiom and one inference rule:

- Axiom: $A[\mu\alpha.\,A/\alpha] \to \mu\alpha.\,A$
- Inference rule: If $B \to A[B/\alpha]$, then $B \to \nu\alpha.\,A$.

Soundness of the axiom follows from the fact that the interpretation of $\mu\alpha.\,A$ is a (pre-)fixed point of $\lambda\alpha.\,A$, while soundness of the inference rule follows from the fact that validity of $B \to A[B/\alpha]$ implies that $[\![B]\!]$ is a post-fixed point of $\lambda\alpha.\,A$, and $\nu\alpha.\,A$ is interpreted by the greatest post-fixed point.

On the other hand, completeness remained an open question for more than ten years [4]. It was finally proven by Igor Walukiewicz in [29].

This deductive system can be written in sequent calculus form; the rules consist of the rules of classical sequent calculus together with the following rules, shown in two-sided form:

$$\frac{\Gamma \vdash \Delta, A}{[x]\Gamma \vdash \langle x\rangle\Delta, [x]A}\,[x]\mathrm{R} \qquad \frac{\Gamma, A \vdash \Delta}{[x]\Gamma, \langle x\rangle A \vdash \langle x\rangle\Delta}\,\langle x\rangle\mathrm{L}$$

$$\frac{\Gamma \vdash \Delta, A[\mu\alpha.\,A/\alpha]}{\Gamma \vdash \Delta, \mu\alpha.\,A}\,\mu\mathrm{R} \qquad \frac{\Gamma, A[\nu\alpha.\,A/\alpha] \vdash \Delta}{\Gamma, \nu\alpha.\,A \vdash \Delta}\,\nu\mathrm{L}$$

$$\frac{B \vdash A[B/\alpha]}{B \vdash \nu\alpha.\,A}\,\nu\mathrm{R} \qquad \frac{A[B/\alpha] \vdash B}{\mu\alpha.\,A \vdash B}\,\mu\mathrm{L}$$

The equivalence between classical sequent calculus and the classical Hilbert system is easily extended to the mu-calculus, showing that this sequent calculus is sound and complete for the semantics.

More recent work by Aldwinckle and Cockett [1] considers an alternative deductive system that allows cut-elimination, using what are called the *circular proof rules.* To prove $\Gamma \vdash \Delta, \nu\alpha.\,A$ ($\nu$-introduction on the right), the sequent $\Gamma \vdash \Delta, A$ is proved with assumption $\Gamma \vdash \Delta, \alpha$, where $\alpha$ does not occur freely (including in outstanding assumptions) except in $A$. (The use of sequents as assumptions that can be discharged is analogous to such use of formulas in natural deduction systems.) Also, to prove a sequent $\Gamma \vdash \Delta, \alpha$ where there is an open assumption corresponding to $\nu\alpha. A$, a fresh atom $\beta$ and a new assumption $\Gamma \vdash \Delta, \beta$ can be introduced and the sequent $\Gamma \vdash \Delta, A[\beta/\alpha]$ proved; this rule is known as *regeneration*. When regeneration is used, any assumptions involving $\alpha$ are duplicated with $\alpha$ replaced with $\beta$. $\mu$ on the left is handled dually. In [1], the cut-elimination property, soundness and completeness, and equivalence with Kozen's axiomatization are proven.

# Chapter 5

# Modal Linear Logic

## 5.1 Motivation

In this chapter we will consider possible ways of combining linear logic and modal logic. There are several reasons that we might want to do so. One reason is simply to see if the additional distinctions of linear logic have any effect on the theory of modalities. Also, modalities might be useful in applications of linear logic. One way to use modalities in linear logic is that some traditional modalities, such as temporal connectives, can apply to resources as well as to facts.

It is also possible to use modalities in linear logic in ways that do not apply to usual logics. The best-known example of modalities specific to linear logic is the exponentials, which have been part of linear logic since its introduction by Girard in [11]. Modalities might also be used to describe incidental information about resources. For instance, in modeling a computer system, $[x]a$ might mean that a process $x$ controls a resource $a$, while the formula $a$ on its own might mean that the resource $a$ is available to be allocated. While such information can be maintained by means of predicates in classical logic, using linear logic has the advantage of intrinsically being able to describe various combinations of resources using the linear connectives.

Two approaches to obtaining modal linear logics will be considered. One is to construct a deductive system based on a classical deductive system for **K** or one of the other well-known modal logics, specifically those from [23, 24]. This approach builds on earlier work such as Martini and Masini's work on 'linear exponentials' [22] and D'Agostino et al.'s work on modalities in general implication systems including a fragment of linear logic [9], although the details of the algebraic semantics appear to be new (except for the similarity between **S4** and the linear exponentials). Soundness and completeness are proved using the techniques of Girard's proofs of soundness and completeness for LLSC [11, 12].

The other approach is to generalize the relational semantics of modal logic to apply to linear logic. This is done in a way that does not appear to have been previously considered, using phase spaces together with Kripke frames. A deductive system is developed which also appears to be new, although the general technique of indexed sequents used in its definition is well-known [5]. Soundness and completeness theorems are proved, and the resulting logic is compared with that obtained by the first approach. It is proved that the two logics are distinct, while being conservative over linear logic and corresponding to the same classical modal logic **KD**.

## 5.2 Syntax

**Definition 5.1** *The formulas of (basic) modal linear logic are defined by the following BNF:*

$$\begin{array}{lcl} \mathbf{formula}, A, B & ::= & \mathbf{atom} \mid \mathbf{atom}^{\perp} \mid A \otimes B \mid A \parr B \mid A \mathbin{\&} B \mid A \oplus B \\ & & \mid \mathbf{1} \mid \perp \mid \top \mid \mathbf{0} \mid\ !A \mid\ ?A \mid \Box A \mid \Diamond A \end{array}$$

*We extend the negation of linear logic with* $(\Box A)^{\perp} := \Diamond(A^{\perp})$ *and* $(\Diamond A)^{\perp} := \Box(A^{\perp})$.

**Convention 5.2** *The unary connectives have the highest binding priority, followed by the binary connectives.*

Fragments of modal linear logic can be defined in the same way as for plain linear logic. Of particular interest is modal MALL, obtained by dropping the exponentials ! and ?. Multi-modal linear logic is also possible, replacing $\Box$ and $\Diamond$ with $[x]$ and $\langle x \rangle$ for $x$ in some set $X$.

## 5.3 Modal Axiomatics in Linear Logic

The syntactic approach to modal linear logics is straightforward: We simply consider LLSC extended with sequent rules for the modal connectives. We recall the sequent rules from the classical case:

$$\textbf{K:}\qquad \frac{\vdash \Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box\Diamond_{\mathbf{K}}$$

$$\textbf{KD:}\qquad \frac{\vdash \Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box\Diamond_{\mathbf{KD}} \qquad \frac{\vdash \Gamma}{\vdash \Diamond\Gamma}\,\Diamond_{\mathbf{KD}}$$

$$\textbf{T:}\qquad \frac{\vdash \Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box\Diamond_{\mathbf{T}} \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, \Diamond A}\,\Diamond_{\mathbf{T}}$$

$$\textbf{S4:}\qquad \frac{\vdash \Diamond\Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box_{\mathbf{S4}} \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, \Diamond A}\,\Diamond_{\mathbf{S4}}$$

None of these rules involve any of the classical connectives, except for those implicit in the sequent formalism, so there are no choices to be made in translating them to linear logic; they can be used as they are. Corresponding to each of these modal logics there is a linear equivalent: $\mathbf{K}_{\text{lin}}$, $\mathbf{KD}_{\text{lin}}$, etc.

This approach has been used in almost all prior work on modalities in linear logic. Martini and Masini [22] considered LL sequent calculus with the Contraction and Weakening rules dropped, which is identical to MALL with an **S4** modality !, and proved a cut-elimination theorem. D'Agostino, Gabbay, and Russo [9] defined syntax and quantale-based semantics for (a fragment of) linear logic with modalities, in a general way that applies also to intuitionistic and classical logic.

The definition of a normal modal logic generalizes naturally to linear logic. However, since we are interested in cut-elimination, the sequent presentation is more useful.

From a syntactic point of view, it is important to verify that the usual results continue to hold: the substitution theorem and cut-elimination.

**Proposition 5.3 (Substitution)** *The following is a derivable rule in LL sequent calculus with any of the four sets of modal sequent rules and with the Identity rule* *restricted to atomic formulas:*

$$\dfrac{\vdash A_1^{\perp}, A_1' \quad \vdash A_2^{\perp}, A_2' \quad \cdots \quad \vdash A_n^{\perp}, A_n'}{\vdash B^{\perp}[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n], B[A_1'/\alpha_1, A_2'/\alpha_2, \ldots, A_n'/\alpha_n]}\,{\scriptstyle \mathrm{ST}} \quad \textit{(B positive in } \alpha_i\textit{),}$$

**Proof.** We consider the derived rules from the proof of Theorem 2.10 with one additional rule $\mathrm{ST}_{\Box,\Diamond}$, derivable in all four logics:

$$\dfrac{\vdash A^{\perp}, A'}{\vdash \Box A^{\perp}, \Diamond A'}\,{\scriptstyle \Box\Diamond_{\mathrm{K/KD/T}}} \qquad \dfrac{\dfrac{\vdash A^{\perp}, A'}{\vdash A^{\perp}, \Diamond A'}\,{\scriptstyle \Diamond_{\mathrm{S4}}}}{\vdash \Box A^{\perp}, \Diamond A'}\,{\scriptstyle \Box_{\mathrm{S4}}}$$

Now the inductive argument from the proof of Theorem 2.10 holds. □

**Proposition 5.4 (Cut-Elimination)** *Any sequent provable in LL sequent calculus with one of the four sets of modal rules is provable without the* Cut *rule.*

**Proof.** The proof is the same as for Theorem 2.12, with the following additional rewrite rules (which are the same as in the classical case proved by Ohnishi and Matsumoto [23, 24]) depending on which rules are used for the modalities:

$$\dfrac{\dfrac{\pi_1\,\overline{\vdash \Gamma, A}}{\vdash \Diamond\Gamma, \Box A}\,{\scriptstyle \Box\Diamond_{\mathrm{K/KD/T}}} \quad \dfrac{\pi_2\,\overline{\vdash A^{\perp}, \Delta, B}}{\vdash \Diamond A^{\perp}, \Diamond\Delta, \Box B}\,{\scriptstyle \Box\Diamond_{\mathrm{K/KD/T}}}}{\vdash \Diamond\Gamma, \Diamond\Delta, \Box B}\,{\scriptstyle \mathrm{Cut}} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_1\,\overline{\vdash \Gamma, A} \quad \pi_2\,\overline{\vdash A^{\perp}, \Delta, B}}{\vdash \Gamma, \Delta, B}\,{\scriptstyle \mathrm{Cut}}}{\vdash \Diamond\Gamma, \Diamond\Delta, \Box B}\,{\scriptstyle \Box\Diamond_{\mathrm{K/KD/T}}}$$

$$\dfrac{\dfrac{\pi_1\,\overline{\vdash \Gamma, A}}{\vdash \Diamond\Gamma, \Box A}\,{\scriptstyle \Box\Diamond_{\mathrm{KD}}} \quad \dfrac{\pi_2\,\overline{\vdash A^{\perp}, \Delta}}{\vdash \Diamond A^{\perp}, \Diamond\Delta}\,{\scriptstyle \Diamond_{\mathrm{KD}}}}{\vdash \Diamond\Gamma, \Diamond\Delta}\,{\scriptstyle \mathit{Cut}} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_1\,\overline{\vdash \Gamma, A} \quad \pi_2\,\overline{\vdash A^{\perp}, \Delta}}{\vdash \Gamma, \Delta}\,{\scriptstyle \mathrm{Cut}}}{\vdash \Diamond\Gamma, \Diamond\Delta}\,{\scriptstyle \Diamond_{\mathrm{KD}}}$$

$$\dfrac{\dfrac{\pi_1\,\overline{\vdash \Gamma, A}}{\vdash \Diamond\Gamma, \Box A}\,{\scriptstyle \Box\Diamond_{\mathrm{T}}} \quad \dfrac{\pi_2\,\overline{\vdash A^{\perp}, \Delta}}{\vdash \Diamond A^{\perp}, \Delta}\,{\scriptstyle \Diamond_{\mathrm{T}}}}{\vdash \Diamond\Gamma, \Delta}\,{\scriptstyle \mathrm{Cut}} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_1\,\overline{\vdash \Gamma, A} \quad \pi_2\,\overline{\vdash A^{\perp}, \Delta}}{\vdash \Gamma, \Delta}\,{\scriptstyle \mathrm{Cut}}}{\vdash \Diamond\Gamma, \Delta}\,{\scriptstyle \Diamond^{*}_{\mathrm{T}}}$$

$$\dfrac{\pi_1\,\overline{\vdash \Gamma, A^{*}} \quad \dfrac{\pi_2\,\overline{\vdash A^{\perp *}, \Delta, B}}{\vdash A^{\perp *}, \Delta, \Diamond B}\,{\scriptstyle \Diamond_{\mathrm{T/S4}}}}{\vdash \Gamma, \Delta, \Diamond B}\,{\scriptstyle \mathrm{Cut}*} \quad \Longrightarrow \quad \dfrac{\dfrac{\pi_1\,\overline{\vdash \Gamma, A^{*}} \quad \pi_2\,\overline{\vdash A^{\perp *}, \Delta, B}}{\vdash \Gamma, \Delta, B}\,{\scriptstyle \mathrm{Cut}*}}{\vdash \Gamma, \Delta, \Diamond B}\,{\scriptstyle \Diamond_{\mathrm{T/S4}}}$$

$$\dfrac{\dfrac{\pi_1\,\overline{\vdash \Diamond\Gamma, A}}{\vdash \Diamond\Gamma, \Box A}\,{\scriptstyle \Box_{\mathrm{S4}}} \quad \dfrac{\pi_2\,\overline{\vdash A^{\perp}, \Delta}}{\vdash \Diamond A^{\perp}, \Delta}\,{\scriptstyle \Diamond_{\mathrm{S4}}}}{\vdash \Diamond\Gamma, \Delta}\,{\scriptstyle \mathrm{Cut}} \quad \Longrightarrow \quad \dfrac{\pi_1\,\overline{\vdash \Diamond\Gamma, A} \quad \pi_2\,\overline{\vdash A^{\perp}, \Delta}}{\vdash \Diamond\Gamma, \Delta}\,{\scriptstyle \mathrm{Cut}}$$

$$\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Diamond\Gamma, \Box A} \qquad \dfrac{{}^{\pi_2}\dfrac{}{\vdash \Diamond A^{\perp}, \Diamond\Delta, B}}{\vdash \Diamond A^{\perp}, \Diamond\Delta, \Box B}\,\Box_{\mathrm{S4}}}{\vdash \Diamond\Gamma, \Diamond\Delta, \Box B}\,\mathrm{Cut} \quad \Longrightarrow \quad \dfrac{\dfrac{{}^{\pi_1}\dfrac{}{\vdash \Diamond\Gamma, \Box A} \qquad {}^{\pi_2}\dfrac{}{\vdash \Diamond A^{\perp}, \Diamond\Delta, B}}{\vdash \Diamond\Gamma, \Diamond\Delta, B}\,\mathrm{Cut}}{\vdash \Diamond\Gamma, \Diamond\Delta, \Box B}\,\Box_{\mathrm{S4}}$$

All of these cut-elimination rules satisfy the necessary condition on cut degrees, and they cover all of the additional cases both for principal and non-principal formulas that arise with modal connectives. For **S4**, as for the linear exponentials which are based on this modality, there are certain cases where a non-principal reduction cannot be applied on one side but some reduction must apply on the other. □

All of the results above generalize easily to the case of multiple modal connectives. Indeed, full LL with an added modality already has two independent modalities, since the exponentials are treated as modalities.

## 5.4 Algebraic Semantics

As shown in the previous subsection, extending modal inference rules to linear logic is straightforward. The next question to ask is whether or not it is possible to define an equally simple semantics. Indeed, this can be done by extending the algebraic semantics of modal logic.

**Definition 5.5** *A* **K**-*modal topolinear space* $\mathcal{X} = (X, \perp, \times, 1, \mathcal{K}, g)$ *is a topolinear space* $\mathcal{X} = (X, \perp, \times, 1, \mathcal{K})$ *together with a function* $g : \mathcal{X} \to \mathcal{X}$ *satisfying the following properties for* $F, G \in \mathcal{X}$.

- $F \subset G$ *implies* $g(F) \subset g(G)$ *(monotonicity)*
- $\mathbf{1} \subset g(\mathbf{1})$ *(half-distributivity over* $\mathbf{1}$*)*
- $g(F) \otimes g(G) \subset g(F \otimes G)$ *(half-distributivity over tensor)*

As in the case of open facts in topolinear spaces, the properties of $g$ are chosen to build soundness of the deductive system into the models. In fact, for completeness it will suffice to consider the case where $g(F) = (h(F))^{\perp\perp}$ where $h$ is a monoid endomorphism on $(X, \times, 1)$. However, in the tradition of algebraic semantics, only those conditions required to guarantee soundness are built in.

Similarly, we can define models for other modal linear logics.

