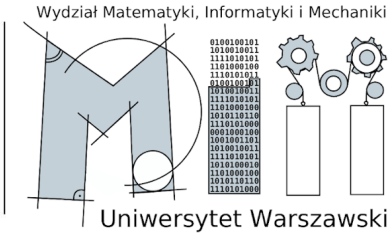
Some proof-theoretical approaches to Monadic Second-Order logic

Pierre Pradic



Numéro National de Thèse : 2020LYSEN028

THÈSE DE DOCTORAT DE L'UNIVERSITÉ DE LYON
opérée par
l'École Normale Supérieure de Lyon
en cotutelle avec **l'Université de Varsovie**

École Doctorale ED512
École Doctorale en Informatique et Mathématiques de Lyon

Spécialité de doctorat : Informatique

Soutenue publiquement le 23/06/2020, par :
Pierre Pradic

Some proof-theoretical approaches to Monadic Second-Order logic

Quelques liens entre logique Monadique du Second Ordre et théorie de la démonstration

---

Devant le jury composé de :

Hofstra Pieter, Professeur, Université d'Ottawa	Rapporteur
Simpson Alexander, Professeur, Université de Ljubljana	Rapporteur
Ong Luke, Professeur, University of Oxford	Examinateur
de Paiva Valeria, Chercheure, Samsung Research America (Mountain View)	Examinatrice
Silva Alexandra, Professeure, University College London	Examinatrice
Riba Colin, Maître de Conférences, ENS de Lyon	Directeur de thèse
Michalewski Henryk, Professeur, Université de Varsovie	Co-directeur de thèse

Acknowledgements

First and foremost I owe a huge deal to the supervision of Colin and Henryk, whom I thank heartfully. Both of them were extremely supportive at each step in my journey as a grad student, in matters both scientific and otherwise, despite the odds (e.g., my less-than-sunny disposition while writing). Their scientific work and outlook was an inspiration during my research, which I hope to carry on in the future.

Huge thanks to Pieter Hofstra and Alex Simpson who accepted to review my manuscript. I am glad to have had their feedback, especially since parts of this thesis was motivated by some of their prior work. This is also why I was pleased to have Valeria de Paiva presiding my defence; I am also very happy to have had Luke Ong and Alexandra Silva be part of the jury. I only knew them in print through some of their papers and their reputation beforehand, so I was honored to have them. Thanks to all of them for making my defence possible (and an altogether nice experience!) despite the trying circumstances.

I thank everyone at the LIP and in the automata group in Warsaw for making those stimulating and pleasant working environments. There are *many* more people I am grateful to for helping me navigate the world of research. Amongst them are my (former) supervisors and coauthors who somehow bore with me: Michael Benedikt, Chad E. Brown, Amina Doumane, Armaël Guéneau, Emmanuel Haucourt, Pierre Hyvernat, Leszek A. Kołodziejczyk, Neel R. Krishnaswami, Denis Kuperberg, Alexandre Miquel, Lê Thành Dũng Nguyễn, Damien Pous, Michał Skrzypczak and Thomas Streicher. I would like to thank them, as well as the broader community.

Companionship without logic is good too; in addition to some of the above, I also thank Adrien, Alexandre, Alice, Aurore, Etienne, Florent, Jakub, Jérémy, Marc, Laureline, Margot, Mouna, Róisín and Saara for their friendship, as well as others who I am probably unfairly forgetting. Last but not least, thanks to my family for their love and unconditional support.

Contents

Introduction

Logic, recursivity, constructivism

The origin of logic as a discipline can be traced back as far as antiquity, but mathematical logic as we know it today really started its infancy at the beginning of the 20th century. The impetus behind this development was the quest for a foundation of mathematical practice, partly out of fear of inconsistencies derived from dubious axioms (such as unrestricted comprehension in Frege's set theory). A significant step in this development was the realization that the language of logic and the rules of reasoning could be studied as mathematical objects unto themselves. Thanks to this perspective, Hilbert could spell out an ambitious program as an attempt to radically solve the crisis of foundations. The stated goals were to prove, within basic arithmetic that

1. mathematics could have a complete axiomatization
2. all mathematics could be reduced to basic arithmetic (finite reductionism)
3. basic arithmetic could be shown to be internally consistent.

Beyond the pleasing philosophical ramifications that an internal consistency result would have had, the first two points would also imply that all formal mathematical statements could be mechanically decided. Hilbert's hopes were dashed by Gödel's incompleteness theorems which invalidated all of the above in one fell swoop. The incompleteness theorem rely on encoding formulas φ and proofs π as numbers $\ulcorner\varphi\urcorner$ and $\ulcorner\pi\urcorner$ which can then effectively manipulated in the language of formal arithmetic to formalize provability. The first incompleteness theorem states that for reasonable arithmetical theories $\mathcal{T}$, the formalization of the self-referential sentence G intuitively standing for "G is not provable in $\mathcal{T}$" is independent from $\mathcal{T}$: $\mathcal{T}$ does not prove G, nor its negation. Thus point 1. is refuted, as well as (arguably) 2. The second incompleteness theorem refutes directly the third point, as it states that a formalized consistency statement $\mathrm{Con}(\mathcal{T})$ is necessarily independent from $\mathcal{T}$. While Hilbert's program as outlined above is unrealizable, the incompleteness theorems did not spell the end of research on foundations. On the contrary, one takeaway of incompleteness is that the classification of formal theories in terms of, for instance, *relative consistency* (formalizable in weak theories as $\mathrm{Con}(\mathcal{T}) \Rightarrow \mathrm{Con}(\mathcal{T}')$) or conservativity is non-trivial and deserved further study.

An issue related to those foundational concerns is the field of *computability* or *recursion theory*, the formal study of what is computable (in principle) by a machine. Computability occupies a critical foundational (if not necessarily practical) rôle in computer science as a whole. The basis for the field is the precise formalization of the class of *recursive functions*, which correspond to those functions $\mathbb{N} \to \mathbb{N}$ which are mechanizable. While a number of fundamental technical ideas and concepts from recursion theory would find suitable adaptation both in the implementation of real-world computers and programming languages and in logic, perhaps the most basic result is that some very natural (and useful!) functions $\mathbb{N} \to \mathbb{N}$ are in fact, provably not recursive. A very important such function is the truth function $f : \mathbb{N} \to \{0, 1\}$ corresponding to Hilbert and Ackermann's *Entscheidungsproblem*. Its specification says that $f(\ulcorner\varphi\urcorner) = 1$ if and only if φ is a true sentence of arithmetic. The non-recursiveness of this function is, of course, deeply tied to the incompleteness theorem. Similarly to formulas, partial recursive functions $g : \mathbb{N} \rightharpoonup \mathbb{N}$ admit encodings as numerals $g \mapsto \ulcorner g\urcorner$ which allow to define the most well-known non-recursive function corresponding to the so-called *halting problem* which asks for a function $f : \mathbb{N} \to \{0, 1\}$ such that, for every partial recursive function g, $f(\ulcorner g\urcorner) = 1$ if and only if $f(0)$ is defined. The non-recursiveness of this function is proved by a diagonal argument. Starting from those two, the computability of many such functions (or *decision problems* as those are called when the codomain is $\{0, 1\}$) have then been been studied by computer scientists and mathematicians alike.