**Definition 5.6** *A* **K***-modal topolinear space* $\mathcal{X}$ *is called:*

- *a* **KD***-modal topolinear space if* $g(\perp) \subset \perp$
- *a* **T***-modal topolinear space if* $g(F) \subset F$ *for all* $F \in \mathcal{X}$
- *an* **S4***-modal topolinear space if* $g(F) = (F \cap Y)^{\perp\perp}$ *for a submonoid* $Y$ *of* $X$

*The term 'modal topolinear space' is used to refer to any of these possibilities ambiguously.*

Clearly, a **T**-modal topolinear space is a **KD**-modal topolinear space, and an **S4**-modal topolinear space is a **T**-modal topolinear space.

The modal connectives have corresponding operations on modal topolinear spaces.

**Definition 5.7** *The connectives* $\Box$ *and* $\Diamond$ *are defined on modal topolinear spaces as follows:*

- $\Box F := g(F)$
- $\Diamond F := \left(g(F^{\perp})\right)^{\perp}$

So a modal connective $\Box$ is simply interpreted by a function on facts satisfying certain properties, and $\Diamond$ is interpreted by duality. This is analogous to BAOs for the classical case.

**Definition 5.8** *A modal topolinear model* $\mathcal{M} = (\mathcal{X}, f)$ *is defined analogously to a topolinear model:* $\mathcal{X}$ *is a modal topolinear space and* $f$ *is a function* $\text{Atoms} \to \mathcal{X}$.

The interpretation of formulas and sequences of formulas is defined in a manner exactly analogous to interpretation in topolinear models: connectives are interpreted by the corresponding operations.

**Proposition 5.9 (Soundness)** *If $\vdash \Gamma$ is provable in* **K***-modal LLSC, then $1 \in [\![\Gamma]\!]$ in every* **K***-modal topolinear model $\mathcal{M}$ (and similarly for* **KD**, **T**, *and* **S4***).*

**Proof.** The proof is by induction on a derivation of $\vdash \Gamma$, and it is enough to verify those cases that do not occur in usual LLSC.

For **K**, there is only the $\Box\Diamond_{\mathbf{K}}$ rule. Suppose we have a proof ending in this rule. We write it in two-sided form (left-hand formulas just stand in for their negations on the right):

$$\frac{A_1, A_2, \ldots, A_n \vdash B}{\Box A_1, \Box A_2, \ldots, \Box A_n \vdash \Box B}\,\Box\Diamond_{\mathbf{K}}$$

where $\Gamma = A_1, A_2, \ldots, A_n$. Now we have

$$[\![\Box A_1 \otimes \Box A_2 \otimes \cdots \otimes \Box A_n]\!] = g([\![A_1]\!]) \otimes g([\![A_2]\!]) \otimes \cdots \otimes g([\![A_n]\!]).$$

By repeated application of half-distributivity of $g$ over tensor (or over $\mathbf{1}$ if $n = 0$), we obtain

$$g([\![A_1]\!]) \otimes g([\![A_2]\!]) \otimes \cdots \otimes g([\![A_n]\!]) \subset g([\![A_1]\!] \otimes [\![A_2]\!] \otimes \cdots \otimes [\![A_n]\!]).$$

Now by the induction hypothesis, $1 \in [\![\Gamma^\perp, B]\!] = [\![(\invamp \Gamma^\perp) \invamp B]\!] = ([\![A_1]\!] \otimes [\![A_2]\!] \otimes \cdots \otimes [\![A_n]\!]) \multimap [\![B]\!]$, and by Proposition 2.29,

$$[\![A_1]\!] \otimes [\![A_2]\!] \otimes \cdots \otimes [\![A_n]\!] \subset [\![B]\!].$$

Now by monotonicity of $g$,

$$g([\![A_1]\!] \otimes [\![A_2]\!] \otimes \cdots \otimes [\![A_n]\!]) \subset g([\![B]\!]) = [\![\Box B]\!].$$

Combining the above inclusions by transitivity, we obtain

$$[\![\Box A_1 \otimes \Box A_2 \otimes \cdots \otimes \Box A_n]\!] \subset [\![\Box B]\!].$$

Again using Proposition 2.29, this gives $1 \in [\![\Box A_1 \otimes \Box A_2 \otimes \cdots \otimes \Box A_n]\!] \multimap [\![\Box B]\!]$, and rewriting this by the definition of interpretation and duality, we obtain $1 \in [\![\Diamond\Gamma^\perp, \Box B]\!]$ as required.

For **KD**, we also have the $\Diamond_{\mathbf{KD}}$ rule. Suppose we have a proof ending in this rule:

$$\frac{\vdash \Gamma}{\vdash \Diamond\Gamma}\,\Diamond_{\mathbf{KD}}$$

By the induction hypothesis, $1 \in [\![\Gamma]\!] = [\![\Gamma]\!] \parr \bot = [\![\Gamma, \bot]\!]$. By soundness of the **K**-rule as shown above, $1 \in [\![\Diamond\Gamma, \Box\bot]\!] = [\![\Diamond\Gamma]\!] \parr [\![\Box\bot]\!]$. Finally, since $[\![\Box\bot]\!] = g(\bot) \subset \bot$, we get $1 \in [\![\Diamond\Gamma]\!]$ as required.

For **T**, we also have the $\Diamond_{\mathbf{T}}$ rule. Soundness of this rule, however, is clear from $[\![A]\!] \subset [\![\Diamond A]\!]$, which follows from $F \subset \left(g(F^{\perp})\right)^{\perp}$ which follows in turn from the condition $g(F) \subset F$ for all $F$.

For **S4**, we also have the $\Box_{\mathbf{S4}}$ rule. Suppose we have a proof ending in this rule:

$$\frac{\Box A_1, \Box A_2, \ldots, \Box A_n \vdash B}{\Box A_1, \Box A_2, \ldots, \Box A_n \vdash \Box B}\,\Box_{\mathbf{S4}}$$

where $\Gamma = A_1, A_2, \ldots, A_n$. Now we have

$$[\![\Box A_1 \otimes \Box A_2 \otimes \cdots \otimes \Box A_n]\!] = g([\![A_1]\!]) \otimes g([\![A_2]\!]) \otimes \cdots \otimes g([\![A_n]\!]).$$

Using the condition on $g$ and Proposition 2.29, we obtain

$$[\![\Box A_1 \otimes \Box A_2 \otimes \cdots \otimes \Box A_n]\!] = \Big(([\![A_1]\!] \cap Y)([\![A_2]\!] \cap Y) \cdots ([\![A_n]\!] \cap Y)\Big)^{\perp\perp} = F^{\perp\perp}$$

where $F = \big([\![A_1]\!] \cap Y\big)\big([\![A_2]\!] \cap Y\big) \cdots \big([\![A_n]\!] \cap Y\big)$. But since $Y$ is a submonoid, $F \subset Y$. Now $F^{\perp\perp} = (F \cap Y)^{\perp\perp} \subset (F^{\perp\perp} \cap Y)^{\perp\perp}$, and $(F^{\perp\perp} \cap Y) \subset F^{\perp\perp}$, so $F^{\perp\perp} = (F^{\perp\perp} \cap Y)^{\perp\perp} = \Box F^{\perp\perp}$. By the induction hypothesis, $1 \in [\![\Diamond\Gamma^{\perp}, B]\!] = [\![(\parr \Diamond\Gamma^{\perp}) \parr B]\!] = F^{\perp\perp} \multimap [\![B]\!]$, and by Proposition 2.29, $F^{\perp\perp} \subset [\![B]\!]$. Now

$$[\![\Box B]\!] = ([\![B]\!] \cap Y)^{\perp\perp} \supset (F^{\perp\perp} \cap Y)^{\perp\perp} = F^{\perp\perp},$$

so again by Proposition 2.29, $1 \in F^{\perp\perp} \multimap [\![\Box B]\!] = [\![\Diamond\Gamma^{\perp}, \Box B]\!]$ as required.

The appropriate cases above, together with the usual cases for linear logic, complete the induction and the proof of soundness for all four logics. □

**Proposition 5.10 (Completeness)** *If* $1 \in [\![\Gamma]\!]$ *in every* **K**-*modal topolinear model* $\mathcal{M}$, *then* $\vdash \Gamma$ *is provable in* **K**-*modal LLSC, and similarly for* **KD**, **T**, *and* **S4**.

**Proof.** To prove completeness, we must extend the syntactic topolinear model for LLSC to a syntactic modal topolinear model $\mathcal{M}_{\mathrm{syn}}$. Recall that

$$\mathrm{Pr}(A) := \{\, \Gamma \mid \Gamma \vdash A \text{ is provable} \,\},$$

$X = \mathrm{Pr}(\top)$ is the set of multisets of formulas, $\perp = \mathrm{Pr}(\perp)$ is the set of multisets of formulas provable as sequents, $\times$ is concatenation of multisets, and 1 is the empty multiset. The function $g : \mathcal{X} \to \mathcal{X}$ is defined by $g(F) := \big(h(F)\big)^{\perp\perp}$, where $h : X \to X$ is defined by $h(\Gamma) := \Box\Gamma$.

First we check that $g$ satisfies the necessary conditions. Since $h$ is clearly a monoid homomorphism, the conditions for a **K**-modal topolinear space are immediate. If we are considering **KD**, $g(\perp) = \{\, \Box\Gamma \mid \Gamma \vdash \text{ is provable } \}^{\perp\perp} \subset \perp$ by the $\Diamond_{\mathbf{KD}}$ rule and Proposition 2.29. If we are considering **T**, $g(F) = \{\, \Box\Gamma \mid \Gamma \in F \,\}^{\perp\perp} \subset F$ since provability of $\Gamma, \Delta \vdash$ implies provability of $\Box\Gamma, \Delta \vdash$ by repeated application of the $\Diamond_{\mathbf{T}}$ rule.

Finally, if we are considering **S4**, we let $Y$ be the set of multisets of formulas with principal connective $\Box$, which is clearly a submonoid of $X$. We show that $h(F)$ and $F \cap Y$ have the same negation. Indeed, as we have seen for **T**, $\Gamma \in F$ implies $\Box\Gamma \in F$, so $h(F) \subset F \cap Y$ and $\big(h(F)\big)^{\perp} \supset (F \cap Y)^{\perp}$. For the other inclusion, suppose $\Gamma \in \big(h(F)\big)^{\perp}$, i.e., $\Gamma, \Box\Delta \vdash$ is provable for all $\Delta \in F$. Now if $\Box\Delta \in F$, then $\Gamma, \Box\Box\Delta \vdash$ is provable, and since $\Box A \vdash \Box\Box A$ is provable for any formula $A$ by the rules Id and $\Box_{\mathbf{S4}}$, $\Gamma, \Box\Delta \vdash$ is provable using Cut. Thus $\Gamma \in (F \cap Y)^{\perp}$. So $\big(h(F)\big)^{\perp} = (F \cap Y)^{\perp}$ and $g(F) = \big(h(F)\big)^{\perp\perp} = (F \cap Y)^{\perp\perp}$ as required.

Now only one thing remains to be proved to make the completeness argument for topolinear models work, and that is that $\mathrm{Pr}(\Box A) = \Box\,\mathrm{Pr}(A)$; then $\mathrm{Pr}(\Diamond A) = \Diamond\,\mathrm{Pr}(A)$ by duality (Lemma 2.44) and the proof goes through.

By the $\Box\Diamond_{\mathbf{K}}$-rule (which is derivable in the other logics), $h(\mathrm{Pr}(A)) \subset \mathrm{Pr}(\Box A)$, and since $\mathrm{Pr}(\Box A)$ is a fact by Lemma 2.44, by Proposition 2.29 we obtain $\big(h(\mathrm{Pr}(A))\big)^{\perp\perp} \subset \mathrm{Pr}(\Box A)$, or $\Box\,\mathrm{Pr}(A) \subset \mathrm{Pr}(\Box A)$.

For the other inclusion, we need $\mathrm{Pr}(\Box A) \subset \big(h(\mathrm{Pr}(A))\big)^{\perp\perp}$, or by Lemma 2.25, $\mathrm{Pr}(\Box A)\big(h(\mathrm{Pr}(A))\big)^{\perp} \subset \perp$. Suppose $\Gamma \in \mathrm{Pr}(\Box A)$ and $\Delta \in \big(h(\mathrm{Pr}(A))\big)^{\perp}$. Then $\Gamma \vdash \Box A$ is provable, and $\Delta, \Box\Lambda \vdash \perp$ is provable for all $\Lambda$ such that $\Lambda \vdash A$. In particular, take

$\Lambda = A$, then $\Delta, \Box A \vdash \bot$ is provable, and by the Cut rule, $\Gamma, \Delta \vdash \bot$ is provable, so $\Gamma, \Delta \in \bot$. Since $\Gamma$ and $\Delta$ were arbitrary, the inclusion $\mathrm{Pr}(\Box A)\big(h(\mathrm{Pr}(A))\big)^{\perp} \subset \bot$ follows. Thus, $\mathrm{Pr}(\Box A) = \Box\,\mathrm{Pr}(A)$ and the proof of completeness goes through. □

This proof of completeness treats the modal connectives very similarly to the exponential connectives ! and ?. This is not especially surprising, since the exponentials in LLSC (without free storage) are treated as a special kind of modality, and the non-structural rules for the exponentials, Dereliction and Storage, are the same as the rules for **S4**.

It should also be noted that the proof of completeness generalizes easily to the case of multiple modal connectives.

None of the results for modal axiomatics and algebraic semantics in linear logic are particularly different from known results in classical modal logic and linear logic with exponential modalities. This is in contrast to the relational semantics to be considered next, which does not agree with the classically corresponding algebraic semantics.

## 5.5 Relational Semantics

A second approach to constructing a modal linear logic is to generalize the relational semantics of modal logic, which have almost come to define modal logic. This approach is not quite so straightforward. In fact, the usual presentation of relational structures makes use of the Boolean truth values $\{\mathbf{T}, \mathbf{F}\}$, for which there is no linear logic analogue. However, the truth values of classical relational semantics can be replaced with power set algebras while preserving soundness and completeness.

**Definition 5.11** *A powerset Kripke model $\mathcal{M} = (\mathcal{F}, X, f)$ consists of a frame $\mathcal{F} = (W, R)$, a set $X$, and a labeling $f : W \times \mathrm{Atoms} \to \mathcal{P}(X)$.*

*The interpretation of a modal formula $A$ at a world $w$ in a powerset Kripke model $\mathcal{M}$ is a subset of $X$ defined by $[\![a]\!]_w := f(w,a)$, $[\![\Box A]\!]_w := \bigcap_{wRw'} [\![A]\!]_{w'}$, $[\![\Diamond A]\!]_w := \bigcup_{wRw'} [\![A]\!]_{w'}$, and the usual Boolean algebra interpretation for the classical connectives.*

*A modal formula $A$ is valid in a powerset Kripke model $\mathcal{M}$ if $[\![A]\!]_w = X$ at all worlds $w$. It is valid if it is valid in all power set algebra relational models.*

**Proposition 5.12** *Validity in the class of powerset Kripke models based on a class of frames $\mathbb{F}$ is equivalent to validity in the class of (usual) Kripke models based on $\mathbb{F}$.*

**Proof.** It is clear that validity in a powerset Kripke model $\mathcal{M} = (\mathcal{F}, X, f)$ is equivalent to validity in the set of Kripke models $\{ \mathcal{M}_x = (\mathcal{F}, L_x) \mid x \in X \}$, where $L_x \subset W \times \text{Atoms}$ is defined by $(w, a) \in L_x$ iff $x \in f(w, a)$; the result follows trivially. □

As we have seen, power set algebras are a special case of phase spaces; so we can attempt to generalize this variant of the classical modal semantics to linear logic.

**Definition 5.13** *A topolinear Kripke model $\mathcal{M} = (\mathcal{F}, \mathcal{X}, f)$ consists of a frame $\mathcal{F} = (W, R)$, a topolinear space $\mathcal{X} = (X, \perp, \times, 1, \mathcal{K})$, and a labeling $f : W \times \text{Atoms} \to \mathcal{X}$.*

**Definition 5.14** *The interpretation $[\![A]\!]_w$ of a formula $A$ at a world $w$ in a topolinear Kripke model $\mathcal{M}$ is defined inductively by:*

- $[\![a]\!]_w := f(w, a)$
- $[\![A \otimes B]\!]_w := [\![A]\!]_w \otimes [\![B]\!]_w$ *and similarly for the other linear logic connectives*
- $[\![\Box A]\!]_w := \bigcap \{ [\![A]\!]_{w'} \mid w \mathrel{R} w' \}$
- $[\![\Diamond A]\!]_w := \left( \bigcup \{ [\![A]\!]_{w'} \mid w \mathrel{R} w' \} \right)^{\perp\perp}$

*The interpretation of a sequence of formulas $\Gamma$ is defined as for topolinear models, i.e., by par.*

These definitions also are straightforward generalizations of the classical case. However, we will see that the algebraic and relational semantics defined here in fact determine different logics.

## 5.6 A Deductive System for the Relational Semantics

The search for a straightforward axiomatization of the relational semantics on usual sequents appeared to lead nowhere. However, a sequent calculus for the relational semantics can be constructed by the use of sequents with additional structure, called *indexed sequents*. This technique has been used for classical modal logic, such as by Braüner [5] to obtain cut-elimination for **S5**, and in earlier work by M. Fitting and by G. Mints. We consider **KD** modal logic because there is a problem with using **K**, which will be considered later.