Related to the concept of computability, and more broadly, feasibility is the theme of *constructivism* in logic. While a consensus was reached around considering that while there is now

a mainstream consensus that theorems which can be conceivably be derived from the axioms of ZF(C) and classical logic as formalized by Hilbert are uncontroversial, there are schools of thoughts challenging this state of affair on philosophical grounds. In particular, Brouwer pointed out that proofs in classical logic were unsatisfactory because of the principle of excluded middle, which allows to prove the existence of mathematical objects without providing an explicit construction of said object. This led him to reject excluded middle in his school of *intuitionism*. This gave rise to the so-called Brouwer-Heyting-Kolmogorov (BHK) interpretation of logic where proofs are to be informally thought of as computation of witnesses of validity of the statements, which forbids the use of the principle of excluded middle $\varphi \vee \neg\varphi$ or, equivalently, reductio ad absurdum $\neg\neg\varphi \Rightarrow \varphi$. Broadly speaking, we call such formalisms *intuitionistic* or *constructive*[1]. While one might be concerned that moving to constructive systems limits unduly the scope of provable statements, constructive logics usually turn out to be more expressive as double-negation translations allow to embed classical logic within constructive logic, and thus show in passing that constructive and classical logics can be shown to be equiconsistent. This first step and subsequent proof-theoretical investigations thus revealed constructive logic to be a precious tool for the global understanding of mathematical logic, independently of any philosophical commitment. Typically, intuitionistic proof systems are more well-behaved from the point of view of proof-theory, which is reflected by confluent cut-elimination and strong witnessing properties for instance. The latter may be seen as an internalization of the philosophical guarantee of intuitionism: when an object is shown to exist constructively, an explicit, computable method is given to produce said object. Proving such witnessing properties withing mathematics can be done by using realizability models, where formulas are interpreted by set of proofs rather than mere truth values. A paradigmatic example of this approach is *Kleene's realizability*, which interprets formulas of (higher-order) arithmetic as sets of recursive functions called *realizers*. Typically, a formula $\forall x \in \mathbb{N}\ \exists y \in \mathbb{N}\ \varphi(x, y)$ is interpreted by the set of *recursive* functions $f : \mathbb{N} \to \mathbb{N}$ such that $\varphi(x, f(x))$ holds. The underlying logic is intrinsically intuitionistic as, if assuming classical foundations, the negation of excluded middle $\neg\forall A \quad (A \vee \neg A)$ holds as a direct consequence of the undecidability of the halting problem in the associated model.

There is much more to say on the developments of recursion theory, constructivism and mathematical logic, their flourishing interactions and related fields of research. However that goes well beyond the scope of this short introduction whose purpose is to introduce the themes of foundational strength, recursivity and intuitionism.

Monadic Second-Order logic and automata

While Gödel's theorem implies that the theories of arithmetic, which are considered rather modest foundations in which logic is still formalizable, are undecidable, this does not preclude more restricted logics from being so. This perspective is appealing from a practical point of view if one is interested in automatically verifying that computer programs or controller chips are bug-free in restricted settings. This has given rise to multiple verification logics such as LTL, CTL or the modal μ-calculus, all of which can be decided.

Monadic Second-Order logic (abbreviated MSO from now on) designates a class of classical theories which are powerful enough to interpret many verification logics while still remaining decidable. The precise definition of MSO varies according to the underlying universe, but the language is generated in the same way: it is the language of second order-logic where the second-order quantification is restricted to unary (hence the name *monadic*) predicates, which can equivalently be regarded as sets. Formally speaking, a minimal language for MSO can be given by the following grammar where x designate individual variables, X set variables and $P(x_1, \ldots, x_n)$ ranges over basic predicates of the underlying structure.

$$\varphi, \psi ::= x \in X \mid P(x_1, \ldots, x_n) \mid \exists x.\varphi \mid \exists X.\varphi \mid \varphi \wedge \psi \mid \neg\varphi$$

Typical instances of MSO are MSO over the structure of natural numbers equipped with its order $(\mathbb{N}, <)$ (henceforth abbreviated MSO(ω)) and MSO over the infinite binary tree $(\{a, b\}^*, S_a, S_b)$ where S_i designates the successor relation (i.e. $S_i(x, y)$ holds if and only if $y = xi$) and $\{a, b\}^*$ the set of words over the finite alphabet $\{a, b\}$. The key to deciding these MSO theories is their tight

[1] As this thesis does not delve into philosophical issues related to constructivism, we will use the two terms interchangeably. In particular, we do not refer to Brouwerian axioms incompatible with classical logic when calling a system intuitionistic in the sequel, but merely to the rejection of the law of excluded middle/double negation elimination. The interested reader may consult [73] for an introduction to the main strands of constructive mathematics and the basic specificities of Brouwerian intuitionism.

connection with the theory of *automata* over infinite words and labeling of the infinite tree. We now focus the discussion on word automata and $\mathsf{MSO}(\omega)$; similar observations can be made for trees.

Automata over finite words are a formal devices computing languages $\mathcal{P}(A^*)$ (the *regular languages*), which may be seen as specific casesof (linear-time) Turing machines computing a function $A^* \to \{0,1\}$. This means in particular that finite-state automata may be coded with finite data which can be effectively manipulated. Finite-state automata are much less expressive than general Turing machines. One advantage of automata, beyond simplicity, is that one may algorithmically decide interesting semantic properties such as the emptiness problem (whether a given automaton recognizes any word at all). This is to be contrasted against the impossibility of solving any such meaningful problem for general recursive functions due to Rice's theorem. Infinite word automata are also formally defined with finitary data[2], but are meant to define language of infinite words, i.e., subsets of $A^{\mathbb{N}}$ instead of A^*. These sets are typically uncomputable: even for a fixed automaton $\mathcal{A}$, there is no recursive map $f : \mathbb{N} \to \{0,1\}$ such that given a code $\ulcorner u \urcorner$ of recursive word $u \in A^{\mathbb{N}}$, $f(\ulcorner u \urcorner) = 1$ if and only if u is recognized by $\mathcal{A}$. The reason for this is that, while the sequence of states appearing in a run of an infinite word automaton is computable from its input, the notion of accepting run is not recursive. For Büchi automata for instance, it asks that a final state appear infinitely often; deciding this for an arbitrary sequence of state is strictly harder than even the halting problem.

This increased computing power does not prevent infinite word automata and the associated notion of ω-regular language from sharing nice properties with finite word automata and regular languages. For instance, a key property one may algorithmically decide whether the language defined by a Büchi automaton is empty or not. ω-regular languages, as regular languages, are also stable under union, complement and projection (the latter operation corresponding to existential quantification). However, establishing those properties is harder than in the finite case. Typically, while complementing a non-deterministic Büchi automaton may still be done algorithmically, the conceptually easier way of doing so does not necessarily go through determinization, but rather a more algebraic construction. Furthermore, arguing that these more involved constructions are sound require non-constructive arguments.

Those constructions allow to give a semantic-preserving translation from $\mathsf{MSO}(\omega)$ formulas to automata, which, thanks to the decidability of emptiness checking for automata, provides an effective procedure to decide $\mathsf{MSO}(\omega)$ formulas: to do so, translate the formula to an automaton and run an algorithm to determine whether the language recognized by this automaton is empty or not. There is also a semantic-preserving translation back from Büchi automata to $\mathsf{MSO}(\omega)$, thus establishing in a precise sense that $\mathsf{MSO}(\omega)$ is *the* logic of infinite word automata.