**Definition 5.15** *An indexed formula is of the form* $[s]\,A$ *where* $A$ *is a formula and* $s \in \mathbb{N}^*$. *An indexed sequent is of the form* $\vdash \Gamma$ *where* $\Gamma$ *is a sequence of indexed formulas. If* $s$ *is empty, the indexed formula* $[s]\,A$ *may be abbreviated* $A$.

Here $\mathbb{N}^*$ denotes the set of finite sequences of natural numbers. Sequences are denoted $s, t, \ldots$. Concatenation of sequences is written $*$, and the empty sequence is written $\varepsilon$. If $s = t * t'$ then we say that $t$ is an *initial subsequence* of $s$, even if $t' = \varepsilon$.

Sequences of indexed formulas are denoted $\Gamma, \Delta, \ldots$. It will be specified whether or not a particular sequence consists of indexed formulas, when it is not clear from context.

**Definition 5.16** *The set of indices of a sequence of indexed formulas* $\Gamma$, *denoted* $\mathrm{Ind}(\Gamma)$, *is the set of initial subsequences of indices occurring in* $\Gamma$. *If* $\Gamma$ *is empty we define* $\mathrm{Ind}(\Gamma) = \{\varepsilon\}$. *If* $\mathrm{Ind}(\Gamma) = \{\varepsilon\}$ *then we say* $\Gamma$ *is closed.*

**Definition 5.17** *The* $\mathbf{KD}_{\mathrm{r}}$*-modal linear logic sequent calculus is defined on indexed sequents* $\vdash \Gamma$ *by the following rules:*

$$\frac{}{\vdash [s]\,A, [s]\,A^{\perp}}\,\mathrm{Id} \qquad \frac{\vdash \Gamma, [s]\,A \quad \vdash [s]\,A^{\perp}, \Delta}{\vdash \Gamma, \Delta}\,\mathrm{Cut} \qquad \frac{\vdash \Gamma}{\vdash \sigma(\Gamma)}\,\mathrm{Ex}$$

$$\frac{\vdash \Gamma, [s]\,A \quad \vdash \Gamma, [s]\,B}{\vdash \Gamma, [s]\,A \,\&\, B}\,\& \qquad \frac{}{\vdash \Gamma, [s]\,\top}\,\top \qquad \frac{\vdash \Gamma, [s]\,A}{\vdash \Gamma, [s]\,A \oplus B}\,\oplus_1 \qquad \frac{\vdash \Gamma, [s]\,B}{\vdash \Gamma, [s]\,A \oplus B}\,\oplus_2$$

$$\frac{\vdash \Gamma, [s]\,A \quad \vdash \Delta, [s]\,B}{\vdash \Gamma, \Delta, [s]\,A \otimes B}\,\otimes \qquad \frac{}{\vdash [s]\,\mathbf{1}}\,\mathbf{1} \qquad \frac{\vdash \Gamma, [s]\,A, [s]\,B}{\vdash \Gamma, [s]\,A \parr B}\,\parr \qquad \frac{\vdash \Gamma}{\vdash \Gamma, [s]\,\bot}\,\bot$$

$$\frac{\vdash \Gamma, [s]\,A}{\vdash \Gamma, [s]\,?A}\,\mathrm{D} \qquad \frac{\vdash ?\Gamma, [s]\,A}{\vdash ?\Gamma, [s]\,!A}\,\mathrm{S} \qquad \frac{\vdash \Gamma}{\vdash \Gamma, [s]\,?A}\,\mathrm{W} \qquad \frac{\vdash \Gamma, [s]\,?A, [s]\,?A}{\vdash \Gamma, [s]\,?A}\,\mathrm{C}$$

$$\frac{\vdash \Gamma, [s * i]\,A}{\vdash \Gamma, [s]\,\Box A}\,\Box \quad (s * i \notin \mathrm{Ind}(\Gamma)) \qquad \frac{\vdash \Gamma, [s * i]\,A}{\vdash \Gamma, [s]\,\Diamond A}\,\Diamond$$

*In the case of the Storage rule,* $?\Gamma$ *means to apply* $?$ *to each of the formulas in* $\Gamma$*, leaving the indices untouched.*

In this sequent calculus $\Box$ and $\Diamond$ play the role of quantifiers, and indices act as free variables. However, as in usual modal logics, there is no need for a notion of bound variables in formulas, as they are implicit in the modal connectives. On the other hand, as in classical predicate logic, there is a notion of bound variables in *proofs*: the index $s{*}i$ (or rather, its final element $i$) in the $\Box$ rule is effectively bound by that rule.

Again we check that the usual syntactic results hold. The use of indexed formulas requires the Substitution Theorem to be stated somewhat differently.

**Definition 5.18** *An occurrence of a literal* $\alpha$ *in a formula* $A$ *is said to have (modal) depth* $d$ *if it is in the scope of* $d$ *modal connectives.*

*The set of depths at which a literal* $\alpha$ *occurs in a formula* $A$ *is denoted* $D_\alpha(A)$.

**Proposition 5.19 (Substitution)** *The following is a derivable rule in* $\mathbf{KD}_{\mathfrak{r}}$*-modal LLSC with the Identity rule restricted to atomic formulas:*

$$\frac{\cdots \quad \vdash [s * 0^d]\, A_i^{\perp}, [s * 0^d]\, A_i' \quad \cdots}{\vdash [s]\, B^{\perp}[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n], [s]\, B[A_1'/\alpha_1, A_2'/\alpha_2, \ldots, A_n'/\alpha_n]}\,\mathrm{ST}$$

*where* $B$ *is positive in* $\alpha_i$*, and there is a premise* $\vdash [s * 0^d]\, A_i^{\perp}, [s * 0^d]\, A_i'$ *for each* $i \in \{1, 2, \ldots, n\}$ *and each* $d \in D_{\alpha_i}(B)$.

**Proof.** We consider the derived rules from the proof for LLSC, extended with indices $s$ on all formulas, with one additional rule $\mathrm{ST}_{\Box,\Diamond}$:

$$\cfrac{\cfrac{\vdash [s * 0]\, A^{\perp}, [s * 0]\, A'}{\vdash [s * 0]\, A^{\perp}, [s]\, \Diamond A'}\,\Diamond}{\vdash [s]\, \Box A^{\perp}, [s]\, \Diamond A'}\,\Box$$

Now the inductive argument from the proof of Theorem 2.10 holds. The definition of depth ensures that if $B = \alpha_i$, then there is a premise with indices $s$, and that in the inductive cases, the premises needed for the smaller instances of ST are among those supplied. $\Box$

The requirement to provide premises with different indices for occurrences at different depths is a result of the way indices are used. However, it is not a major problem, since provability is invariant under common prefixes on indices. This will be proven later using cut-elimination.

**Definition 5.20** *Given a proof $\pi$, the substitution of $j$ for $i$ under $s$ in $\pi$, denoted $\pi[s * (j/i)]$, is defined by replacing every initial subsequence $s * i$ of an index in $\pi$ with $s * j$. We require for the moment that $s * j$ not occur in the set of indices of any sequent in $\pi$; thus, it is clear that the side condition on the $\Box$ rule is preserved and the result is a well-formed proof.*

In the case where a proof ends in a $\Box$ rule, a substitution in the proof of the premise for the natural number $i$ eliminated by the rule is analogous to alpha-conversion for formulas with quantifiers. We may thus apply Barendregt's convention to proofs; however, only one case is important, and that is for the process of substitution just defined. By using alpha-conversion, we can relax the requirement that $s * j$ does not occur in $\pi$ to a requirement that $s * j \notin \mathrm{Ind}(\Gamma)$, where $\Gamma$ is the conclusion of $\pi$.

**Proposition 5.21 (Cut-Elimination)** *Any sequent provable in* $\mathbf{KD}_{\mathrm{r}}$*-modal LLSC is provable without the* Cut *rule.*

**Proof.** The proof is similar to that of Theorem 2.12, but it is necessary to describe how the LLSC rewrite rules are to be interpreted on indexed sequents. For rewrite rules for non-principal cut formulas, the cut formulas are given an index $s$ and the principal formula an index $t$; for rewrite rules for principal cut formulas, the cut formulas are given an index $s$. All other formulas appearing in the rewrite rules are either premises whose indices are determined by the rules, or part of arbitrary sequences of formulas which now become arbitrary sequences of indexed formulas.

The Cut! rule on indexed sequents is written here for clarity:

$$\frac{\vdash \Gamma, [s]\,!A \quad \vdash ([s]\,?A^{\perp})^{n}, \Delta}{\vdash \Gamma, \Delta}\,\mathrm{Cut!}$$

The indices on all the cut formulas must match; this is consistent with the fact that the indices on cut formulas in a Cut rule and contracted formulas in a Contraction rule must match.

With the conventions above for indices, the LLSC rewrite rules handle all the cases not involving the modal connectives. For those connectives, three new rewrite rules are needed:

$$\dfrac{\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, [s*i]\,A, [t]\,B^*}}{\vdash \Gamma, [s]\,\Diamond A, [t]\,B^*}{\scriptstyle\Diamond} \quad {}^{\pi_2}\overline{\vdash [t]\,B^{\perp *}, \Delta}}{\vdash \Gamma, \Delta, [s]\,\Diamond A}{\scriptstyle\text{Cut}*} \quad\Longrightarrow\quad \dfrac{\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, [s*i]\,A, [t]\,B^*} \quad {}^{\pi_2}\overline{\vdash [t]\,B^{\perp *}, \Delta}}{\vdash \Gamma, \Delta, [s*i]\,A}{\scriptstyle\text{Cut}*}}{\vdash \Gamma, \Delta, [s]\,\Diamond A}{\scriptstyle\Diamond}$$

$$\dfrac{\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, [s*i]\,A, [t]\,B^*}}{\vdash \Gamma, [s]\,\Box A, [t]\,B^*}{\scriptstyle\Box} \quad {}^{\pi_2}\overline{\vdash [t]\,B^{\perp *}, \Delta}}{\vdash \Gamma, \Delta, [s]\,\Box A}{\scriptstyle\text{Cut}*} \quad\Longrightarrow\quad \dfrac{\dfrac{{}^{\pi_1[s*(j/i)]}\overline{\vdash \Gamma, [s*j]\,A, [t]\,B^*} \quad {}^{\pi_2}\overline{\vdash [t]\,B^{\perp *}, \Delta}}{\vdash \Gamma, \Delta, [s*j]\,A}{\scriptstyle\text{Cut}*}}{\vdash \Gamma, \Delta, [s]\,\Box A}{\scriptstyle\Box}$$

$$\dfrac{\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, [s*i]\,A}}{\vdash \Gamma, [s]\,\Box A}{\scriptstyle\Box} \quad \dfrac{{}^{\pi_2}\overline{\vdash [s*j]\,A^{\perp}, \Delta}}{\vdash [s]\,\Diamond A^{\perp}, \Delta}{\scriptstyle\Diamond}}{\vdash \Gamma, \Delta}{\scriptstyle\text{Cut}} \quad\Longrightarrow\quad \dfrac{{}^{\pi_1[s*(j/i)]}\overline{\vdash \Gamma, [s*j]\,A} \quad {}^{\pi_2}\overline{\vdash [s*j]\,A^{\perp}, \Delta}}{\vdash \Gamma, \Delta}{\scriptstyle\text{Cut}}$$

In the case of the second rule, we choose $j$ such that $s * j$ does not occur in $\text{Ind}(\Gamma)$ or $\text{Ind}(\Delta)$, or as an initial subsequence of $t$. These rules handle the two non-principal formula cases and one principal formula case that are new in $\mathbf{KD}_r$-modal LLSC. The last two rewrite rules make use of substitution for indices in proofs. Furthermore, the conclusions of the reducts are indeed as shown because of the free variable condition on the $\Box$ rule. $\Box$

**Proposition 5.22** *The sequent* $\vdash [s * t_1]\,A_1, [s * t_2]\,A_2, \ldots, [s * t_n]\,A_n$ *is provable iff the sequent* $\vdash [t_1]\,A_1, [t_2]\,A_2, \ldots, [t_n]\,A_n$ *is provable.*

**Proof.** A cut-free proof of one sequent can be transformed into a proof of the other by uniformly adding or deleting a common prefix on all indices. It is easily checked that the premises of any rule (except Cut) must share any common prefix of the indices in the conclusion, and that the correctness of rule applications is not affected by such common prefixes. $\Box$

Thus provability is invariant under common prefixes of indices. We can therefore consider $\mathbf{KD}_r$-modal LLSC with non-logical axioms not using indices, by allowing an arbitrary common index on the formulas of each axiom. This must be done if the non-logical axioms are intended to be globally true, as otherwise they cannot be used under modal connectives.

## 5.7 Soundness and Completeness

For the proof of soundness and completeness, it will be necessary to interpret open sequents. In order to do so, we need a notion of environment similar to what is used in predicate logic.

**Definition 5.23** *An environment $E$ in a topolinear Kripke model $\mathcal{M}$ is a function $E : V \to W$ where $V$ is a nonempty subset of $\mathbb{N}^*$ that is closed under initial subsequences, satisfying $E(s)\ R\ E(s * i)$ whenever $s * i \in V$.*

**Definition 5.24** *A sequence of indexed formulas $\Gamma$ is interpretable in an environment $E$ if $\mathrm{Ind}(\Gamma) \subset \mathrm{dom}(E)$.*

**Definition 5.25** *The interpretation of a sequence of indexed formulas $\Gamma$ in an environment $E$ in which it is interpretable is given by*

$$[\![ [s_1]\,A_1, [s_2]\,A_2, \dots, [s_n]\,A_n ]\!]_E := \bigparr_{i=1}^{n} [\![A_i]\!]_{E(s_i)}.$$

**Definition 5.26** *Given an environment $E$ with $s \in \mathrm{dom}(E)$, a natural number $i$, and a world $w$ such that $E(s)\ R\ w$, we define an environment $E[s * (w/i)] : V' \to W$, where $V' = \{\, t \in \mathrm{dom}(E) \mid t \neq s * i * r \text{ for any } r \in \mathbb{N}^* \,\} \cup \{s * i\}$, by*

$$E[s * (w/i)](t) := \begin{cases} w & \text{if } t = s * i \\ E(t) & \text{otherwise.} \end{cases}$$

It is clear that $E[s * (w/i)]$ satisfies the condition on environments, and that if $\Gamma$ is interpretable in $E$ and $s * i \notin \Gamma$, then $\Gamma$ is interpretable in $E[s * (w/i)]$ and $[\![\Gamma]\!]_{E[s*(w/i)]} = [\![\Gamma]\!]_E$.

**Proposition 5.27 (Soundness)** *If $\vdash \Gamma$ is provable in* **KD**$_\mathrm{r}$*-modal LLSC, then $1 \in [\![\Gamma]\!]_E$ for every topolinear Kripke model $\mathcal{M}$ on a right-unbounded frame and every environment $E$ in which $\Gamma$ is interpretable.*

**Proof.** The proof is by induction on a derivation of $\vdash \Gamma$, for each particular model $\mathcal{M}$ and for all environments $E$. The only two cases that differ from the proof for LLSC are when the last rule is one of the modal rules.

If the last rule is $\Box$, we have a proof of the form

$$\frac{\Delta \vdash [s * i]\, A}{\Delta \vdash [s]\, \Box A}\,\Box$$

where $s * i \notin \Delta$. We assume $1 \in \left[\!\left[\Delta^{\perp}, [s * i]\, A\right]\!\right]_E$ for all environments $E$, and we must prove $1 \in \left[\!\left[\Delta^{\perp}, [s]\, \Box A\right]\!\right]_E$ for all environments $E$ (subject to conditions of interpretability). But this can be shown by direct reasoning:

$$\begin{array}{rcl}
\left[\!\left[\Delta^{\perp}, [s]\, \Box A\right]\!\right]_E & = & [\![\Delta^{\perp}]\!]_E \mathbin{⅋} [\![\Box A]\!]_{E(s)} \\
& = & [\![\Delta^{\perp}]\!]_E \mathbin{⅋} \left(\bigcap \{\, [\![A]\!]_w \mid E(s)\; R\; w \,\}\right) \\
& = & \bigcap \{\, [\![\Delta^{\perp}]\!]_E \mathbin{⅋} [\![A]\!]_w \mid E(s)\; R\; w \,\} \\
& & \quad \text{(by distributivity of ⅋ over } \textstyle\bigcap) \\
& = & \bigcap \{\, [\![\Delta^{\perp}]\!]_{E[s*(w/i)]} \mathbin{⅋} \left[\!\left[[s * i]\, A\right]\!\right]_{E[s*(w/i)]} \mid E(s)\; R\; w \,\} \\
& = & \bigcap \{\, \left[\!\left[\Delta^{\perp}, [s * i]\, A\right]\!\right]_{E[s*(w/i)]} \mid E(s)\; R\; w \,\}
\end{array}$$

But by the induction hypothesis $1 \in \left[\!\left[\Delta^{\perp}, [s * i]\, A\right]\!\right]_{E'}$ for all environments $E'$ subject to interpretability, so $1 \in \left[\!\left[\Delta^{\perp}, [s]\, \Box A\right]\!\right]_E$ as required.

If the last rule is $\Diamond$, we have a proof of the form

$$\frac{\Delta \vdash [s * i]\, A}{\Delta \vdash [s]\, \Diamond A}\,\Diamond$$

where $s * i \in \Delta$. We assume $1 \in \left[\!\left[\Delta^{\perp}, [s * i]\, A\right]\!\right]_E$ for all environments $E$, and we must prove $1 \in \left[\!\left[\Delta^{\perp}, [s]\, \Diamond A\right]\!\right]_E$ for all environments $E$ (subject to conditions of interpretability). This time there are two cases. If $s * i \in \Delta$, then we let $E' = E$. Otherwise, we let $E' = E[s * (w/i)]$, where $w$ is a world such that $E(s)\; R\; w$, which exists by right-unboundedness. Now we proceed by direct reasoning:

$$\begin{array}{rcl}
\left[\!\left[\Delta^{\perp}, [s]\, \Diamond A\right]\!\right]_E & = & [\![\Delta^{\perp}]\!]_E \mathbin{⅋} [\![\Diamond A]\!]_{E(s)} \\
& = & [\![\Delta^{\perp}]\!]_E \mathbin{⅋} \left(\bigcup \{\, [\![A]\!]_w \mid E(s)\; R\; w \,\}\right)^{\perp\perp}
\end{array}$$

$$\begin{aligned} &\supset && [\![\Delta^\perp]\!]_{E'} \parr [\![A]\!]_{E'(s*i)} \\ &= && [\![\Delta^\perp, [s*i]\,A]\!]_{E'} \end{aligned}$$

But by the induction hypothesis $1 \in [\![\Delta^\perp, [s*i]\,A]\!]_{E'}$ for all environments $E'$ subject to interpretability, so $1 \in [\![\Delta^\perp, [s]\,\Diamond A]\!]_E$ as required. □

**Proposition 5.28 (Completeness)** *If $1 \in [\![\Gamma]\!]_E$ for every topolinear Kripke model $\mathcal{M}$ on a right-unbounded frame and every environment $E$ in which $\Gamma$ is interpretable, then $\vdash \Gamma$ is provable in* $\mathbf{KD}_\mathrm{r}$*-modal LLSC.*

To avoid problems with the exponentials, we follow the approach of [12] using Example 2.35 to present it in terms of topolinear spaces.

**Definition 5.29** *The syntactic topolinear Kripke model $\mathcal{M}_\mathrm{syn}$ is based on the topolinear space $\mathcal{X} = (X, \perp, \times, 1, \mathcal{K})$, where $X$ is the set of multisets of indexed formulas where we ignore the multiplicity of formulas with principal connective ! (this can be achieved by taking a quotient of the monoid of multisets), $\times$ is concatenation of multisets, 1 is the empty multiset, $\perp := \mathrm{Pr}_\varepsilon(\perp)$, and $\mathcal{K} := \{\, F^\perp \mid F \subset I \cap \mathbf{1} \,\}$ as in Example 2.35, where*

$$\mathrm{Pr}_s(A) := \{\, \Gamma \mid \Gamma \vdash [s]\,A \textit{ is provable in } \mathbf{KD}_\mathrm{r}\textit{-modal LLSC} \,\}.$$

*Here the set of idempotents $I$ is the set of multisets of indexed formulas with principal connective !. We take $W := \mathbb{N}^*$, $R := \{\, (s, s*i) \mid s \in \mathbb{N}^* \,\}$, and $f(s,a) := \mathrm{Pr}_s(a)$.*

*The syntactic environment $E_\mathrm{syn}$ is the identity function on $\mathbb{N}^*$.*

It was shown in Example 2.35 that the conditions on $\mathcal{K}$ are satisfied.

Due to the invertibility of the rule for $\perp$,

$$\perp = \{\, \Gamma \mid \Gamma \vdash \text{is provable in } \mathbf{KD}_\mathrm{r}\text{-modal LLSC} \,\}.$$

so in fact $\perp = \mathrm{Pr}_s(\perp)$ not just for $s = \varepsilon$, but for all indices $s$.

**Proof of Proposition 5.28** The usual completeness argument will hold if it can be shown that $[\![A]\!]_s = \mathrm{Pr}_s(A)$ for arbitrary formulas $A$. Only two inductive steps differ from the plain linear logic case with arbitrary indices added: those for the exponentials and the modal connectives.

For the exponentials, we have

$$?\,\mathrm{Pr}_s(A) = (\mathrm{Pr}_s(A^\perp) \cap I \cap \mathbf{1})^\perp.$$

We must show that this is equal to $\mathrm{Pr}_s(?A)$. Suppose $\Gamma \in \mathrm{Pr}_s(?A)$, i.e., $\Gamma \vdash [s]\,?A$ is provable. Then if $\Delta \in \mathrm{Pr}_s(A^\perp) \cap I \cap \mathbf{1}$, we have that $\Delta \vdash [s]\,A^\perp$ is provable, and $\Delta$ is composed of ! formulas. Thus by the Storage rule, $\Delta \vdash [s]\,!A^\perp$ is provable, and by the Cut rule, $\Gamma, \Delta \vdash$ is provable. Thus we have shown $Pr_s(?A) \subset ?Pr_s(A)$.

Conversely, suppose $\Gamma \in ?\,\mathrm{Pr}_s(A) = (\mathrm{Pr}_s(A^\perp) \cap I \cap \mathbf{1})^\perp$. Now $[s]\,!A^\perp \in \mathrm{Pr}_s(A^\perp)$ by the Identity and Dereliction rules, $[s]\,!A^\perp \in I$ by the definition of $X$ and $\times$, and $[s]\,!A \in \mathbf{1} = \perp^\perp$ since provability of $\Gamma \vdash$ implies provability of $\Gamma, [s]\,!A \vdash$ by the Weakening rule. So $\Gamma, [s]\,!A^\perp \vdash$, or equivalently $\Gamma \vdash [s]\,?A$, is provable. Thus $\Gamma \in \mathrm{Pr}_s(?A)$. So we have shown $?\,\mathrm{Pr}_s(A) = \mathrm{Pr}_s(?A)$ and the analogous result for ! follows by Lemma 2.44.

For the modal connectives, we consider $\Box$, and again the other case follows by duality (Lemma 2.44).

We must show that $\mathrm{Pr}_s(\Box A) = \bigcap_{i \in \mathrm{N}} \mathrm{Pr}_{s*i}(A)$. Suppose $\Gamma \in \bigcap_{i \in \mathrm{N}} \mathrm{Pr}_{s*i}(A)$. Then we may take $k \notin \Gamma$, and then $\Gamma \in \mathrm{Pr}_{s*k}(A)$. So $\Gamma \vdash [s*k]\,A$, and by the $\Box$ rule, $\Gamma \vdash [s]\,\Box A$, and $\Gamma \in \mathrm{Pr}_s(\Box A)$.

Conversely, suppose $\Gamma \in \mathrm{Pr}_s(\Box A)$. Then $\Gamma \vdash [s]\,\Box A$ is provable. We construct a proof of $\Gamma \vdash [s*i]\,A$ for arbitrary $i$:

$$\dfrac{\Gamma \vdash [s]\,\Box A \qquad \dfrac{\dfrac{}{[s*i]\,A \vdash [s*i]\,A}\,\mathrm{Id}}{[s]\,\Box A \vdash [s*i]\,A}\,\Box_{\mathrm{L}}}{\Gamma \vdash [s*i]\,A}\,\mathrm{Cut}$$

Thus $\Gamma \in \bigcap_{i \in \mathrm{N}} \mathrm{Pr}_{s*i}(A)$. So $\mathrm{Pr}_s(\Box A) = \bigcap_{i \in \mathrm{N}} \mathrm{Pr}_{s*i}(A)$, and by an inductive argument similar to that of the usual LL completeness proof, $[\![A]\!]_s = \mathrm{Pr}_s(A)$ for all $A$.

Now it is not enough to prove completeness for single formulas and extend to sequents by par, because the rule for $⅋$ does not apply to formulas with differing indices. Instead, suppose

$$1 \quad \in \quad [\![[s_1]\,A_1, [s_2]\,A_2, \ldots, [s_n]\,A_n]\!]_{\mathcal{M}_{\mathrm{syn}}, E_{\mathrm{syn}}}$$

$$
\begin{aligned}
&= \left(\llbracket A_1\rrbracket^{\perp}_{s_1}\llbracket A_2\rrbracket^{\perp}_{s_2}\cdots\llbracket A_n\rrbracket^{\perp}_{s_n}\right)^{\perp}\\
&= \left((\mathrm{Pr}_{s_1}(A_1))^{\perp}(\mathrm{Pr}_{s_2}(A_2))^{\perp}\cdots(\mathrm{Pr}_{s_1}(A_1))^{\perp}\right)^{\perp}
\end{aligned}
$$

Now $[s_i]\,A_i^{\perp} \in (\mathrm{Pr}_{s_i}(A_i))^{\perp}$ since $\Gamma \vdash [s_i]\,A_i$ is provable iff $\Gamma, [s_i]\,A_i^{\perp} \vdash$ is provable, so

$$[s_1]\,A_1^{\perp}, [s_2]\,A_2^{\perp}, \ldots, [s_n]\,A_n^{\perp} \in (\mathrm{Pr}_{s_1}(A_1))^{\perp}(\mathrm{Pr}_{s_2}(A_2))^{\perp}\cdots(\mathrm{Pr}_{s_1}(A_1))^{\perp},$$

and by the definition of negation in phase spaces,

$$1 \times \left([s_1]\,A_1^{\perp}, [s_2]\,A_2^{\perp}, \ldots, [s_n]\,A_n^{\perp}\right) \in \perp,$$

which means $[s_1]\,A_1^{\perp}, [s_2]\,A_2^{\perp}, \ldots, [s_n]\,A_n^{\perp} \vdash$ is provable, or equivalently,

$$\vdash [s_1]\,A_1, [s_2]\,A_2, \ldots, [s_n]\,A_n$$

is provable. Since the sequence of indexed formulas was arbitrary, this proves completeness. □

It seems reasonable to expect that similar techniques will work for other modal logics such as **S5**, since indexed sequents have been used in the classical case at least for **S5** [5]. However, a problem arises if we attempt to adapt the linear relational semantics to model a linear logic version of **K**.

In the case of sequent calculi for classical first-order logic, it is sometimes possible to remove the requirement that models be nonempty sets by imposing the opposite of the free variable condition for $\forall$ on $\exists$: we require that the quantified variable *does* occur in the context. This requires a modification to the Cut rule, since the presence of a variable, regardless of its position in the sequent, now involves an implicit assumption that the domain of interpretation is nonempty. The restriction is that a closed sequent cannot be obtained from an open sequent by Cut. Such a restriction may be questionable, but at least there is no restriction on Cut with only closed sequents, which are often the only sequents that we are really interested in.

A similar attempt can be made with $\mathbf{KD}_{\mathrm{r}}$-modal linear logic, imposing a free variable condition on the $\Diamond$ rule. Here it is quite clear that the intent is to construct a deductive system for closed sequents, so the restriction on Cut is not a major problem. The cut-elimination property continues to hold. The sequent $\Box a \vdash \Diamond a$ (the D axiom), which is not valid in topolinear Kripke semantics without the condition of right-unboundedness, is not provable. However, a sequent such as $\Diamond a \,\&\, \Box b \vdash \Diamond a \,\&\, \Diamond b$ is also not provable, but it is valid: when interpreted at a world with no successor, both sides are **0**. Thus, completeness fails. This seems to be a result of the fact that existence or nonexistence of worlds is treated classically; perhaps in this sense the topolinear Kripke semantics is a hybrid of linear and classical semantics. It is not clear whether or not either the semantics or the deductive system can be modified to achieve completeness, but the fact that the 'obvious' generalizations to **K** (which *do* work for classical logic) fail suggests that perhaps neither would be satisfactory even if it were possible.

## 5.8 Comparison of Algebraic and Relational Semantics

In this section we compare the algebraic and relational semantics, primarily via their sound and complete deductive systems, KD-modal and $\mathbf{KD}_{\mathrm{r}}$-modal LLSC.

**Proposition 5.30** *The rules of* **KD***-modal LLSC are derivable in* $\mathbf{KD}_{\mathrm{r}}$*-modal linear logic, if we annotate sequents with arbitrary common indices. Thus* $\mathbf{KD}_{\mathrm{lin}}$ *is included in* $\mathbf{KD}_{\mathrm{r}}$.

**Proof.** The necessary derivations are:

$$\dfrac{\dfrac{\vdash [s*i]\,\Gamma, [s*i]\,A}{\vdash [s]\,\Diamond\Gamma, [s*i]\,A}\Diamond^{\bullet}}{\vdash [s]\,\Diamond\Gamma, [s]\,\Box A}\Box \qquad \dfrac{\vdash [s*i]\,\Gamma}{\vdash [s]\,\Diamond\Gamma}\Diamond^{\bullet}$$

□

Next we consider distributivity and half-distributivity properties for the modal connectives over the linear logic connectives.

**Proposition 5.31** *The following half-distributivity properties are provable in the indicated logics.*

- *Provable in* **KD**-*modal linear logic:*

$$\Box A \otimes \Box B \vdash \Box(A \otimes B) \qquad \Box A \oplus \Box B \vdash \Box(A \oplus B) \qquad \Box(A \mathbin{\&} B) \vdash \Box A \mathbin{\&} \Box B$$

$$\Diamond(A \parr B) \vdash \Diamond A \parr \Diamond B \qquad \Diamond(A \mathbin{\&} B) \vdash \Diamond A \mathbin{\&} \Diamond B \qquad \Diamond A \oplus \Diamond B \vdash \Diamond(A \oplus B)$$

$$\Box A \otimes \Diamond B \vdash \Diamond(A \otimes B) \qquad \mathbf{1} \vdash \Box\mathbf{1} \qquad \mathbf{1} \vdash \Diamond\mathbf{1} \qquad \mathbf{0} \vdash \Box\mathbf{0} \qquad \mathbf{0} \vdash \Diamond\mathbf{0}$$

$$\Box(A \parr B) \vdash \Box A \parr \Diamond B \qquad \Diamond\bot \vdash \bot \qquad \Box\bot \vdash \bot \qquad \Diamond\top \vdash \top \qquad \Box\top \vdash \top$$

- *Provable in* $\mathbf{KD}_{\mathrm{r}}$-*modal but not* **KD**-*modal linear logic:*

$$\Diamond(A \otimes B) \vdash \Diamond A \otimes \Diamond B \qquad \Box A \mathbin{\&} \Box B \vdash \Box(A \mathbin{\&} B)$$

$$\Box A \parr \Box B \vdash \Box(A \parr B) \qquad \Diamond(A \oplus B) \vdash \Diamond A \oplus \Diamond B$$

$$\Box\mathbf{1} \vdash \mathbf{1} \qquad \Diamond\mathbf{1} \vdash \mathbf{1} \qquad \Box\mathbf{0} \vdash \mathbf{0} \qquad \Diamond\mathbf{0} \vdash \mathbf{0}$$

$$\bot \vdash \Diamond\bot \qquad \bot \vdash \Box\bot \qquad \top \vdash \Diamond\top \qquad \top \vdash \Box\top$$

- *Not provable in* $\mathbf{KD}_{\mathrm{r}}$-*modal linear logic:*

$$\Box(A \otimes B) \vdash \Box A \otimes \Box B \qquad \Box(A \parr B) \vdash \Box A \parr \Box B \qquad \Box(A \oplus B) \vdash \Box A \oplus \Box B$$

$$\Diamond A \parr \Diamond B \vdash \Diamond(A \parr B) \qquad \Diamond A \otimes \Diamond B \vdash \Diamond(A \otimes B) \qquad \Diamond A \mathbin{\&} \Diamond B \vdash \Diamond(A \mathbin{\&} B)$$

$$\Box(A \otimes B) \dashv\vdash \Box A \otimes \Diamond B \qquad \Box(A \oplus B) \dashv\vdash \Box A \oplus \Diamond B$$

$$\Box A \parr \Diamond B \dashv\vdash \Diamond(A \parr B) \qquad \Box A \mathbin{\&} \Diamond B \dashv\vdash \Diamond(A \mathbin{\&} B)$$

*(Here* $\dashv\vdash$ *is used to indicate that neither direction is provable; it is just shorthand for two sequents.)*

**Proof.** For **KD**, we consider the following proof-trees:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathrm{Id} \quad \dfrac{}{B \vdash B}\,\mathrm{Id}}{A, B \vdash A \otimes B}\,\otimes_{\mathrm{R}}}{\Box A, \Box B \vdash \Box(A \otimes B)}\,\Box\Diamond_{\mathrm{KD}}}{\Box A \otimes \Box B \vdash \Box(A \otimes B)}\,\otimes_{\mathrm{L}} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathrm{Id}}{A \vdash A \oplus B}\,\oplus_{\mathrm{R}}}{\Box A \vdash \Box(A \oplus B)}\,\Box\Diamond_{\mathrm{KD}} \quad \dfrac{\dfrac{\dfrac{}{B \vdash B}\,\mathrm{Id}}{B \vdash A \oplus B}\,\oplus_{\mathrm{R}}}{\Box B \vdash \Box(A \oplus B)}\,\Box\Diamond_{\mathrm{KD}}}{\Box A \oplus \Box B \vdash \Box(A \oplus B)}\,\oplus_{\mathrm{L}}$$

$$\dfrac{\dfrac{\dfrac{}{\vdash \mathbf{1}}\,\mathbf{1}_{\mathrm{R}}}{\vdash \Box\mathbf{1}}\,\Box\Diamond_{\mathrm{KD}}}{\mathbf{1} \vdash \Box\mathbf{1}}\,\mathbf{1}_{\mathrm{L}} \qquad \dfrac{}{\mathbf{0} \vdash \Box\mathbf{0}}\,\mathbf{0}_{\mathrm{L}}$$

It is clear that as far as cut-free proofs of half-distributivities in **KD**-modal linear logic are concerned, the only thing that can be changed (aside from the choice of two-sided presentations of the sequents) is the placement of boxes and diamonds in the modal rules. This allows both the provability and unprovability claims for **KD** to be quickly verified.