The constructiveness of MSO

As we saw in the previous discussion, $\mathsf{MSO}(\omega)$ and various generalizations has a peculiar link to constructivism: they are logics which are inherently non-constructive which can be decided effectively. While this observation is rather obvious because of the connection with Büchi automata which go beyond computable functions, it should be stressed that it is not the case for many decidable logics such as, for instance, bounded arithmetic, the first-order logic of dense linear orders (i.e. the theory of $(\mathbb{Q}, <)$) or real closed fields (the theory of $(\mathbb{R}, <, +, \cdot)$)[3]

The thesis is thus centered around the following informal question, where the less logically inclined reader may substitute "theory of automata over infinite structures" for MSO.

Question. *How (non-)constructive is* MSO*?*

Let us stress that this question is both broad and informal and that the present thesis does not address it in full generality. It should rather be regarded as the common motivation for topics studied as part of this thesis, which is itself split into two thematically distinct parts.

Part I contains developments pertaining to the constructiveness of $\mathsf{MSO}(\omega)$ from the point of view of the BHK interpretation. The main goal there is to study intuitionist variants of $\mathsf{MSO}(\omega)$ with an eye towards the extraction of effective computational content from proofs: we want witnesses for $\forall\exists$ statements to be able to compute recursive maps between sets of infinite words[4].

[2] In particular, Büchi automata consist of the same data as non-deterministic finite-state automata.

[3] Assuming that $\neg x \neq y \Rightarrow x = y$ holds for $x, y \in \mathbb{R}$ in the "constructive" metatheory of interest. This is the case if $\mathbb{R}$ designates Cauchy reals and Markov's principle holds.

[4] Note that if one is just happy to find explicit definitions of possibly non-computable such functions, this is entirely doable. This corresponds to the *uniformization problem*, which has a nice solution for $\mathsf{MSO}(\omega)$: relations defined in $\mathsf{MSO}(\omega)$ may be uniformized in $\mathsf{MSO}(\omega)$ [66, 15].

In fact, we are going to make one further restriction in order to both simplify drastically our setting and draw from automata-theoretic results: our realizers will consist of functions that are computable by *Mealy machines*, possibly the most simple class of finite-state, letter-to-letter transducers. Such a machine with input alphabet A and output alphabet B generates a sequence of length-preserving functions between words $A^n \to B^n$ which can be regarded as a single function $A^{\mathbb{N}} \to B^{\mathbb{N}}$ over infinite words.

Part II on the other hand is not concerned with constructiveness in the sense of intuitionism, but rather with the foundational strength of MSO theories. The main informal objective here is, rather than delimiting what is intuitionistic in MSO, to see what are the minimal axiomatic requirements to make MSO behave "as usual". More specifically, we study Büchi's decidability theorem for $\mathsf{MSO}(\omega)$ in the context of *Reverse Mathematics*, a vast foundational program launched by Friedman to classify theorems of everyday mathematics according to their logical strength, or, informally, degree of non-constructiveness. Concretely, this is achieved showing, over a weak base theory based on a restriction of second-order arithmetic, that the theorem under consideration is equivalent to the axioms of a stronger subsystem of second-order arithmetic. Most of the time, the weak base theory is taken to be RCA_0 (Recursive Comprehension Axiom), a weak subsystem of arithmetic where induction is limited to Σ^0_1 formulas and comprehension is limited to recursive sets (while still featuring full excluded middle). It will thus turn out that the decidability of $\mathsf{MSO}(\omega)$, as well as the soundness of complementation of Büchi automata are equivalent to induction for Σ^0_2 formulas, which is also sufficient to prove the soundness of a determinization procedure. Part II then concludes by giving some preliminary results towards a similar analysis for MSO over the rationals (formally speaking, the structure $(\mathbb{Q}, <)$). These results seem to point out that the decidability theorem for this theory sits strictly between the decidability of $\mathsf{MSO}(\omega)$ and MSO over the infinite tree.

The two parts are self-contained and may be read independently from one another. We refer to their respective introductions for a more detailed chapter-by-chapter description of the contributions. The bulk of those contribution is the attempt to synthesize and expand the work we presented in [56, 58, 57] in Part I. Part II contains the material presented in [42] with minimal modifications in addition to the preliminary results pertaining to MSO over $\mathbb{Q}$.

Part I

A Curry-Howard approach to Church's synthesis

Summary The first part of this thesis is devoted to studying restrictions of $\mathsf{MSO}(\omega)$ with strong witnessing properties. The main goal here is to have logical systems with a Curry-Howard correspondence allowing for a straightforward extraction of programs from proofs. This is achieved by building proof-relevant models for the logical systems in question. In contrast with most usual Curry-Howard settings, we restrict ourselves to extracting only a small subcass of recursive functions, namely those which corresponds to deterministic finite-state synchronous letter-to-letter transducers, i.e. *Mealy machines*. This restriction is rather natural from the point of view of automata theory as there is an obvious kinship between transducers, infinite word automata and thus $\mathsf{MSO}(\omega)$. This will manifest as connexions between our development and Church's synthesis problem. Furthermore, while there are many notions of transducers with greater expressive power (typically regular or polyregular transductions as defined in [8]), Mealy machines have the crucial advantage of having a notion of cartesian products corresponding to the underlying cartesian product of alphabets. On the other hand, we work with a rather unusually weak computational model from the point of view of the Curry-Howard correspondence as

1. all realizers $f : A^\omega \to B^\omega$ are causal, i.e. $f(a)_n$ only depends on $a_0, \ldots, a_n$.

2. there is no natural notion of higher-order functions available (and thus a priori no proof-relevant interpretation of intuitionistic implication).

We stick firmly to (1) throughout the thesis and never consider alternatives. After some preliminary material in Chapter 1 and 2, we investigate a simple theory and a companion proof-relevant model for extraction in Chapter 3. This setting has the advantage of being elementary and being a nice refinement of the usual correspondence between $\mathsf{MSO}(\omega)$ formulas and non-deterministic Muller automata, while allowing for extraction in the above sense. However, it suffers the full brunt of (2) and thus allows only to interpret a minimal set of connectives allowing for double-negation translations; in particular, there is no primitive intuitionistic implication $\Rightarrow$. Chapter 4 attempts to partially circumvent restriction (2) by moving to a more general setting related to alternating automata in which a richer theory based on linear logic is interpreted. This time, the lack of higher-order functions in the category of Mealy machines means that a general notion of exponential modality is lacking in the logic. However, exponential modalities are seen to be definable for polarized formulas corresponding to non-deterministic/universal automata. Underlying the construction is a notion of infinite games for which winning strategies correspond to our notion of realizers. Chapter 5 and 6 start from the remark that the combinators on games defined in 4 are reminiscent of Dialectica interpretations. After recalling the Dialectica construction in a fibred setting over a cartesian-closed base in Chapter 5, we fix a convenient cartesian-closed base of causal functions (i.e., where we do not break (1) but ignore (2)) and give a similar transformation which, when applied to the standard proof-irrelevant model result in an extension of the realizability model of Chapter 4. Finally, Chapter 7 discusses how to adapt this material to restrict to finite-state realizers to get a model equivalent to the one presented in Chapter 4 and exploits the formal similarities with Dialectica exposed in the previous chapter to obtain a complete axiomatization of the model.