As for $\mathbf{KD_r}$-modal linear logic, it is clear from the semantics that the constants are invariant under the modal connectives. The following derivations prove the additional half-distributivities valid in this logic:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{[0]A \vdash [0]A}\,\mathrm{Id}}{\Box A \vdash [0]A}\,\Box_L}{\Box A \mathbin{\&} \Box B \vdash [0]A}\,\&_L \qquad \dfrac{\dfrac{\dfrac{}{[0]B \vdash [0]B}\,\mathrm{Id}}{\Box B \vdash [0]B}\,\Box_L}{\Box A \mathbin{\&} \Box B \vdash [0]B}\,\&_L}{\dfrac{\Box A \mathbin{\&} \Box B \vdash [0]A \mathbin{\&} B}{\Box A \mathbin{\&} \Box B \vdash \Box(A \mathbin{\&} B)}\,\Box_R}\,\&_R \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{[0]A \vdash [0]A}\,\mathrm{Id}}{\Box A \vdash [0]A}\,\Box_L \qquad \dfrac{\dfrac{}{[0]B \vdash [0]B}\,\mathrm{Id}}{\Box B \vdash [0]B}\,\Box_L}{\dfrac{\Box A \parr \Box B \vdash [0]A, [0]B}{\Box A \parr \Box B \vdash [0]A \parr B}\,\parr_R}\,\parr_L}{\Box A \parr \Box B \vdash \Box(A \parr B)}\,\Box_R$$

Again there are few possibilities for cut-free proofs of half-distributivities, and the claims of unprovability can be easily checked. (A semantic proof using counter-models would work as well.) □

It is clear why certain sequents are provable in $\mathbf{KD_r}$-modal but not **KD**-modal linear logic: in constructing a proof of one of these sequents from the bottom up, the instance of the linear logic connective inside the modality must be eliminated before the one outside. But the **KD** modal rule can only be applied to remove the enclosing modality once all formulas have modal principal connectives. The $\mathbf{KD_r}$ modal rule, on the other hand, can be applied in a situation where not all of the context formulas are modal.

Unlike in classical modal logic where, for instance, $\Box$ distributes over $\wedge$, there are no full distributivities whatsoever for the modal connectives in **KD**-modal linear logic.

Considering the informal semantics of Section 2.4, if we view formulas as representing resources available on a specified day and $\Box A$ as a coupon to obtain $A$ tomorrow, then a sequent $\Box A \otimes \Box B \vdash \Box(A \otimes B)$, valid in both logics, would mean that if we have two coupons valid tomorrow then we can treat them as a single coupon for two things, valid tomorrow; the converse, valid in neither logic, would not hold informally since a coupon generally cannot be divided. $\Box(A \mathbin{\&} B) \vdash \Box A \mathbin{\&} \Box B$, valid in both logics, would mean that if we have a coupon for a choice of items tomorrow, we can make the choice today and treat the coupon as being for only one of the items. The converse is valid in $\mathbf{KD}_\mathrm{r}$-modal but not **KD**-modal linear logic. It would mean that if we have a choice of two coupons today, then we can defer that choice to tomorrow; this should not hold in general. Thus, for this informal temporal semantics, **KD**-modal linear logic would seem to be the better choice. On the other hand, if $\Box$ is to represent a modality that should be independent of the notion of a choice represented by $\&$, then $\mathbf{KD}_\mathrm{r}$-modal linear logic might be the better alternative. No such modality is immediately apparent, however.

**Proposition 5.32** *The algebraic and relational semantics define distinct logics, conservative over linear logic, which collapse to identical logics when the classical collapse axiom (or its analogue with an arbitrary common index, as appropriate) is added.*

**Proof.** Distinctness of the **KD**-modal and $\mathbf{KD}_\mathrm{r}$-modal logics follows from the existence of sequents provable in one but not the other, as shown above. Conservativity over LL follows from the cut-elimination theorems for the two logics.

As for classical collapse, the results of Proposition 2.8 hold here as well; so the deductive systems with the CC axiom induce well-defined deductive systems on sequents of the same form but with classical rather than linear connectives. The induced deductive system for **KD**-modal linear logic is clearly equivalent to the usual classical sequent calculus for **KD**; so since **KD**-modal linear logic is included in $\mathbf{KD}_\mathrm{r}$-modal linear logic, it is enough to prove soundness of the induced deductive system for $\mathbf{KD}_\mathrm{r}$-modal linear logic for the classical relational semantics on right-unbounded frames, for which **KD**-modal classical logic is sound and complete.

Using the technique of Examples 2.32 and 2.35, we can view the power set algebra $\mathcal{P}(\{*\}) \cong \{\mathbf{T}, \mathbf{F}\}$ as a topolinear space. Now for any classical model $\mathcal{M}$ we may construct a modal topolinear model $\mathcal{M}'$ on the same frame as $\mathcal{M}$, with the topolinear space corresponding to $\{\mathbf{T}, \mathbf{F}\}$ and a labeling corresponding to the one from $\mathcal{M}$. If we identify the facts of the topolinear space with the corresponding classical truth values, we have $[\![A^C]\!]_{\mathcal{M}} = [\![A]\!]_{\mathcal{M}'}$ for any formula $A$, as is easily checked. Now soundness of

$\mathbf{KD_r}$-modal linear logic for modal topolinear models, together with soundness of the CC axiom in this particular topolinear space, imply soundness of the induced deductive system for the classical relational semantics, and the result follows. □

This is an interesting result, because it indicates that despite the fact that their axioms do not use any of the classical connectives except implication, it is possible to adapt some modal logics to linear logic in more than one way.

On the other hand, the relational semantics has serious deficiencies in the linear logic setting, particularly its inability to interpret a logic corresponding to classical **K** modal logic. Thus it is not clear whether or not this semantics should be accepted in a general notion of modal linear logics.

# Chapter 6

# Fixpoint Linear Logic

## 6.1 Motivation

In this chapter we will consider a combination of modal mu-calculus with linear logic called *fixpoint linear logic*, based on the algebraic semantics of **K**-modal linear logic. Again there are several reasons why one might want to use such a system. One reason is simply to extend the expressive power of modal linear logics. In particular, the use of fixpoint operators allows the connectives of usual temporal logics such as CTL to be recovered, as in the case of classical logic.

There is another reason to study fixpoint operators in linear logic, and that is because they give an alternative interpretation for the exponentials, based on the Free Storage rule and corresponding categorical semantics described in [18, 28]. If a satisfactory proof theory can be obtained for fixpoint linear logic, it could become a viable alternative to the usual linear logic with modal exponentials for applications of linear logic as a resource logic. As mentioned in Section 2.8, the Free Storage rule validates principles that are informally sound in a logic of resources but not sound in LL sequent calculus.

We consider first the algebraic semantics of fixpoint linear logic based on phase spaces, then a deductive system based on Kozen's axiomatization for the modal mu-calculus [17]. There does not appear to be any prior work on explicit fixpoint operators in linear logic, although certain categorical semantics such as that of Lafont [18] have made use of fixed points. We show the deductive system to be sound for the algebraic semantics and thus conservative over MALL. We then consider the syntactic (more precisely, proof-theoretical) issues of substitution and cut-elimination theorems. A rewrite system is proposed for partial cut-elimination in this system, and translations of LLSC with and without free storage into fixpoint linear logic are considered. Finally, several open problems regarding this logic are discussed, particularly completeness and weak normalization of the rewrite system.

## 6.2 Syntax

**Definition 6.1** *The formulas of fixpoint linear logic are defined by the following BNF, with the added restriction that in $\nu\alpha. A$ or $\mu\alpha. A$, $A$ must be positive in $\alpha$:*

$$\begin{array}{lcl} \textbf{formula}, A, B & ::= & \textbf{atom} \mid \textbf{atom}^\perp \mid A \otimes B \mid A \parr B \mid A \,\&\, B \mid A \oplus B \\ & & \mid \mathbf{1} \mid \perp \mid \top \mid \mathbf{0} \mid !A \mid ?A \mid [\textbf{label}]A \mid \langle\textbf{label}\rangle A \\ & & \mid \mu\,\textbf{literal}.A \mid \nu\,\textbf{literal}.A \end{array}$$

*We extend the definition of negation with $([x]A)^\perp := \langle x\rangle(A^\perp)$, $(\langle x\rangle A)^\perp := [x](A^\perp)$, $(\nu\alpha. A)^\perp := \mu\alpha^\perp.(A^\perp)$, and $(\mu\alpha. A)^\perp := \nu\alpha^\perp.(A^\perp)$.*

**Convention 6.2** *As in the case of the classical modal mu-calculus, we consider formulas up to alpha-conversion and choose representatives according to Barendregt's convention. Here we may use both positive and negative literals in quantifiers; where convenient, we will assume without loss of generality that positive literals are used.*

*Binding priorities are the same as in the classical modal mu-calculus case.*

When the set of labels consists of one element $x$, we write $\Box$ for $[x]$ and $\Diamond$ for $\langle x\rangle$.

## 6.3 Semantics

We again consider only the case of a single pair of modal connectives, and the multimodal case is similar.

We use the algebraic semantics corresponding to Axiom K since the fixpoint operations take a particularly simple form in this semantics. The definitions are similar to the classical case. Fixpoints can also be defined in the relational semantics, with formulas being interpreted by functions from worlds to facts; this approach will not be considered here.

**Definition 6.3** *If $\mathcal{M} = (\mathcal{X}, f)$ is a modal topolinear model and $F \in \mathcal{X}$, then $\mathcal{M}[F/\alpha]$ is the modal topolinear model on the modal topolinear space $\mathcal{X}$ with labeling*

$$f[F/\alpha](a) := \begin{cases} F & \textit{if } a = \alpha \\ f(a) & \textit{otherwise} \end{cases}$$

**Definition 6.4** *A lambda-abstraction or context is of the form $\lambda\alpha.\,A$ where $\alpha$ is an atom and $A$ is a formula. Lambda-abstractions on negative literals are defined according to the usual convention.*

**Definition 6.5** *The interpretation of formulas $A$ by facts $[\![A]\!] \in \mathcal{X}$, and of contexts $\lambda\alpha.\,A$ by functions $[\![\lambda\alpha.\,A]\!] : \mathcal{X} \to \mathcal{X}$, in a modal topolinear model $\mathcal{M}$ is defined inductively in the usual way with the following additional definitions for fixpoint formulas:*

- $[\![\lambda\alpha.\,A]\!](F) := [\![A]\!]_{\mathcal{M}[F/\alpha]}$
- $[\![\mu\alpha.\,A]\!] := \bigcap \{\, F \in \mathcal{X} \mid [\![\lambda\alpha.\,A]\!](F) \subset F \,\}$
- $[\![\nu\alpha.\,A]\!] := \left(\bigcup \{\, F \in \mathcal{X} \mid F \subset [\![\lambda\alpha.\,A]\!](F) \,\}\right)^{\perp\perp}$

*where we assume that quantified literals are positive.*

**Definition 6.6** *A fact $F \in \mathcal{X}$ is called a pre-fixed point of $\lambda\alpha.\,A$ in a model $\mathcal{M}$ if $[\![\lambda\alpha.\,A]\!](F) \subset F$, a post-fixed point if $[\![\lambda\alpha.\,A]\!](F) \supset F$, and a fixed point if $[\![\lambda\alpha.\,A]\!](F) = F$.*

**Lemma 6.7** *$[\![\lambda\alpha.\,A]\!]$ is monotone increasing for $A$ positive in $\alpha$.*

**Proof.** The proof is by induction on $A$. The base case is when $A = \alpha$, in which case $[\![\lambda\alpha.\,A]\!]$ is the identity function, or when $A$ is a literal distinct from $\alpha$ and $\alpha^{\perp}$, in which case it is a constant function. Otherwise, we consider cases for $A$'s principal connective:

- If $A = B \otimes C$, then by the induction hypothesis $\lambda\alpha.\, B$ and $\lambda\alpha.\, C$ are monotone increasing. Then if $F \subset G$, we have

  $$\begin{array}{rcl} [\![\lambda\alpha.\, A]\!](F) & = & ([\![\lambda\alpha.\, B]\!](F)[\![\lambda\alpha.\, C]\!](F))^{\perp\perp} \\ & \subset & ([\![\lambda\alpha.\, B]\!](G)[\![\lambda\alpha.\, C]\!](G))^{\perp\perp} \\ & = & [\![\lambda\alpha.\, A]\!](G). \end{array}$$

  The other cases of MALL connectives and exponentials are similar.

- If $A = \mu\beta.\, B$, then if $\beta$ is $\alpha$ or $\alpha^\perp$, we have a constant function. Otherwise, we have $[\![A]\!]_{\mathcal{M}} = \bigcap \{\, F \in \mathcal{X} \mid [\![B]\!]_{\mathcal{M}[F/\beta]} \subset F \,\}$. For any $F \in \mathcal{X}$, we have

  $$\begin{array}{rcl} [\![\lambda\alpha.\, A]\!]_{\mathcal{M}}(F) & = & [\![A]\!]_{\mathcal{M}[F/\alpha]} \\ & = & \bigcap \{\, H \in \mathcal{X} \mid [\![B]\!]_{\mathcal{M}[F/\alpha][H/\beta]} \subset H \,\} \\ & = & \bigcap \{\, H \in \mathcal{X} \mid [\![\lambda\alpha.\, B]\!]_{\mathcal{M}[H/\beta]}(F) \subset H \,\}. \end{array}$$

  Now suppose $F \subset G$. Then,

  $$[\![\lambda\alpha.\, B]\!]_{\mathcal{M}[H/\beta]}(F) \subset [\![\lambda\alpha.\, B]\!]_{\mathcal{M}[H/\beta]}(G)$$

  by the induction hypothesis,

  $$\{\, H \in \mathcal{X} \mid [\![\lambda\alpha.\, B]\!]_{\mathcal{M}[H/\beta]}(G) \subset H \,\} \subset \{\, H \in \mathcal{X} \mid [\![\lambda\alpha.\, B]\!]_{\mathcal{M}[H/\beta]}(F) \subset H \,\}$$

  since the first condition implies the second, and

  $$\bigcap \{\, H \in \mathcal{X} \mid [\![\lambda\alpha.\, B]\!]_{\mathcal{M}[H/\beta]}(F) \subset H \,\} \subset \bigcap \{\, H \in \mathcal{X} \mid [\![\lambda\alpha.\, B]\!]_{\mathcal{M}[H/\beta]}(G) \subset H \,\}$$

  since the intersection of a larger set is smaller. Thus we have $[\![\lambda\alpha.\, A]\!]_{\mathcal{M}}(F) \subset [\![\lambda\alpha.\, A]\!]_{\mathcal{M}}(G)$ as required.

- The case $A = \nu\beta.\, B$ is similar, or we can proceed by duality since

  $$\begin{array}{rcl} [\![\nu\beta.\, B]\!] & = & \left(\bigcup \{\, F \in \mathcal{X} \mid F \subset [\![\lambda\alpha.\, A]\!](F) \,\}\right)^{\perp\perp} \\ & = & \left(\bigcap \{\, F \in \mathcal{X} \mid [\![\lambda\alpha^\perp.\, A^\perp]\!](F) \subset F \,\}\right)^{\perp} \\ & = & ([\![\mu\beta^\perp.\, B^\perp]\!])^{\perp}. \end{array}$$

  where the second step is justified as in the proof of the proposition below. □

**Proposition 6.8** *$[\![\mu\alpha.\, A]\!]$ and $[\![\nu\alpha.\, A]\!]$ are fixed points of $\lambda\alpha.\, A$.*

**Proof.** By Lemma 6.7, the function $[\![\lambda\alpha.\, A]\!]$ is monotone increasing for $A$ positive in $\alpha$. Thus, the property of being a pre-fixed point of $\lambda\alpha.\, A$ is preserved by intersections, so the interpretation of $\mu\alpha.\, A$ is the least pre-fixed point of $\lambda\alpha.\, A$. As for $\nu$-formulas, $F$ is a post-fixed point of $\lambda\alpha.\, A$ iff

$$F \subset [\![\lambda\alpha.\, A]\!](F).$$

Since negation is monotone decreasing, this is true iff

$$\left([\![\lambda\alpha.\, A]\!](F)\right)^{\perp} \subset F^{\perp}.$$

But using the definition of $[\![\lambda\alpha.\, A]\!]$, we can rewrite this as

$$[\![\lambda\alpha^{\perp}.\, A^{\perp}]\!](F^{\perp}) \subset F^{\perp},$$

which means that $F^{\perp}$ is a pre-fixed point of $\lambda\alpha^{\perp}.\, A^{\perp}$. Thus, the interpretation of a $\nu$-formula is the greatest post-fixed point of the corresponding context by duality.