Detailed outline

Chapter 1 gives background information required on automata over infinite words, transducers and Church's synthesis. This chapter is rather short and non-technical; in particular the most combinatorial results are merely referenced and stated. First, non-deterministic automata over infinite words recognizing ω-regular languages are defined. The stability under boolean connectives and projections are discussed, highlighting that the soundness of most construction is straightforward save for the one obtained by Büchi's complementation theorem [12] and McNaughton's determinization theorem [48]. Then, a complete axiomatization of $\mathsf{MSO}(\omega)$ due to Siefkes [65] is introduced, as well as very basic material on Mealy machines. Finally, Church's synthesis and the Büchi-Landweber theorem [13] are introduced.

Chapter 2 first introduces preliminary technical material regarding Mealy machines for later chapters. It is remarked that alphabet and functions generated by Mealy machines may be arranged in a category with cartesian products but no internal homsets (i.e. no notion of λ-abstraction). We then prove that this class of synchronous function is stable under a construction corresponding to guarded recursion [7, 53]. A term syntax for Mealy machines based on this combinator with a suitable equational theory is given and shown to be sound and complete. Then, we show that

$\mathsf{MSO}(\omega)$ is equivalent to a first-order theory of equality between streams, FOM, which in particular has terms for Mealy machines. Formally speaking, we show that that one may be interpreted in the other and lift the complete axiomatization of $\mathsf{MSO}(\omega)$ to FOM. This allows us to substitute FOM for $\mathsf{MSO}(\omega)$ in the sequel, which makes subsequent developments much more straightforward.

Chapter 3 defines an intuitionistic subtheory SFOM of FOM and a suitable Curry-Howard correspondence allowing for the extraction of Mealy machines from proofs. The language of SFOM is restricted to formulas built with $\exists$, $\neg$, $\wedge$ and atomic equalities and its theory is a non-classical subtheory of FOM which is still strong enough to allow a double-negation translation of FOM into SFOM. The extraction of finite-state realizers is ensured by considering a proof-relevant model of SFOM. The main idea behind this model is to interpret formulas as non-deterministic Muller automata in a standard way, but then require that SFOM proofs be mapped to simulations between the automata rather than being mere witnesses of language inclusions. This chapter is meant as a counterpart to [56] where the very same model is discussed for a theory SMSO, which is to $\mathsf{MSO}(\omega)$ what SFOM is to FOM.

Chapter 4 goes further by considering a theory LSFOM based on linear logic also admitting a sound extraction procedure of finite-state Mealy machines from proofs. The advantage of LSFOM over SFOM is that it features more connectives, namely, universal quantification and linear implication while actually *extending* the theory LSFOM. An approach entirely analogous to the one in Chapter 3 is taken. First the definition of the logic is given: LSFOM is formally based on full intuitionistic multiplicative linear logic (FIMLL as defined in [34]), augmented with equalities and first-order reasoning. On top of that, a polarity system is given to regulate the admissible instances of contraction and weakening, together with exponential connectives defined only over polarized formulas. Then, the embedding of FOM in LSFOM is given. This embedding, which was chosen because of its simplicity and the underlying automata-theoretic intuition, is not standard for linear logic, but rather tied to the polarity system of LSFOM. Alternatives are also briefly remarked upon. Finally, a proof-relevant model of LSFOM is defined to ensure soundness with respect to synthesis. The model refines the one given in the previous chapter by allowing for general alternating automata. The notion of simulation thus becomes much more intricate, so we stay rather informal and postpone the fine description of the realizers and associated combinators for later in order to focus on intuitions. This chapter is meant as a counterpart to [58] where this model is introduced.

Chapter 5 starts with the observation that the model considered in Chapter 4 shares a lot of formal similarities (such as being a model of FIMLL) with Dialectica categories (namely the categories $D\mathbf{C}$ of [21]). In order to make such a connexion more precise, this Chapter is dedicated to introducing Dialectica fibrations. After a short introduction to the basic concepts of categorical logic involved, we recall the definition of the Dialectica construction $p \mapsto \mathfrak{Dial}(p)$ over fibrations and as well as the related $\mathfrak{Sum}$ and $\mathfrak{Prod}$ discussed in [31]. Then, taking full advantage of the relationship between the three maps, we consider rather unusual exponentials modalities for Dialectica, namely, those that arise through the fibred adjunctions between $\mathfrak{Sum}(p)$, $\mathfrak{Dial}(p)$ and $\mathfrak{Prod}(p)$. This is not something often considered for Dialectica, as these adjunctions are only definable when p already has simple quantifications[5]. We then remark that although Dialectica categories are not *-autonomous in most cases, one may show that there exist (non-canonical) retracts of the canonical morphism $\big((A \multimap \bot) \multimap \bot\big) \multimap A$ when starting from the category of sets and assuming the full axiom of choice. We then conclude the chapter by giving and proving the characterization theorem, including the formulas featuring our rather unorthodox exponentials.

Chapter 6 is devoted to adpating the $\mathfrak{Dial}$ construction to produce game-based models generalizing the one given in Chapter 4. To do so, we first describe a convenient higher-order extension $\mathbb{S}$ of the category Mealy that we use as a base. $\mathbb{S}$ is defined as a full subcategory of the topos of trees $\mathbb{T}$, a natural setting for denotational settings of the guarded λ-calculus. The reason for considering $\mathbb{S}$ instead of $\mathbb{T}$ is that a key combinatorial element in building our category of games is a notion of pointwise exponentials which cannot be defined for all trees . We retain however cartesian-closure of $\mathbb{S}$, as well as the usual guarded fixpoint operator. We then use this category to define a category of zigzag games DZ, which is shown to be a model of MELL. A crucial observation there is that internal-homsets are only needed to define the exponential !, while the rest is handled thanks to the guarded fixpoint operator and our notion of pointwise functions. This development is

[5]Recall that Gödel's original use for the Dialectica transformation was for a quantifier-free p.

a stepping stone towards defining the operation $p \mapsto \mathfrak{Dial}^{\blacktriangleright}(p)$ over $\mathbb{S}$-fibrations, which is intended to map a boolean model of the first-order logic with equalities to a higher-order analogue of the model presented in Chapter 4. After establishing that there is a fibred LNL-adjunction between $\mathfrak{Dial}^{\blacktriangleright}(p)$ and $\mathfrak{Dial}(p)$, the rest of the chapter mirrors the material in the previous chapter: $\mathfrak{Dial}^{\blacktriangleright}(p)$ is proven to be sound with respect to first-order full intuitionistic logic with equalities and a similar characterization theorem is given. Perhaps the key difference is that this characterization theorem reveals that $\mathfrak{Dial}^{\blacktriangleright}(p)$ satisfies an axiom invalidated in the "standard model".

Chapter 7 bridges the gap between the higher-order model over $\mathbb{S}$ provided in the previous chapter and the automata-based model described in Chapter 4 (which may be regarded as a fibration over Mealy). This is done by first noticing that the morphisms used in the construction of DZ, $\mathfrak{Dial}^{\blacktriangleright}$ and the afferant logical structure could be carried out without using the internal homsets of $\mathbb{S}$ if one ignored the exponentials. We thus define an inductively generated subcategory $\mathbb{S}^{\mathrm{fin}}$ of $\mathbb{S}$ which retains enough morphisms and combinators (most crucially, the parametric guarded fixpoint combinator and the pointwise exponential) to carry out analogues of those constructions $\mathsf{DZ}_{\mathrm{fin}}$ and $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}$, the latter acting on fibrations over $\mathbb{S}^{\mathrm{fin}}$ instead of fibrations over $\mathbb{S}$. We then show that the category Mealy embeds into $\mathbb{S}^{\mathrm{fin}}$ by exploiting the results of Chapter 2, and then that $\mathbb{S}^{\mathrm{fin}}$ embedds into an elementary completion of Mealy, its Karoubi envelope $\mathrm{Kar}(\mathsf{Mealy})$. We also touch briefly on how fibrations over some category $\mathbb{C}$ can be taken to a fibration over $\mathrm{Kar}(\mathbb{C})$ and vice-versa. This then allows to discuss how to make $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}$ act on fibrations over Mealy rather than $\mathbb{S}^{\mathrm{fin}}$, and then proceed to give a high-level discussion on how the results discussed in Chapter 5 and 6 adapt to $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}$ in order to interpret LSFOM and its polarized exponentials. Finally, the suitable restriction of the characterization theorem proven in Chapter 6 to our newly obtained model is leveraged to extend the axiomatization of LSFOM into a complete theory LSFOM^{+}, mimicking the main result of [57]. Besides relying on the characterization theorem, the completeness proof also crucially rely on the Büchi-Landweber theorem and the ad-hoc double linear negation elimination discussed in previous chapters.

Notational conventions for Part I We may write $\mathbb{N}$ or ω for the set of natural numbers. If $a, b \in \mathbb{N}$, $[\![a, b]\!]$ denotes the set $\{k \in \mathbb{N} \mid a \leq k \leq b\}$. Given a sets X and I, we sometimes $x = (x_i)_{i \in I}$ for sequences $x \in X^I$, and x_i for the application $x(i)$ when it is more idiomatic to do so. Typically, we do this for sequences (for instance, the evaluation of a function $f : A^\omega \to B^\omega$ on the sequence $(a_i)_{i \in \mathbb{N}}$ and position $n \in \mathbb{N}$ may be written $f(a)_n$). We also sometimes write $(x_i)_{i=0}^n$ for families $X^{[\![0,n]\!]}$. Non-empty finite sets are called *alphabets*. We assume a knowledge of the definitions of category, cartesian-closure and functors for all of Part I. No category-theoretic concept beyond those are required until Chapter 5. We adopt a set of notation for basic categorical constructions, that are also employed for concrete functions between sets. $\circ$ is reserved for composition of arrows. $\mathbf{Set}$ denotes the category of sets and functions and $\mathbf{FinSet}_{\geq \mathbf{1}}$ denotes the full subcategory of sets whose objects are alphabets. Given a category $\mathbb{C}$ and objects A and B of $\mathbb{C}$, we write $[A, B]_{\mathbb{C}}$ for the homset from A to B, $A \times B$ for the cartesian product and A^B for the exponential (provided they exist). If $\mathbb{C}$ has a terminal object, it is written 1 and we write ! for the (uniquely determined) morphisms $A \to 1$. Given maps $f : Z \to A$ and $g : Z \to B$, we write $\langle f, g \rangle$ for the pairing $Z \to A \times B$ determined by the universal property of the cartesian product and $\pi_i : A_1 \times A_2 \to A_i$ the projection maps ($i \in \{1, 2\}$). We generalize these notations to the n-ary case for every $n \in \mathbb{N}$ in the obvious way. We write $\mathrm{ev} : A^B \times B \to A$ for the evaluation map in a cartesian closed category and given $f : A \times B \to C$, we write $\Lambda(f) : A \to C^B$ for its curryfication.

Although we shall introduce it later, let us mention that we will frequently use the abbreviation f.s. to mean *finite-state* in the sequel.

Chapter 1

Background: automata, Mealy machines and Church's synthesis

This chapter gives a short introduction to the correspondence between infinite word-automata and $\mathsf{MSO}(\omega)$, Mealy machines and Church's synthesis problem, which motivates our notion of constructiveness for the intuitionistic subsystems of $\mathsf{MSO}(\omega)$ we study in later chapters. Relevant classical results are merely stated. For more thorough introduction to these topics especially infinite word automata, we redirect the reader to the textbooks [54, 71] and the survey article [72] regarding Church's synthesis. The reader familiar with the aforementioned content might safely skip this chapter, maybe with the exception of Section 1.2 which mentions a complete axiomatization of $\mathsf{MSO}(\omega)$ due to Siefkes [65].

1.1 $\mathsf{MSO}(\omega)$ and automata

We first recall the seminal connection between $\mathsf{MSO}(\omega)$ and finite-state automata over infinite words. As discussed in the introduction, the language of a MSO-theory contains all boolean connectives, first-order quantification and quantification over unary[1] predicates. This leaves the term language and atomic first-order predicates to be fixed; here, we have in a constant term symbol $\dot{\mathsf{Z}}$ for 0 and a term symbol $\dot{\mathsf{S}}$ for the successor function $n \mapsto n+1$.

$$\begin{array}{lcl} t, u & ::= & \dot{\mathsf{Z}} \mid \dot{\mathsf{S}}(t) \mid x \\ \varphi, \psi & ::= & t \in X \mid \exists x.\varphi \mid \exists X.\varphi \mid \varphi \wedge \psi \mid \neg\varphi \end{array}$$

$\mathsf{MSO}(\omega)$ might be thus regarded as a subsystem of second-order arithmetic, albeit a rather weak one: addition $+$ is undefinable as a relation for instance. The main reason why it is impossible to use the power of second-order logic to design impredicative encoding is because of the restriction over unary predicates and the lack of a pairing function. Having either pairing or addition definable in $\mathsf{MSO}(\omega)$ would make the language as expressive as second-order arithmetic, which in turn would mean that theory would be undecidable; this would contradict Büchi's decidability theorem.

Another appeal of $\mathsf{MSO}(\omega)$ as a formal system is its tight connexion with infinite-state automata over infinite words. They operate very much like automata over finite words, save for the acceptance condition, which needs to distinguish infinite runs. As there are several interesting such acceptance modes, we first give a generic definition.

Definition 1.1.1. *A non-deterministic infinite word automaton over the alphabet A is a tuple $\mathcal{A} = (Q, I, \Delta, \Omega) : A$ where*

- *Q is a finite set of states*
- *I is a subset of Q dubbed the* initial states
- *$\Delta \subseteq Q \times A \times Q$ is the transition relation*
- *$\Omega \subseteq Q^\omega$ is the acceptance condition*

[1] One may also call them *monadic*, justifying the name MSO. We do not, so as to avoid suggesting any connexion with monads.

An ω-word $w \in A^\omega$ is recognized by $\mathcal{A}$ if and only if there is a sequence $q = (q_n)_{n\in\mathbb{N}} \in \Omega$ such that $q_0 \in I$ and $(q_n, a_n, q_{n+1}) \in \Delta$ for every $n \in \mathbb{N}$. We write $\mathcal{L}(\mathcal{A})$ for the set of words $\subseteq A^\omega$ recognized by the automaton $\mathcal{A}$.

$\mathcal{A}$ is called deterministic if I is a singleton $\{q^\iota\}$ and Δ is isomorphic to the graph of a function $\delta : \Sigma \times Q \to Q$.

In the usual cases, Ω is given by some finitary data. The way Ω is generated from such data corresponds to the different acceptance modes alluded to earlier. In this introduction, we briefly discuss Büchi, parity and Müller acceptance.