Now suppose $F$ is the least pre-fixed point of $\lambda\alpha.\, A$. By monotonicity, $[\![\lambda\alpha.\, A]\!](F)$ is also a pre-fixed point of $\lambda\alpha.\, A$; and if it were strictly smaller than $F$, that would contradict minimality of $F$, so it must be equal to $F$ and $F$ is a fixed point. Similarly the greatest post-fixed point must be a fixed point to avoid contradicting maximality. □

**Corollary 6.9** $[\![\nu\alpha.\, A]\!] = \bigcup \{\, F \in \mathcal{X} \mid F \subset [\![\lambda\alpha.\, A]\!](F) \,\}$*; that is, the double negation in the definition was redundant.*

**Proof.** Since $[\![\nu\alpha.\, A]\!]$ is a fixed point of $\lambda\alpha.\, A$, it occurs in the set on the right-hand side and the union is already a fact. □

## 6.4 Deductive System

A deductive system for fixpoint linear logic ($\mathrm{LL}_\mu$) can be constructed by using Kozen's axiomatization. The rules (in the case of a single dual pair of modalities) are:

$$\frac{}{\vdash A, A^\perp}\,\mathrm{Id} \qquad \frac{\vdash \Gamma, A \quad \vdash A^\perp, \Delta}{\vdash \Gamma, \Delta}\,\mathrm{Cut} \qquad \frac{\vdash \Gamma}{\vdash \sigma(\Gamma)}\,\mathrm{Ex}$$

$$\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B}\,\& \qquad \frac{}{\vdash \Gamma, \top}\,\top \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\,\oplus_1 \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\,\oplus_2$$

$$\frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\,\otimes \qquad \frac{}{\vdash \mathbf{1}}\,\mathbf{1} \qquad \frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\,\parr \qquad \frac{\vdash \Gamma}{\vdash \Gamma, \bot}\,\bot$$

$$\frac{\vdash \Gamma, A}{\vdash \Diamond\Gamma, \Box A}\,\Box \qquad \frac{\vdash \Gamma, A[\mu\alpha.\,A/\alpha]}{\vdash \Gamma, \mu\alpha.\,A}\,\mu \qquad \frac{\vdash B^\perp, A[B/\alpha]}{\vdash B^\perp, \nu\alpha.\,A}\,\nu$$

We can verify soundness at once using a straightforward lemma.

**Lemma 6.10** $[\![A[B/\alpha]]\!]_{\mathcal{M}} = [\![\lambda\alpha.\,A]\!]_{\mathcal{M}}([\![B]\!]_{\mathcal{M}})$.

**Proof.** The result follows by an easy induction on $A$. □

**Proposition 6.11 (Soundness)** *The sequent calculus above is sound for the semantics of the previous section.*

**Proof.** Soundness of the LL proof rules is the same as in LL, except for Cut and Identity; it must be shown that $[\![A^\perp]\!] = [\![A]\!]^\perp$. This is proved by induction on $A$, with the only case differing from K-modal LL being fixpoint formulas, for which a proof was given in the proof of Lemma 6.7. Soundness of the $\mu$-rule now follows from the fact that $\mu\alpha.\,A$ is a (pre-)fixed point of $\lambda\alpha.\,A$, and soundness of the $\nu$-rule from the fact that $\nu\alpha.\,A$ is the *greatest* post-fixed point of $\lambda\alpha.\,A$, using Lemma 6.10. □

**Corollary 6.12** *$LL_\mu$ is conservative over MALL.*

**Proof.** Any MALL sequent provable in $\mathrm{LL}_\mu$ sequent calculus is valid in phase spaces by soundness, since the interpretation of MALL connectives is unchanged; then it is provable in MALL sequent calculus by completeness of that deductive system. □

Completeness of $\mathrm{LL}_\mu$ sequent calculus is more difficult, and remains an open question.

The usual syntactic results, the substitution theorem and cut-elimination, fail to hold for this sequent calculus. However, we can try to recover certain special cases, thus localizing the failure.

**Definition 6.13** *An occurrence of a literal $\alpha$ in a formula $A$ is said to have (fixpoint) depth $d$ if it is in the scope of $d$ fixpoint quantifiers.*

**Proposition 6.14 (Substitution)** *The following is a derivable rule in $LL_\mu$ with the Identity rule restricted to atomic and fixpoint formulas:*

$$\frac{\vdash A_1^\perp, A_1' \quad \vdash A_2^\perp, A_2' \quad \cdots \quad \vdash A_n^\perp, A_n'}{\vdash B^\perp[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n], B[A_1'/\alpha_1, A_2'/\alpha_2, \ldots, A_n'/\alpha_n]}\,\mathrm{ST} \quad (B \textit{ positive in } \alpha_i),$$

**Proof.** We consider the derived rules from the proof for **K**-modal linear logic with one additional rule $\mathrm{ST}_{\mu,\nu}$:

$$\cfrac{\cfrac{\vdash A^\perp[\mu\alpha^\perp.\, A^\perp/\alpha^\perp], A'[\nu\alpha.\, A/\alpha]}{\vdash \mu\alpha^\perp.\, A^\perp, A'[\nu\alpha.\, A/\alpha]}\,\mu}{\vdash \mu\alpha^\perp.\, A^\perp, \nu\alpha.\, A'}\,\nu$$

The proof is by induction on the maximum depth of occurrences of $\alpha_i$ in $B$, and the size of $B$. The base case is when $B$ is a literal, or a fixpoint formula where the maximum depth is zero; then either $B = \alpha_i$ for some $i$, and the conclusion matches one of the premises, or none of the $\alpha_i$ or $\alpha_i^\perp$ occur in $B$ and the restricted Identity rule applies. The induction cases from the proofs of Theorem 2.10 and Proposition 5.3 do not increase the maximum fixpoint depth, so they apply here as well. The remaining case is when $B$ is a fixpoint formula, such as $B = \nu\alpha.\, B'$ (the other case is similar); but then the derived rule $\mathrm{ST}_{\mu,\nu}$ derives the given instance of ST from an instance of ST with lower maximum fixpoint depth:

$$\cfrac{\cfrac{\vdash A_1^\perp, A_1' \quad \vdash A_2^\perp, A_2' \quad \cdots \quad \vdash A_n^\perp, A_n'}{\vdash B''^\perp[C/\alpha][A_1/\alpha_1', A_2/\alpha_2', \ldots, A_n/\alpha_n'], B''[C/\alpha][A_1'/\alpha_1', A_2'/\alpha_2', \ldots, A_n'/\alpha_n']}\,\mathrm{ST}}{\vdash \mu\alpha^\perp.\, B'^\perp[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n], \nu\alpha.\, B'[A_1'/\alpha_1, A_2'/\alpha_2, \ldots, A_n'/\alpha_n]}\,\mathrm{ST}_{\mu,\nu}$$

where $C = \nu\alpha.\, B'[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n]$, $B'' = B'[a_i'/\alpha_i]$, and the $a_i'$ are distinct atoms not occurring in $C$. □

When the proof of Proposition 6.14 is applied with $n = 0$ and $B = \nu\alpha.B'$, the resulting derivation is the Identity rule on $B$. We could instead try to use the induction case, and we would get the following result:

$$\dfrac{\dfrac{\dfrac{}{\vdash B'^{\perp}[\mu\alpha^{\perp}.B'^{\perp}/\alpha^{\perp}], B'[\nu\alpha.B'/\alpha]}\,\mathrm{Id}}{\vdash \mu\alpha^{\perp}.B'^{\perp}, B'[\nu\alpha.B'/\alpha]}\,\mu}{\vdash \mu\alpha^{\perp}.B'^{\perp}, \nu\alpha.B'}\,\nu$$

Reducing this identity rule to identity rules on atoms and fixpoint formulas will, in general, produce copies of the identity rule on $B$. So we obtain a nonterminating recursive expansion for the Identity rule on fixpoint formulas.

## 6.5 Partial Cut-Elimination

A rewrite system can be defined which transforms proofs in fixpoint LL sequent calculus using the Cut rule, in such a way that at least some instances of that rule can be eliminated.

Since there is an alternate sequent formulation of the mu-calculus that supports cut-elimination [1], it would perhaps be a better idea to adapt that system to linear logic and attempt to prove a (full) cut-elimination theorem. However, the author became aware of this work only after the results of this section had been developed. We are not aware of any work extending the work in [1] to linear logic. The question of partial cut-elimination with Kozen's axiomatization may still be of some interest, particularly for its connection to $\mathrm{LL}_{\mathrm{FS}}$, although less so for the purpose of obtaining a proof theory of fixpoint linear logic.

As in the LL case where the extended rule Cut! was used, the rewrite system here requires an extension of the deductive system with derived rules. In this case the ST rule justified by the Substitution Theorem is used.

While it would be simpler to use the $\mathrm{ST}_*$ rules from the proof of the substitution theorem, this causes problems because the $\mathrm{ST}_{\mu,\nu}$ rule is not an instance of ST. A cut of ST against $\mu$ or $\nu$ can be eliminated very cleanly, while a cut of $\mathrm{ST}_{\mu,\nu}$ against a fixpoint rule cannot. So we must work with ST itself and we will need a lemma to deal with cuts of ST against ST. First we make some definitions.

**Definition 6.15** *A substitution is a function* $\sigma : \mathrm{Atoms} \to \Phi$ *where* $\Phi$ *is the set of all formulas.*

*The support of a substitution* $\sigma$ *is*

$$\mathrm{supp}(\sigma) := \{\, a \in \mathrm{Atoms} \mid \sigma(a) \neq a \,\}.$$

*Substitutions will be assumed to have finite support; this assumption is made, among other reasons, to ensure that alpha-conversion can be used where needed.*

*The application of a substitution* $\sigma$ *to a formula* $A$*, denoted* $A[\sigma]$*, is defined by* $a[\sigma] = \sigma(a)$*,* $a^\perp[\sigma] = (\sigma(a))^\perp$*, and distributivity over all the connectives; in the case of fixpoint quantifiers, this distributivity is of the form* $\mu\alpha.\, A[\sigma] = \mu\alpha.(A[\sigma])$ *where it is assumed by alpha-conversion that* $\alpha$ *does not occur in either* $\mathrm{supp}(\sigma)$ *or* $A[\sigma]$*.*

*We say* $\sigma$ *is a substitution from* $A$ *to* $B$*, denoted* $A \xrightarrow{\sigma} B$ *or* $\sigma : A \longrightarrow B$*, if* $\mathrm{supp}(\sigma) \subset \mathrm{FA}(A)$ *and* $A[\sigma] = B$*. We say* $\sigma$ *is a positive substitution from* $A$ *to* $B$*, denoted* $A \xrightarrow[+]{\sigma} B$ *or* $\sigma : A \xrightarrow[+]{} B$*, if it is a substitution from* $A$ *to* $B$ *and* $A$ *is positive in the atoms of* $\mathrm{supp}(\sigma)$*.*

It is easily checked that a substitution from $A$ to $B$ is unique if it exists. Thus the category **Sub** with formulas (up to alpha-conversion) as objects and substitutions from $A$ to $B$ as $\mathrm{Hom}(A, B)$ is a poset. Similarly there is a poset category **Sub**$^+$ with formulas as objects and positive substitutions from one formula to another as morphisms.

The notation $A/a$ will sometimes be used to write substitutions explicitly, or $\sigma, A/a$ to modify $\sigma$ at one point $a$ (normally one not already in the support of $\sigma$). Substitutions on negative literals are defined by $A^\perp/a^\perp = A/a$.

A form of alpha-conversion applies to the ST rule. This is based on the fact that in the usual presentation of this rule,

$$\frac{\vdash A_1^\perp, A_1' \quad \vdash A_2^\perp, A_2' \quad \cdots \quad \vdash A_n^\perp, A_n'}{\vdash B^\perp[A_1/\alpha_1, A_2/\alpha_2, \ldots, A_n/\alpha_n], B[A_1'/\alpha_1, A_2'/\alpha_2, \ldots, A_n'/\alpha_n]}\,\mathrm{ST},$$

the formula $B$ and literals $\alpha_i$ are not uniquely determined by the premises and the conclusion. Specifically, a literal $\alpha_i$ can be replaced with another literal $\beta$ which does not occur in $B$, and $B$ replaced with $B[\beta/\alpha_i]$, while preserving correctness of the rule. We adopt the same conventions as for alpha-conversion of formulas: ST rules are defined up to this notion of alpha-conversion, and representatives are chosen using Barendregt's convention.

An instance of the ST rule may be written in the form

$$\frac{\cdots \quad \vdash \sigma(a_i)^\perp, \tau(a_i) \quad \cdots}{\vdash A^\perp[\sigma], A[\tau]}\,\mathrm{ST}$$

where $A \xrightarrow[+]{\sigma} A[\sigma]$ and $A \xrightarrow[+]{\tau} A[\tau]$, and $a_i$ ranges over $\mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau)$. Alpha-conversion is needed to ensure that the literals for which formulas are substituted are positive; and alpha-conversion (on the atoms in $\mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau)$) continues to apply to this modified version of the rule. We may assume that $A$ is not a literal, since we could otherwise replace the ST rule with one of its premises or an Identity rule on atoms as in the base case of the Substitution Theorem.

**Lemma 6.16** *Given substitutions* $\sigma_1 : A_1 \xrightarrow[+]{} B$ *and* $\sigma_2 : A_2 \xrightarrow[+]{} B$*, there exist a formula* $C$ *and substitutions* $\tau_1 : C \xrightarrow[+]{} A_1$ *and* $\tau_2 : C \xrightarrow[+]{} A_2$ *such that* $\sigma_1 \circ \tau_1 = \sigma_2 \circ \tau_2$*, and for every atom* $a$*, at least one of* $\tau_1(a)$ *and* $\tau_2(a)$ *is an atom.*

**Proof.** The proof is by induction on $A_1$ and $A_2$. We prove a slightly different statement: We drop the requirement $\sigma_1 \circ \tau_1 = \sigma_2 \circ \tau_2$ because it is trivial in a poset category (although it will be useful later), and we prove that $C$, $\tau_1$, and $\tau_2$ can be chosen in such a way that $\mathrm{supp}(\tau_1) \cup \mathrm{supp}(\tau_2) \in S$ for an arbitrary set $S \subset \mathrm{Atoms}$ that is neither finite nor cofinite (in Atoms) and that does not include any atom occurring in one of the given formulas.

We consider cases for $A_1$ and $A_2$.

- If at least one is a literal, say $A_1 = \alpha$, then we take $C = a$ if $\alpha$ is positive, $a^\perp$ otherwise, for arbitrary $a \in S$. We set $\tau_1 = A_1/C$ and $\tau_2 = A_2/C$. $\tau_1(a)$ is $\alpha$ or $\alpha^\perp$, whichever is an atom, and $\tau_1(b) = b$ for any other atom $b$.

- If $A_1$ and $A_2$ have differing principal connectives, we obtain a contradiction from $A_1[\sigma_1] = A_2[\sigma_2]$.

- If $A_1$ and $A_2$ have a principal connective that is not a fixpoint operator, all of the cases are similar so we consider only $\otimes$. We have $A_1 = A_{1,1} \otimes A_{1,2}$ and $A_2 = A_{2,1} \otimes A_{2,2}$, and by the definition of substitution we also have $B = B_1 \otimes B_2$ and $\sigma_i : A_{i,j} \xrightarrow[+]{} B_j$ for $i, j \in \{1, 2\}$. By the induction hypothesis there exist formulas $C_i$ and substitutions $\tau_{1,i} : C_i \xrightarrow[+]{} A_{1,i}$ and $\tau_{2,i} : C_i \xrightarrow[+]{} A_{2,i}$ for $i \in \{1, 2\}$, with $\mathrm{supp}(\tau_{j,1}) \subset S_1$ and $\mathrm{supp}(\tau_{j,2}) \subset S_2$ for $j \in \{1, 2\}$ where $S_1$ and $S_2$ are disjoint infinite subsets of $S$. Now we take $C = C_1 \otimes C_2$ and $\tau_i = \tau_{i,1} \circ \tau_{i,2}$ for $i \in \{1, 2\}$. That we have $\tau_i : C \xrightarrow[+]{} A_i$ as a consequence of the disjointness of $S_1$ and $S_2$ and the fact that those sets do not include any atom occurring in one of the given formulas (we use here the fact that substitutions with disjoint support commute). Finally, the condition on $\tau_1(a)$ and $\tau_2(a)$ follows from the induction hypothesis since the supports of $\tau_{1,i}$ and $\tau_{2,i}$ are disjoint for $i \in \{1, 2\}$.

- If $A_1$ and $A_2$ have a fixpoint principal connective, we may apply the same reasoning as above if we choose the quantified literal according to Barendregt's convention. □

This lemma can be modified to construct $C$ in such a way that $C$ is a substitution instance of any other formula $C'$ that satisfies the stated properties (with its own substitutions $\tau_1'$ and $\tau_2'$) excluding the condition on atoms. From a category-theoretic point of view, this means that the category $\mathbf{Sub}^+$ has *pullbacks*. The same result can be proven for the category **Sub**. These results, however, will not be needed: the condition on atoms is what we will use, not the universal property of pullbacks.