Definition 1.1.2. *Let $\mathcal{A} = (Q, I, \Delta, \Omega) : A$ be a non-deterministic automaton. If $X \subseteq \mathcal{P}(Q)$, define $[X]_\infty \subseteq Q^\omega$ to be the set of sequences of states such that the set of states appearing infinitely often is X.*

$$[X]_\infty := \{q \in Q^\omega \mid \{r \mid \forall k \exists n \geq k \; q_n = r\} \in X\}$$

If the accepting condition Ω of $\mathcal{A}$ is given by

- *a set of* accepting states *$F \subseteq Q$ such that*

$$\Omega = \{q \in Q^\omega \mid \forall k \exists n \geq k \; q_n \in F\} = [\{X \mid X \cap F \neq \emptyset\})]_\infty$$

  then $\mathcal{A}$ is called a Büchi automaton*.*

- *a priority function $c : Q \to \mathbb{N}$ such that*

$$\Omega = \{q \in Q^\omega \mid \limsup_{n\in\mathbb{N}} c(q_n) \text{ is even}\} = [\{X \subseteq Q \mid \sup_{q\in X} c(q) \text{ is even}\}]_\infty$$

  then $\mathcal{A}$ is called a parity automaton.

- *a set $\mathcal{F} \subseteq \mathcal{P}(Q)$ such that*

$$\Omega = [\mathcal{F}]_\infty$$

  then $\mathcal{A}$ is called a Muller automaton*.*

Note that every Büchi automaton may be seen as a parity automaton by mapping the set of accepting states F to its characteristic function $\chi_F : Q \to 2 \subseteq \mathbb{N}$, and every parity automaton may be seen as a Muller automaton. Conversely, a non-deterministic Muller automaton $\mathcal{A} = (Q, I, \Delta, [\mathcal{F}]_\infty) : A$ can effectively be turned into a Büchi automaton $\mathcal{A}^B$ recognizing the same language (see e.g. [54, Theorem 7.1]).

Proposition 1.1.3. *Non-deterministic Büchi, parity and Muller automata recognize the same languages.*

These automata thus provide finite representations for languages $L \subseteq \mathcal{P}(A^\omega)$ of infinite words, the ω-regular languages. One should also note that this representation is effective in the following sense.

Proposition 1.1.4. *There exists an algorithm taking as input a Büchi/parity/Muller automaton $\mathcal{A}$ and decides whether the language $\mathcal{L}(\mathcal{A})$ recognized by a empty or not.*

Proof. Given that the translation leading to Proposition 1.1.3 are effective, it is sufficient to prove the decidability of emptiness for Büchi automata. To do so, given a Büchi automaton $\mathcal{A} = (Q, I, \Delta, [F]_\infty) : A$, it suffices to be able to tag the states from which a non-empty language may be recognized. First tag the set $F' \subseteq F$ of final states such that $f \in F'$ if and only if there exists a non-empty-word $a_0, \ldots, a_k$ tagging a non-trivial cycle containing f, i.e., there exists $q_0, \ldots, q_n$ with $q_0 = q_n = f$ and $(q_i, a_i, q_{i+1}) \in \Delta$ for every $i \leq n$. Then, if a state q is coaccessible from F', then it recognizes a non-empty language. □

This proposition may be used in conjunction with the following correspondence between $\mathsf{MSO}(\omega)$ formulas and automata to derive the decidability of $\mathsf{MSO}(\omega)$.

Theorem 1.1.5. *There exists an algorithm taking as input a $\mathsf{MSO}(\omega)$ formula $\varphi(X_0, \ldots, X_{n-1})$ with the displayed free variables outputting a non-deterministic Büchi automaton $\mathcal{A}_\varphi : 2^n$ such that $w = \langle w_0, \ldots, w_{n-1}\rangle \in \mathcal{L}(\mathcal{A}_\varphi)$ if and only if $\varphi(w_0, \ldots, w_{n-1})$ holds.*

This theorem is proved by emulating the connectives of $\mathsf{MSO}(\omega)$ at the level of automata. This means proving that ω regular languages are sable under projection (the counterpart of $\exists$), intersection ($\wedge$) and complementation. While closure under projection and intersection is rather straightforward, complementation is more challenging. For finite word automata, the complementation procedure relies on a determinization procedure. Then, complementation is easy for deterministic automata. However, while the determinization algorithm for finite word automata is straightforward, the situation with infinite word automata is a bit more delicate. Historically, Büchi first proved that non-deterministic Büchi automata may be complemented using a weak form of Ramsey theorem for pairs to analyze infinite runs [12]. Later on, McNaughton proved [48] that Büchi automata may be determinized into Rabin automata which are in turn easily compiled into deterministic parity automata.

Theorem 1.1.6 (McNaughton)**.** *Given a non-deterministic Büchi automaton $\mathcal{A} : A$, there exists a deterministic parity automaton $\mathcal{D} : A$ such that $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{D})$.*

Remark. *Let us note that the proof of either McNaughton's theorem, or even Büchi's direct complementation argument are inherently non-constructive in the following sense: given a word w and an accepting run of $\mathcal{D}$ over w, then there is no recursive way of computing an accepting run of $\mathcal{A}$ over w. This is to be contrasted against all of the other automata constructions above, which allow for such computations*[2]*.*

1.2 Axiomatizing $\mathsf{MSO}(\omega)$

Before moving on, let us remark that automata give a decision procedure for $\mathsf{MSO}(\omega)$ but say little about its proof-theory at a first glance. Among other things, this does not answer the following question: what is a natural set of minimal axioms for $\mathsf{MSO}(\omega)$? In the sequel, since we shall study subsystems of $\mathsf{MSO}(\omega)$ with the goal of setting up a Curry-Howard correspondence, it is important to recall that the connection with automata also uncovered a natural complete axiomatization of $\mathsf{MSO}(\omega)$.

Theorem 1.2.1 (Siefkes)**.** *The standard model of $\mathsf{MSO}(\omega)$ is fully axiomatized by the basic arithmetical axioms of non-confusion, injectivity of successor and the* comprehension schemes *and* induction schemes*.*

We give a more formal list of these axioms below in Figure 2.5, once $\mathsf{MSO}(\omega)$ has been more properly introduced. This axiomatization is remarkable as it exactly consists of the axioms of second-order arithmetic restricted to the language of $\mathsf{MSO}(\omega)$. Siefkes' original proof [65] does rely heavily on the correspondence between MSO and automata outlined above. A model-theoretic proof is given in [60].

1.3 Mealy machines

One of the appeal of $\mathsf{MSO}(\omega)$ is that it may be seen as a powerful logic for verification. In particular, the decidability of $\mathsf{MSO}(\omega)$ enable to verify properties about finite-state *Mealy machines*, a notion used in the conception of reactive systems like CPU components or microcontroller for various embarked systems. A simplifying assumption is that we have a fixed, discrete synchronous notion of time and that the current state of a given system should only depend on the past. This is captured by the notion of *causal function*.

Definition 1.3.1. *A* causal *function is a function $f : A^\omega \to B^\omega$ such that $f(u)_n = f(v)_n$ whenever $u_i = v_i$ for all $i \leq n$.*

Note that the set of causal functions $f : A^\omega \to B^\omega$ is in one-to-one correspondence with families of functions $(f_n : A^{n+1} \to B)_{n\in\mathbb{N}}$ by taking $f(a)_n = f_n(a|_{[\![0,n]\!]})$. Not all of causal functions f can be concretely implemented in hardware because the amount of data on the input needed to compute f_n may grow with n. A Mealy machine is essentially an intensional description of causal function f where the memory, holding enough information to compute $f(u)_n$ if given u_n, is bounded by a finite set of states.