**Definition 6.17** *The partial cut-elimination rewrite system consists of the MALL cut-elimination rewrite system together with the following rewrite rules for the modal and fixpoint connectives:*

$$\dfrac{\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, A}}{\vdash \Diamond\Gamma, \Box A}{\scriptstyle\Box\Diamond} \qquad \dfrac{{}^{\pi_2}\overline{\vdash A^\perp, \Delta, B}}{\vdash \Diamond A^\perp, \Diamond\Delta, \Box B}{\scriptstyle\Box\Diamond}}{\vdash \Diamond\Gamma, \Diamond\Delta, \Box B}{\scriptstyle\mathrm{Cut}} \quad\Longrightarrow\quad \dfrac{\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, A} \qquad {}^{\pi_2}\overline{\vdash A^\perp, \Delta, B}}{\vdash \Gamma, \Delta, B}{\scriptstyle\mathrm{Cut}}}{\vdash \Diamond\Gamma, \Diamond\Delta, \Box B}{\scriptstyle\Box\Diamond}$$

$$\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, B} \qquad \dfrac{{}^{\pi_2}\overline{\vdash B^\perp, A[\mu\alpha.\, A/\alpha]}}{\vdash B^\perp, \mu\alpha.\, A}{\scriptstyle\mu}}{\vdash \Gamma, \mu\alpha.\, A}{\scriptstyle\mathrm{Cut}} \quad\Longrightarrow\quad \dfrac{\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, B} \qquad {}^{\pi_2}\overline{\vdash B^\perp, A[\mu\alpha.\, A/\alpha]}}{\vdash \Gamma, A[\mu\alpha.\, A/\alpha]}{\scriptstyle\mathrm{Cut}}}{\vdash \Gamma, \mu\alpha.\, A}{\scriptstyle\mu}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A[\mu\alpha.\,A/\alpha]}}{\vdash \Gamma, \mu\alpha.\,A}\,\mu \qquad \dfrac{\dfrac{\pi_2}{\vdash A^\perp[B^\perp/\alpha^\perp], B}}{\vdash \nu\alpha^\perp.\,A^\perp, B}\,\nu}{\vdash \Gamma, B}\,\text{Cut}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A[\mu\alpha.\,A/\alpha]} \quad \dfrac{\dfrac{\dfrac{\pi_2}{\vdash A^\perp[B^\perp/\alpha^\perp], B}}{\vdash \nu\alpha^\perp.\,A^\perp, B}\,\nu}{\vdash A^\perp[\nu\alpha^\perp.\,A^\perp/\alpha^\perp], A[B/\alpha]}\,\text{ST}}{\vdash \Gamma, A[B/\alpha]}\,\text{Cut} \qquad \dfrac{\pi_2}{\vdash A^\perp[B^\perp/\alpha^\perp], B}}{\vdash \Gamma, B}\,\text{Cut}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A[\sigma]} \quad \dfrac{\pi_2}{\vdash \Delta, B[\sigma]}}{\vdash \Gamma, \Delta, A \otimes B[\sigma]}\,\otimes \qquad \dfrac{\cdots \quad \vdash \sigma(a_i)^\perp, \tau(a_i) \quad \cdots}{\vdash A^\perp \parr B^\perp[\sigma], A \otimes B[\tau]}\,\text{ST}}{\vdash \Gamma, \Delta, A \otimes B[\tau]}\,\text{Cut}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A[\sigma]} \quad \dfrac{\cdots \quad \vdash \sigma(a_i)^\perp, \tau(a_i) \quad \cdots}{\vdash A^\perp[\sigma], A[\tau]}\,\text{ST}}{\vdash \Gamma, A[\tau]}\,\text{Cut} \qquad \dfrac{\dfrac{\pi_2}{\vdash \Delta, B[\sigma]} \quad \dfrac{\cdots \quad \vdash \sigma(a_i)^\perp, \tau(a_i) \quad \cdots}{\vdash B^\perp[\sigma], B[\tau]}\,\text{ST}}{\vdash \Delta, B[\tau]}\,\text{Cut}}{\vdash \Gamma, \Delta, A \otimes B[\tau]}\,\otimes$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A[\sigma, \mu\alpha.\,A[\sigma]/\alpha]}}{\vdash \Gamma, \mu\alpha.\,A[\sigma]}\,\mu \qquad \dfrac{\cdots \quad \vdash \sigma(a_i)^\perp, \tau(a_i) \quad \cdots}{\vdash \nu\alpha.\,A^\perp[\sigma], \mu\alpha.\,A[\tau]}\,\text{ST}}{\vdash \Gamma, \mu\alpha.\,A[\tau]}\,\text{Cut}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash \Gamma, A[\sigma, \mu\alpha.\,A[\sigma]/\alpha]} \quad \dfrac{\cdots \quad \vdash \sigma(a_i)^\perp, \tau(a_i) \quad \cdots}{\vdash A^\perp[\nu\alpha.\,A^\perp/\alpha^\perp][\sigma], A[\mu\alpha.\,A/\alpha][\tau]}\,\text{ST}}{\vdash \Gamma, A[\mu\alpha.\,A/\alpha][\tau]}\,\text{Cut}}{\vdash \Gamma, \mu\alpha.\,A[\tau]}\,\mu$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash B^\perp, A[\sigma, B/\alpha]}}{\vdash B^\perp, \nu\alpha.\, A[\sigma]}\,\nu \qquad \dfrac{\cdots \quad \vdash \sigma(a_i)^\perp, \tau(a_i) \quad \cdots}{\vdash \mu\alpha.\, A^\perp[\sigma], \nu\alpha.\, A[\tau]}\,\mathrm{ST}}{\vdash B^\perp, \nu\alpha.\, A[\tau]}\,\mathrm{Cut}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\vdash B^\perp, A[\sigma, B/\alpha]} \qquad \dfrac{\cdots \quad \vdash \sigma(a_i)^\perp, \tau(a_i) \quad \cdots}{\vdash A^\perp[B^\perp/\alpha^\perp][\sigma], A[B/\alpha][\tau]}\,\mathrm{ST}}{\vdash B^\perp, A[\tau, B/\alpha]}\,\mathrm{Cut}}{\vdash B^\perp, \nu\alpha.\, A[\tau]}\,\nu$$

*In the latter two cases, $\alpha$ is chosen according to Barendregt's convention. The correctness of the reducts requires rewriting substituted formulas to bring certain substitutions to the outside, which is justified by the choice of $\alpha$. In the final case, the atoms in the support of $\sigma$ and $\tau$ are also chosen according to Barendregt's convention, using alpha-conversion on* ST *rules.*

*The rules for cuts of principal formulas of* ST *against the other MALL connectives are similar to the case for $\otimes$ and are not shown.*

*We also define a cut-elimination rewrite rule to apply to the following proof:*

$$\dfrac{\dfrac{\cdots \quad \vdash \sigma_1(a_i)^\perp, \sigma_2(a_i) \quad \cdots}{\vdash A^\perp[\sigma_1], A[\sigma_2]}\,\mathrm{ST} \qquad \dfrac{\cdots \quad \vdash \tau_1(b_i)^\perp, \tau_2(b_i) \quad \cdots}{\vdash B^\perp[\tau_1], B[\tau_2]}\,\mathrm{ST}}{\vdash A^\perp[\sigma_1], B[\tau_2]}\,\mathrm{Cut}$$

*Since $A[\sigma_2] = B[\tau_1]$ from correctness of the* Cut *rule, by Lemma 6.16, we let $C$ be a formula and $\rho_1 : C \xrightarrow[+]{} A$ and $\rho_2 : C \xrightarrow[+]{} B$ be substitutions such that $\sigma_2 \circ \rho_1 = \tau_1 \circ \rho_2$, and such that at least one of $\rho_1(a)$ and $\rho_2(a)$ is an atom for any atom $a$.*

*Now we write the reduct as*

$$\dfrac{\cdots}{\vdash C^\perp[\sigma_1 \circ \rho_1], C[\tau_2 \circ \rho_2]}\,\mathrm{ST}$$

*but we must fill in the premises. For each atom $a$ occurring in $C$, (at least) one of $\rho_1(a)$ or $\rho_2(a)$ is atomic; we assume it is the former, the other case being similar. Then let $b = \rho_1(a)$ and $D = \rho_2(a)$. We must include the premise $\vdash b^\perp[\sigma_1], D[\tau_2]$. This premise is proved by*

$$\dfrac{\vdash b^\perp[\sigma_1], b[\sigma_2] \qquad \dfrac{\cdots}{\vdash D^\perp[\tau_1], D[\tau_2]}\,\mathrm{ST}}{\vdash b^\perp[\sigma_1], D[\tau_2]}\,\mathrm{Cut}$$

*where* $b[\sigma_2] = a[\sigma_2 \circ \rho_1] = a[\tau_1 \circ \rho_2] = D[\tau_1]$ *as required. Finally, the first premise of the* Cut *rule was one of the original premises, and the premises required for the* ST *rule are a subset of the original premises as* $D$ *is a subformula of* $B$.

The reduction for ST is rather complicated, but it does achieve its purpose: the Cut on ST and ST is reduced to cuts that, *a priori*, have ST rules on only *one* side; and in the process, no new rules other than Cut and ST are introduced.

Rewriting of ST rules has the effect of performing substitutions in proofs, which preserves validity until an Identity rule is reached at which point the substituted sequent must be proved using one of the premises of the ST rule.

**Proposition 6.18** *A normal form for the partial cut-elimination rewrite system can be translated into a cut-free proof in* $LLSC'_\mu$*, which is* $LLSC_\mu$ *with the* $\nu$ *rule replaced with the rule*

$$\frac{\vdash \Gamma, B \quad \vdash B^\perp, A[B/\alpha]}{\vdash \Gamma, \nu\alpha.\, A}\,\nu'.$$

*(Since the means of translation is not specified, this proposition is actually only about provability.)*

**Proof.** We consider the following additional rewrite rule:

$$\dfrac{{}^{\pi_1}\overline{\vdash \Gamma, B} \qquad \dfrac{{}^{\pi_2}\overline{\vdash B^\perp, A[B/\alpha]}}{B^\perp, \nu\alpha.\, A}\,\nu}{\vdash \Gamma, \nu\alpha.\, A}\,\mathrm{Cut} \quad \Longrightarrow \quad \dfrac{{}^{\pi_1}\overline{\vdash \Gamma, B} \qquad {}^{\pi_2}\overline{\vdash B^\perp, A[B/\alpha]}}{\vdash \Gamma, \nu\alpha.\, A}\,\nu'$$

It can be checked that a normal form for the rewrite system including this additional rule does not use the Cut rule. (There are many cases but the general principle is the same as for LLSC: reductions for non-principal formulas and for principal formulas.) This rule does not introduce additional redexes, so it can clearly be used to obtain a normal form for the extended rewrite system from a normal form for the original one. Instances of the ST rule can be eliminated by the Substitution Theorem, leaving a cut-free proof in $\mathrm{LLSC}'_\mu$. □

In particular, a cut-free proof in $\mathrm{LLSC}'_\mu$ of a sequent not containing any positive occurrence of $\nu$ is a cut-free proof in $\mathrm{LLSC}_\mu$, and thus satisfies the subformula property.

It remains to determine whether or not the rewrite system is weakly normalizing. This is currently an open question. We consider next some possible ways to simplify the problem and apply it to the more familiar setting of linear logic with exponentials, whether with free storage or usual storage.

## 6.6 Free Storage in Fixpoint Linear Logic

We now return to the Free Storage rule considered in Section 2.8, and consider how it can be translated into $\mathrm{LL}_\mu$ (in fact, into the fragment of $\mathrm{LL}_\mu$ without the modal connectives).

**Definition 6.19** *The translation $\overline{A}$ of a linear logic formula $A$ is the fixpoint linear logic formula defined inductively by preservation of literals,*

$$\begin{array}{rcl} \overline{!A} & := & \nu\alpha.\, \mathbf{1} \,\&\, \overline{A} \,\&\, (\alpha \otimes \alpha), \\ \overline{?A} & := & \mu\alpha.\, \bot \oplus \overline{A} \oplus (\alpha \parr \alpha), \end{array}$$

*and distributivity over the other connectives. The atom $\alpha$ is chosen not to occur in $A$.*

**Proposition 6.20** *The translation defined above is a sound translation of $LL_{FS}$ into $LL_\mu$, that is, it preserves provability.*

**Proof.** We must derive the Weakening, Contraction, Dereliction, and Free Storage rules for the translated exponentials. Indeed, the derivations follow:

$$\text{W:}\quad \dfrac{\dfrac{\dfrac{\vdash \Gamma}{\vdash \Gamma, \bot}\,\bot}{\Gamma, \bot \oplus \overline{A} \oplus (\overline{?A} \parr \overline{?A})}\,\oplus^{*}}{\vdash \Gamma, \overline{?A}}\,\mu \qquad\qquad \text{D:}\quad \dfrac{\dfrac{\vdash \Gamma, \overline{A}}{\Gamma, \bot \oplus \overline{A} \oplus (\overline{?A} \parr \overline{?A})}\,\oplus^{*}}{\vdash \Gamma, \overline{?A}}\,\mu$$

$$\text{C:}\quad \dfrac{\dfrac{\dfrac{\vdash \Gamma, \overline{?A}, \overline{?A}}{\vdash \Gamma, \overline{?A} \parr \overline{?A}}\,\parr}{\Gamma, \bot \oplus \overline{A} \oplus (\overline{?A} \parr \overline{?A})}\,\oplus^{*}}{\vdash \Gamma, \overline{?A}}\,\mu \qquad\qquad \text{FS:}\quad \dfrac{\dfrac{B \vdash \mathbf{1} \quad B \vdash \overline{A} \quad B \vdash B \otimes B}{B \vdash \mathbf{1} \,\&\, \overline{A} \,\&\, (B \otimes B)}\,\&_{\mathrm{R}}^{*}}{B \vdash \overline{!A}}\,\nu_{\mathrm{R}}$$

□

We now consider partial cut-elimination, and attempt to define an induced rewrite system on proofs in LLSC$_{\mathrm{FS}}$. For a cut against the side formula of a Free Storage rule, no rewrite rule will apply: this corresponds to the case of a cut against the side formula of a $\nu$ rule. The non-principal formula rewrite rules for Weakening, Dereliction, and Contraction are the obvious ones (the same as in usual LLSC). The case of a cut of the principal formula of one of these rules against the principal formula of Free Storage is the remaining one.

**Proposition 6.21** *Each of the following rewrite rules corresponds, under the translation, to a sequence of rewrite steps in the partial cut-elimination rewrite system:*

$$\dfrac{\dfrac{\dfrac{\pi_1}{B\vdash\mathbf{1}}\quad\dfrac{\pi_2}{B\vdash B\otimes B}\quad\dfrac{\pi_3}{B\vdash A}}{B\vdash !A}\,\mathrm{FS}\qquad\dfrac{\dfrac{\pi_4}{\vdash\Gamma}}{!A\vdash\Gamma}\,\mathrm{W}}{B\vdash\Gamma}\,\mathrm{Cut}\quad\Longrightarrow\quad\dfrac{\dfrac{\pi_1}{B\vdash\mathbf{1}}\quad\dfrac{\dfrac{\pi_4}{\vdash\Gamma}}{\mathbf{1}\vdash\Gamma}\,\mathbf{1}_{\mathrm{L}}}{B\vdash\Gamma}\,\mathrm{Cut}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{B\vdash\mathbf{1}}\quad\dfrac{\pi_2}{B\vdash B\otimes B}\quad\dfrac{\pi_3}{B\vdash A}}{B\vdash !A}\,\mathrm{FS}\qquad\dfrac{\dfrac{\pi_4}{A\vdash\Gamma}}{!A\vdash\Gamma}\,\mathrm{D}}{B\vdash\Gamma}\,\mathrm{Cut}\quad\Longrightarrow\quad\dfrac{\dfrac{\pi_3}{B\vdash A}\quad\dfrac{\pi_4}{A\vdash\Gamma}}{B\vdash\Gamma}\,\mathrm{Cut}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{B\vdash\mathbf{1}}\quad\dfrac{\pi_2}{B\vdash B\otimes B}\quad\dfrac{\pi_3}{B\vdash A}}{B\vdash !A}\,\mathrm{FS}\qquad\dfrac{\dfrac{\pi_4}{!A,!A\vdash\Gamma}}{!A\vdash\Gamma}\,\mathrm{C}}{B\vdash\Gamma}\,\mathrm{Cut}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\pi_2}{B\vdash B\otimes B}\qquad\dfrac{\dfrac{\dfrac{\dfrac{\pi_1}{B\vdash\mathbf{1}}\quad\dfrac{\pi_2}{B\vdash B\otimes B}\quad\dfrac{\pi_3}{B\vdash A}}{B\vdash !A}\,\mathrm{FS}\qquad\dfrac{\dfrac{\dfrac{\pi_1}{B\vdash\mathbf{1}}\quad\dfrac{\pi_2}{B\vdash B\otimes B}\quad\dfrac{\pi_3}{B\vdash A}}{B\vdash !A}\,\mathrm{FS}\quad\dfrac{\pi_4}{!A,!A\vdash\Gamma}}{B,!A\vdash\Gamma}\,\mathrm{Cut}}{B,B\vdash\Gamma}\,\mathrm{Cut}}{B\otimes B\vdash\Gamma}\,\otimes_{\mathrm{L}}}{B\vdash\Gamma}\,\mathrm{Cut}$$

**Proof.** The rewrite sequences are rather long; we present the steps for the Contraction case only. We also abbreviate $\mathbf{1}\,\&\,\overline{A}\,\&\,(C\otimes C)$ as $F(C)$ for formulas $C$.

$$\dfrac{\dfrac{\dfrac{\overline{B}\vdash\mathbf{1}\quad\overline{B}\vdash\overline{A}\quad\overline{B}\vdash\overline{B}\otimes\overline{B}}{\overline{B}\vdash\mathbf{1}\,\&\,\overline{A}\,\&\,(\overline{B}\otimes\overline{B})}\,\&^{\bullet}_{\mathrm{R}}}{\overline{B}\vdash\overline{!A}}\,\nu\qquad\dfrac{\dfrac{\dfrac{\overline{!A},\overline{!A}\vdash\overline{\Gamma}}{\overline{!A}\otimes\overline{!A}\vdash\overline{\Gamma}}\,\otimes_{\mathrm{L}}}{\mathbf{1}\,\&\,\overline{A}\,\&\,(\overline{!A}\otimes\overline{!A})\vdash\overline{\Gamma}}\,\&^{\bullet}_{\mathrm{L}}}{\overline{!A}\vdash\overline{\Gamma}}\,\mu}{\overline{B}\vdash\overline{\Gamma}}\,\mathrm{Cut}$$

$$\downarrow$$

$$\dfrac{\dfrac{\overline{B}\vdash\mathbf{1}\quad\overline{B}\vdash\overline{A}\quad\overline{B}\vdash\overline{B}\otimes\overline{B}}{\overline{B}\vdash F(\overline{B})}\,\&^{\bullet}_{\mathrm{R}}\qquad\dfrac{\dfrac{\dfrac{\dfrac{\overline{B}\vdash\mathbf{1}\quad\overline{B}\vdash\overline{A}\quad\overline{B}\vdash\overline{B}\otimes\overline{B}}{\overline{B}\vdash F(\overline{B})}\,\&^{\bullet}_{\mathrm{R}}}{\overline{B}\vdash\overline{!A}}\,\nu}{F(\overline{B})\vdash F(\overline{!A})}\,\mathrm{ST}\qquad\dfrac{\dfrac{\overline{!A},\overline{!A}\vdash\overline{\Gamma}}{\overline{!A}\otimes\overline{!A}\vdash\overline{\Gamma}}\,\otimes_{\mathrm{L}}}{F(\overline{!A})\vdash\overline{\Gamma}}\,\&^{\bullet}_{\mathrm{L}}}{F(\overline{B})\vdash\overline{\Gamma}}\,\mathrm{Cut}}{\overline{B}\vdash\overline{\Gamma}}\,\mathrm{Cut}$$

$$\downarrow$$

$$\dfrac{\dfrac{\overline{B}\vdash\mathbf{1}\quad\overline{B}\vdash\overline{A}\quad\overline{B}\vdash\overline{B}\otimes\overline{B}}{\overline{B}\vdash F(\overline{B})}\,\&^{\bullet}_{\mathrm{R}}\qquad\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{B}\vdash\mathbf{1}\quad\overline{B}\vdash\overline{A}\quad\overline{B}\vdash\overline{B}\otimes\overline{B}}{\overline{B}\vdash F(\overline{B})}\,\&^{\bullet}_{\mathrm{R}}}{\overline{B}\vdash\overline{!A}}\,\nu}{\overline{B}\otimes\overline{B}\vdash\overline{!A}\otimes\overline{!A}}\,\mathrm{ST}\qquad\dfrac{\overline{!A},\overline{!A}\vdash\overline{\Gamma}}{\overline{!A}\otimes\overline{!A}\vdash\overline{\Gamma}}\,\otimes_{\mathrm{L}}}{\overline{B}\otimes\overline{B}\vdash\overline{\Gamma}}\,\mathrm{Cut}}{F(\overline{B})\vdash\overline{\Gamma}}\,\&^{\bullet}_{\mathrm{L}}}{\overline{B}\vdash\overline{\Gamma}}\,\mathrm{Cut}$$

$$\downarrow$$

$$\dfrac{\overline{B}\vdash\overline{B}\otimes\overline{B}\qquad\dfrac{\dfrac{\dfrac{\dfrac{\overline{B}\vdash\mathbf{1}\quad\overline{B}\vdash\overline{A}\quad\overline{B}\vdash\overline{B}\otimes\overline{B}}{\overline{B}\vdash F(\overline{B})}\,\&^{\bullet}_{\mathrm{R}}}{\overline{B}\vdash\overline{!A}}\,\nu}{\overline{B}\otimes\overline{B}\vdash\overline{!A}\otimes\overline{!A}}\,\mathrm{ST}\qquad\dfrac{\overline{!A},\overline{!A}\vdash\overline{\Gamma}}{\overline{!A}\otimes\overline{!A}\vdash\overline{\Gamma}}\,\otimes_{\mathrm{L}}}{\overline{B}\otimes\overline{B}\vdash\overline{\Gamma}}\,\mathrm{Cut}}{\overline{B}\vdash\overline{\Gamma}}\,\mathrm{Cut}$$

$$\downarrow$$

$$
\begin{prooftree}
\AxiomC{$\overline{B}\vdash\overline{B}\otimes\overline{B}$}
\AxiomC{$\overline{B}\vdash\mathbf{1}$}
\AxiomC{$\overline{B}\vdash\overline{A}$}
\AxiomC{$\overline{B}\vdash\overline{B}\otimes\overline{B}$}
\RightLabel{$\&^{\bullet}_{\mathrm{R}}$}
\TrinaryInfC{$\overline{B}\vdash\mathbf{1}\,\&\,\overline{A}\,\&\,(\overline{B}\otimes\overline{B})$}
\RightLabel{$\nu$}
\UnaryInfC{$\overline{B}\vdash\overline{!A}$}
\AxiomC{$\overline{B}\vdash\mathbf{1}$}
\AxiomC{$\overline{B}\vdash\overline{A}$}
\AxiomC{$\overline{B}\vdash\overline{B}\otimes\overline{B}$}
\RightLabel{$\&^{\bullet}_{\mathrm{R}}$}
\TrinaryInfC{$\overline{B}\vdash\mathbf{1}\,\&\,\overline{A}\,\&\,(\overline{B}\otimes\overline{B})$}
\RightLabel{$\nu$}
\UnaryInfC{$\overline{B}\vdash\overline{!A}$}
\AxiomC{$\overline{!A},\overline{!A}\vdash\overline{\Gamma}$}
\RightLabel{Cut}
\BinaryInfC{$\overline{B},\overline{!A}\vdash\overline{\Gamma}$}
\RightLabel{Cut}
\BinaryInfC{$\overline{B},\overline{B}\vdash\overline{\Gamma}$}
\doubleLine
\RightLabel{$\otimes_{\mathrm{L}}$}
\UnaryInfC{$\overline{B}\otimes\overline{B}\vdash\overline{\Gamma}$}
\RightLabel{Cut}
\BinaryInfC{$\overline{B}\vdash\overline{\Gamma}$}
\end{prooftree}
$$

□

Thus we have a partial cut-elimination rewrite system for LL sequent calculus with free storage. Since none of these rewrite rules introduce ST, we can do away with that rule and its added complexity. However, weak normalization even here remains an open problem.

We can go one step further in our translation, and consider what happens if we translate LLSC with the usual Storage rule into $\mathrm{LLSC}_{\mathrm{FS}}$ using the derivation of Storage given in Section 2.8. It turns out that the usual cut-elimination rewrite rules for LLSC, with the exception of the rewrite rule for non-principal formulas of Storage, correspond to multiple steps under this translation. Furthermore, since the cut-elimination rewrite system in LLSC, with certain restrictions, is strongly normalizing [26, 28], it remains weakly normalizing with the rewrite rule for non-principal formulas of Storage omitted. (This requires checking that the restrictions do not prevent reaching a normal form for the system without them. The usual restrictions prevent commuting one cut through another; to avoid problems, such cut-commutations must be allowed when the upper instance of Cut is one that will never be reduced. This can be done without seriously affecting the proof of strong normalization; we define the complexity of such a non-reducible cut to be zero.) So in this particular special case, we do have weak normalization for the partial cut-elimination rewrite rules.

The fact that full cut-elimination holds for LLSC depends on an essentially *modal* property of the usual linear exponentials: the fact that ! can be introduced only in a context consisting entirely of ? formulas. An alternate approach to cut-elimination may be possible by treating the exponentials not as modalities, but as fixpoints. For applications where 'completeness' for the informal semantics of Section 2.4 is important, this approach may be more appropriate than the usual linear logic approach for the reasons described in Section 2.8.

The fact that there is an alternate deductive system for modal mu-calculus that satisfies full cut-elimination [1] suggests that if that result can be transferred to fixpoint linear logic, perhaps an alternate deductive system for $\mathrm{LL_{FS}}$ can be found that also satisfies cut-elimination.

## 6.7 Open Questions

There remain some significant open questions in fixpoint linear logic.

**Conjecture 6.22 (Completeness)** *$LLSC_\mu$ is complete for the algebraic semantics.*

Completeness is an important property, but proving it is likely to be a difficult problem; indeed, completeness of Kozen's axiomatization in the classical case was eventually proved by Igor Walukiewicz [29], but not for more than a decade after the axiomatization was first proposed (see [4]). On the other hand, perhaps only minor changes to the proof for the classical case would be required.

**Conjecture 6.23 (Weak Normalization)** *The partial cut-elimination rewrite system is weakly normalizing.*

This property holds for the usual LLSC cut-elimination process, but the techniques used in that proof are insufficient to prove the result for fixpoint linear logic. The translation of cut-elimination rewrite rules for LLSC into rewrite sequences in $\mathrm{LLSC}_\mu$ provides some evidence that the rewrite system is formulated correctly (although the use of ST is not fully tested), but there is no *a priori* reason to believe that it is weakly normalizing.

This conjecture loses much of its significance due to [1].

**Conjecture 6.24** *$LLSC_\mu$ is conservative over the translation of $LLSC_{FS}$ into fixpoint formulas, and $LLSC_{FS}$ is conservative over LL excluding ! but not ?.*

This problem also remains open. The usual conservativity-by-cut-elimination argument fails for $\mathrm{LLSC}_\mu$ over $\mathrm{LLSC}_{\mathrm{FS}}$ even assuming weak normalization because the remaining cuts (or $\nu'$ rules) may use fixpoint formulas that are not the translations of linear logic formulas as their cut formulas.

On the other hand, conservativity for sequents not using $\nu$, over both $\mathrm{LL}_{\mathrm{FS}}$ and usual linear logic, would follow from weak normalization.

**Conjecture 6.25** *There are deductive systems for $LL_\mu$ and $LL_{FS}$ that admit cut-elimination theorems.*

It is hoped that the deductive system and proof of cut-elimination of Aldwinckle and Cockett for the classical modal mu-calculus [1] will transfer relatively easily to the linear case. Such a result would likely allow the conservativity results to be established easily, and may be useful in proving completeness and even in deciding the status of weak normalization of the partial cut-elimination rewrite system for Kozen's axiomatization.

At least some of these conjectures must be resolved to obtain a reasonable proof theory of fixpoint linear logic.

# Chapter 7

# Conclusion

It is apparent from our comparison of the two kinds of modal linear logics that we consider that there are some choices to be made in adding modalities to linear logic, which do not arise for classical logic. Specifically, the algebraic and relational semantics, whose equivalence for many well-known classical modal logics has been the basis of much work in modal logic, are no longer equivalent when adapted to linear logic.

The modal and fixpoint linear logics that we have developed may be useful both in applications of linear logic, where modalities may be used to represent peripheral information about resources such as control of resources by various processes in a computer system, and in applications of temporal logics and mu-calculi, where the ability to describe resources directly may lead to more natural ways to represent certain computer-based systems.

There are a number of directions in which modal linear logic could be further developed. One is to extend the deductive system for the relational semantics to correspond to other modal logics than **KD**. Another is to consider whether alternative techniques that have been used for modal sequent calculi, such as Braüner's notion of dependency and connections between formulas [5], can be adapted to model the linear relational semantics.

Although we have not made much progress in developing the proof theory of fixpoint linear logic, our translations of the usual and free storage exponentials into this logic show the potential for using fixpoint operators to control reuse of resources in linear logic. The results of [1] suggest that an interesting approach for future work would be to attempt to adapt the circular proof rules for the fixpoint operators to linear logic, which might result in a sequent calculus with cut-elimination not only for fixpoint linear logic, but also for linear logic with free storage.

# Bibliography

[1] J. ALDWINCKLE and J.R.B. COCKETT, *The Proof Theory of Modal-$\mu$ Logics*, *Proceedings of the Workshop on Fixed Points in Computer Science*, Firenze, Italy, August 2001.

[2] P. BLACKBURN, M. DE RIJKE, and Y. VENEMA, *Modal Logic*, *Cambridge Tracts in Theoretical Computer Science* **53**, Cambridge University Press, 2001.

[3] R. BLUTE, P. SCOTT, *The Shuffle Hopf Algebra and Noncommutative Full Completeness*, Journal of Symbolic Logic 63, pp. 1413-1435, (1998).

[4] J. BRADFIELD and C. STIRLING, *Modal logics and mu-calculi*, in *Handbook of Process Algebra*, J. Bergstra, A. Ponse, and S. Smolka, editors, pp. 293–332, Elsevier, North-Holland, 2001.

[5] TORBEN BRAÜNER, *A Cut-Free Gentzen Formulation of the Modal Logic S5*, *Logic Journal of the IGPL* **8**, pp. 629–643, 2000.

[6] B. F. CHELLAS, *Modal Logic: An Introduction*, Cambridge University Press, 1980.

[7] E. M. CLARKE and E. A. EMERSON, *Design and synthesis of synchronization skeletons using branching time temporal logic*, *Logics of Programs Workshop*, *Lecture Notes in Computer Science* **131**, Springer Verlag, pp. 52–71, 1981.

[8] E. M. CLARKE, O. GRUMBERG, and D. A. PELED, *Model Checking*, The MIT Press, Cambridge, Massachusetts, 1999.

[9] M. D'AGOSTINO, D. M. GABBAY, and A. RUSSO, *Grafting modalities onto substructural implication systems*, *Studia Logica* **59**, 65–102, 1997.

[10] E. EMERSON and E. CLARKE, *Characterizing correctness properties of parallel programs using fixpoints*, LNCS **85**, pp. 169–181, 1980.

[11] J.-Y. GIRARD, *Linear Logic*, *Theoretical Computer Science* **50**, pp. 1–102, 1987.

[12] J.-Y. GIRARD, *Linear Logic, its syntax and semantics*, *Advances in Linear Logic*, eds Girard, Lafont, Regnier, *London Mathematical Society Lecture Notes Series* **222**, Cambridge University Press, pp. 1–42, 1995.

[13] J.-Y. GIRARD, Y. LAFONT, and P. TAYLOR, *Proofs and Types*, *Cambridge Tracts in Theoretical Computer Science* **7**, Cambridge University Press, 1989.

[14] J. S. HODAS and D. MILLER, *Logic Programming in a Fragment of Intuitionistic Linear Logic*, *Information and Computation* **110**, pp. 327–365, 1994.

[15] G. E. HUGHES and M. J. CRESSWELL, *A New Introduction to Modal Logic*, Routledge, New York, 1996.

[16] M. HUTH and M. RYAN, *Logic in Computer Science: Modelling and reasoning about systems*, Cambridge University Press, Cambridge, UK, 2000. With associated web site `www.cs.bham.ac.uk/research/lics/`.

[17] D. KOZEN, *Results on the propositional mu-calculus*, *Theoretical Computer Science* **27**, pp. 333–354, 1983.

[18] Y. LAFONT, *Logiques, Catégories et Machines. Implantation de Langages de Programmation guidé par la Logique Catégorique*, PhD thesis, University of Paris VII, January 1988.

[19] Y. LAFONT, *The linear abstract machine*, *Theoretical Computer Science* **59**, pp. 157–180, 1988.

[20] Y. LAFONT, *The finite model property for various fragments of linear logic*, *Journal of Symbolic Logic* **62** (4), pp. 1202–1208, Association for Symbolic Logic, 1997.

[21] P. LINCOLN, J. MITCHELL, A. SCEDROV, and N. SHANKAR, *Decision problems for propositional linear logic*, *Annals of Pure and Applied Logic* **56**, pp. 239–311, April 1992.

[22] S. MARTINI and A. MASINI, *On the fine structure of the exponential rule*, in J.-Y. Girard, Y. Lafont, and L. Regnier, editors, *Advances in Linear Logic*, pp. 197–210, Cambridge University Press, 1995.

[23] M. OHNISHI and K. MATSUMOTO, *Gentzen method in modal calculi*, *Osaka Mathematical Journal* **9**, pp. 113–130, 1957.

[24] M. OHNISHI and K. MATSUMOTO, *Gentzen method in modal calculi, II*, *Osaka Mathematical Journal* **11**, pp. 115–120, 1959.

[25] M. OKADA, *Girard's Phase Semantics and a Higher Order Cut-Elimination Proof*, unpublished manuscript, available by anonymous ftp at `iml.univ-mrs.fr/pub/okada/PhaseCutElimi.dvi.Z`.

[26] D. ROORDA, *Resource Logics: Proof-theoretical Investigations*, PhD thesis, University of Amsterdam, September 1991.

[27] C. STIRLING, *Modal and temporal logics*, in *Handbook of Logic in Computer Science* vol. 2, S. Abramsky, D. Gabbay, and T. Maibaum, editors, pp. 477–563, Oxford University Press, 1992.

[28] A. S. TROELSTRA, *Lectures on Linear Logic*, *Center for the Study of Language and Information Lecture Notes* **29**, 1992.

[29] I. WALUKIEWICZ, *Completeness of Kozen's axiomatisation of the propositional $\mu$-calculus*, *Proc. 10th IEEE LICS*, pp. 14–24, 1995.