[2]However, the problem of computing an accepting run of $\mathcal{A}$ over w from an accepting run of $\mathcal{D}$ *and* additional data witnessing the acceptance of w (e.g., the highest parity appearing infinitely often and a bound after which only lower parities occur) may very well be doable recursively; these considerations are pregnant in the Reverse Mathematics of Büchi's theorem presented in Chapter 9. Note however that whether such data is available in a constructive metatheory depends on a careful phrasing of the winning condition, which are usually not stable under double-negation in constructive logic!

Definition 1.3.2. *A* Mealy machine *from alphabet A to B is a tuple $\mathcal{M} = (Q, q^\iota, \partial) : A^\omega \to B^\omega$ consisting of*

- *a finite set of states Q*
- *an initial state $q^\iota \in Q$*
- *a transition function $\partial : A \times Q \to B \times Q$.*

By iteration, a Mealy machine defines a function $\partial^* : A^+ \to B \times Q$ (where A^+ is the set of non-empty words over A) by the following recursion:

$$\partial^*(a) = \partial(a, q^\iota) \qquad \partial^*(wa) = \partial(a, \pi_2(\partial^*(w)))$$

which can be used to define a causal function $[\![\mathcal{M}]\!] : A^\omega \to B^\omega$. We call causal functions which can be derived from Mealy machines *finite-state*.

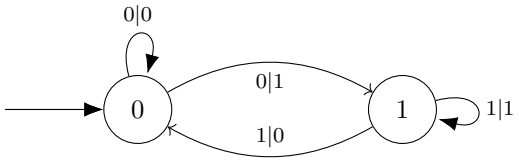
Remark. *All functions induced by finite-state Mealy machines are causal, but the converse does not hold. For instance, all constant functions to 2^ω are causal, but the infinite word $w \in 2^\omega$ such that*

$$w_n = 1 \quad \Leftrightarrow \quad n \text{ is prime}$$

is not implementable by a Mealy machine (with trivial input 1^ω and output 2^ω) with finitely many states.

However, one can consider the notion of Mealy machine with possibly infinite state-space and show that every causal function f admits a minimal[3] *Mealy machine $\mathcal{M}_f$ implementing it, i.e. with $[\![\mathcal{M}_f]\!] = f$. f is thus finite-state if and only if the state space of $\mathcal{M}_f$ is finite.*

Example 1.3.3. *One of the simplest non-trivial family of finite-state causal functions is given by one-step delay functions: given an alphabet A and $a \in A$, write $\mathbf{cons}_a : A^\omega \to A^\omega$ for the finite-state causal function such that $\mathbf{cons}_a(w)(0) = a$ and $\mathbf{cons}_a(w)(n+1) = w(n)$. A minimal machine implementing $\mathbf{cons}_a$ has $|A|$ states; for $A = 2$ and $a = 0$, it may be depicted as follows*

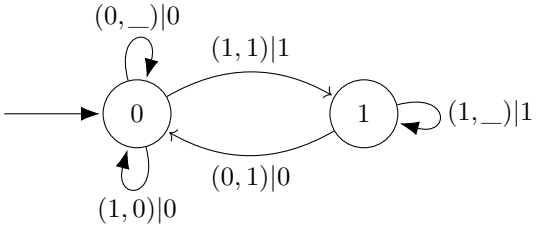


Example 1.3.4. *A typical notion that can be modelled as a Mealy machine is that of a register. Abstractly, a register holding a value belonging to some alphabet A (for a 64-bit architecture, $A = 2^{64}$) may be seen as a causal function $(A \times 2)^\omega \to A^\omega$, where the second input 2 corresponds to an enabling signal stating whether the incoming value on the first component ought be written in memory or be ignored at a given clock tick.*

Given a dummy initial value $a_0 \in A$, this behaviour may be implemented as a Mealy machine with state-space A, initial state a_0 and the transition function $\partial : (A \times 2) \times A \to A \times A$ defined as

$$\partial((a, b), q) := \begin{cases} (q, q) & \text{if } b = 0 \\ (a, a) & \text{otherwise} \end{cases}$$

For $A = 2$ and $a_0 = 0$, this machine may be represented as follows



[3]The situation is exactly the same as with finite-state deterministic automata: minimality is both in the sense of number of states and initiality with-respect to homomorphisms; the notion of homomorphism of Mealy machines shall not detain us here.

$\mathsf{MSO}(\omega)$ is a logic which ostensibly describes sets of integers $X \in \mathcal{P}(\mathbb{N})$, but those can also be regarded as *streams* 2^ω. Therefore, given alphabets $A = 2^k$ and $B = 2^n$ which are powers of 2, it is possible to write MSO formulas $\varphi(X_0, \dots, X_{k-1}, Y_0, \dots, Y_{n-1})$ regarded as input-output specifications for Mealy machines.

Example 1.3.5. *Expanding on Example 1.3.4, one may consider the following specification: if from some point on the write signal is never set to* 1*, then the output of the register stays the same. This may be rendered by the following formula $\varphi(X_0, X_1, Y_0)$, which can be written in first-order logic and a fortiori $\mathsf{MSO}(\omega)$.*

$$\forall n \in \mathbb{N}\ ((\forall k \in \mathbb{N}\ (k \geq n \Rightarrow k \notin X_1)) \ \Rightarrow\ \forall k\ \ (k \geq n \Rightarrow (k \in Y_0 \Leftrightarrow n \in Y_0)))$$

1.4 Model-checking and synthesis

A first natural problem for automatic verification is the following *model-checking* problem: is there an algorithm which, taking as input a (code of a) Mealy machine $\mathcal{M} : 2^k \to 2^n$ and an input-output specification $\varphi(X_0, \dots, X_{k-1}, Y_0, \dots, Y_{n-1})$ determines whether $\mathcal{M}$ satisfy the specification ? That is, is it the case that for every word $i = \langle i_0, \dots, i_{k-1} \rangle \in (2^k)^\omega$ and $o = \langle o_0, \dots, o_{n-1} \rangle \in (2^n)^\omega$ such that $[\![\mathcal{M}]\!](i) = o$ we also have $\varphi(i_0, \dots, i_{k-1}, o_0, \dots, o_{n-1})$?

The answer of this question is *yes* for $\mathsf{MSO}(\omega)$ specifications. One basic idea is to translate the specification φ to a suitable non-deterministic Büchi automaton $\mathcal{A}_\varphi : 2^{k+n}$. Then one may consider using the following substitution lemma for Mealy machine and automata.

Lemma 1.4.1. *Given an automaton $\mathcal{A} = (Q_\mathcal{A}, I_\mathcal{A}, \Delta_\mathcal{A}, \Omega_\mathcal{A}) : B$ and a Mealy machine $\mathcal{M} = (Q_\mathcal{M}, q^\iota_\mathcal{M}, \delta_\mathcal{M}) : A^\omega \to B^\omega$, then the automaton $\mathcal{M}^*\mathcal{A} = (Q_\mathcal{A} \times Q_\mathcal{M}, I_\mathcal{A} \times \{q^\iota_\mathcal{M}\}, \Delta_{\mathcal{M}^*\mathcal{A}}, \pi_1(\Omega_\mathcal{A})) : A$ with*

$$((q, r), a, (q', r')) \in \Delta_{\mathcal{M}^*\mathcal{A}} \Leftrightarrow (q, \pi_1(\delta_\mathcal{M}(a, r)), q') \wedge \pi_2(\delta_\mathcal{M}(a, r)) = r'$$

recognizes those words $w \in A^\omega$ such that $[\![\mathcal{M}]\!](w) \in \mathcal{L}(\mathcal{A})$. Clearly, if $\mathcal{A}$ is a Büchi/parity/Muller automaton, so is $\mathcal{M}^*\mathcal{A}$. Furthermore, if $\mathcal{A}$ is deterministic, so is $\mathcal{M}^*\mathcal{A}$.

If we want to check the machine $\mathcal{M} : (2^k)^\omega \to (2^n)^\omega$ against the specification φ, one way to do it would be to consider the Mealy machine $\mathcal{M}' : (2^k)^\omega \to (2^{k+n})^\omega$ which corresponds to the pairing of $[\![\mathcal{M}]\!]$ with the identity function $(2^k)^\omega \to (2^k)^\omega$. At this point, we know that $\mathcal{M}$ behaves according to the specification φ if and only if the language of $\mathcal{M}'^*\mathcal{A}_\varphi$ is universal. Therefore, it suffices to complement this latest automaton and check emptiness (as described in Proposition 1.1.4) to decide whether $\mathcal{M}$ respects the specification φ.

A further, more ambitious problem, is the *synthesis problem*: is there an algorithm taking as input an input-output specification $\varphi(X_0, \dots, X_{k-1}, Y_0, \dots, Y_{n-1})$ and decides whether or not there exists a Mealy machine $\mathcal{M} : 2^k \to 2^n$ satisfying the specification? Furthermore could this algorithm return a code for $\mathcal{M}$ when such a machine exists?

This question was originally raised by Church [16] and resolved positively by Büchi and Landweber in [13], building on McNaughton's theorem. In a nutshell, the modern understanding of the Büchi-Landweber theorem goes as follows: take a *deterministic* parity automaton $\mathcal{A}_\varphi : 2^{k+n}$ corresponding to the formula φ. Then, define a game on a graph derived from $\mathcal{A}_\varphi$ by replacing every transition by two steps: the universal player O gives a letter $a \in 2^k$, meant as an input and the existential player P answers with a letter $b \in 2^n$. Pairing those two letters gives a letter $\langle a, b \rangle \in 2^{k+n}$, which is used to fire a transition of the automaton. We then say that P wins if and only if the induced run in $\mathcal{A}_\varphi$ is accepting. The definition of the game is set up so that $\exists$ wins if and only if there exists a causal function $2^k \to 2^n$ agreeing with the specification. Then one may use the effective positional determinacy of parity games proved by Emerson and Juta [22]: given the game graph, we may decide who wins, and compute a positional winning strategy. If P wins, then it means that this winning strategy may be seen as a Mealy machine $\mathcal{M} : 2^k \to 2^n$ satisfying the specification φ; otherwise, O wins and no such function exists. The finite-state aspect is given by positionality: $\mathcal{M}$ can be taken to have no more states than $\mathcal{A}_\varphi$. This means in particular that positional determinacy implies that, for any $\mathsf{MSO}(\omega)$ specification, if there is *any* causal function meeting the specification, then there exists a finite-state causal function meeting the same specification.

Chapter 2

Mealy machines and MSO

The goal of this chapter is to present preliminary material which will guide our attempts at giving constructive counterparts to $\mathsf{MSO}(\omega)$. Section 2.1 is dedicated to the proving elementary properties of the category of functions generated by finite-state Mealy machines, as well as some closure properties. Section 2.2 is dedicated to rephrasing $\mathsf{MSO}(\omega)$ as a first-order theory of equality between streams with terms for Mealy machines, which we call FOM. It is shown that the expressive power of $\mathsf{MSO}(\omega)$ and FOM are the same, which will allow us to only consider FOM in the sequel. The main reason for this shift is that having terms for f.s. Mealy machine, our would-be notion of effective function within FOM means that it is amenable to a more pleasant constructivization than if starting from the language of $\mathsf{MSO}(\omega)$.

2.1 The category Mealy of Mealy machines

We now give a few structural properties of the class of finite-state causal functions. First, we show in Subsection 2.1.1 that they may be arranged in a category Mealy admitting cartesian products and a parametric fixpoint operator. but no cartesian-closure, Then, Subsection 2.1.2 is devoted to showing that these basic properties, together with the faithful embedding of the category of non-empty finite sets into Mealy, actually give rise to an extensionally complete term syntax for Mealy machines. Furthermore, this term syntax admits a natural equational theory, which may be shown to be sound and complete for atomic equations.

While the basic properties given in Subsection 2.1.1 are going to play a major rôle in building realizability models, Subsection 2.1.2 is not required for the sequel. Its main purpose is to suggest that an elementary term syntax could be used when defining later systems such as FOM and that the rather brutal equational axiomatization of equality for FOM terms could have been given a more elementary presentation.

2.1.1 Basic properties

First, to arrange finite-state causal functions into a category, we first need to show that they are closed under composition.

Lemma 2.1.1. *Finite-state causal functions are closed under composition.*

Proof. Let $\mathcal{M}_1 = (Q_1, q_1^\iota, \partial_1) : A^\omega \to B^\omega$ and $\mathcal{M}_2 = (Q_2, q_2^\iota, \partial_2) : B^\omega \to C^\omega$ be two Mealy machines. The composition of the underlying causal functions is computed by the machine

$$\mathcal{M}_2 \circ \mathcal{M}_1 = (Q_1 \times Q_2, (q_1^\iota, q_2^\iota), \partial_{2\circ 1})$$

where $\partial_{2\circ 1}$ is computed as the composite

$$A \times Q_{2\circ 1} \cong (A \times Q_1) \times Q_2 \xrightarrow{\partial_1 \times \mathrm{id}} (B \times Q_1) \times Q_2 \cong (B \times Q_2) \times Q_1 \xrightarrow{\partial_2 \times \mathrm{id}} (C \times Q_2) \times Q_1 \cong C \times Q_{2\circ 1}$$

where $Q_{2\circ 1} = Q_1 \times Q_2$ and $\cong$ denotes the obvious isomorphism induced by cartesian products. □

Definition 2.1.2. *Call* Mealy *the following category:*

- *Objects are non-empty finite sets. When $A \in \mathbf{FinSet}_{\geq \mathbf{1}}$, we most often write A^ω for A seen as an object of* Mealy.

- *Morphisms from A^ω to B^ω are finite-state causal functions $A^\omega \to B^\omega$.*

Example 2.1.3. *There is a functor $(-)^\omega : \mathbf{FinSet}_{\geq \mathbf{1}} \to \mathsf{Mealy}$, obtained as the identity on objects and by mapping the functions pointwise on streams. Since all the causal functions in its image may be implemented by single-state Mealy machines, we often call them* memoryless.

Lemma 2.1.4. Mealy *has all cartesian products. Furthermore, $(-)^\omega : \mathbf{FinSet}_{\geq \mathbf{1}} \to \mathsf{Mealy}$ preserves, reflects and create this cartesian structure.*

Proof. As expected from the statement, the cartesian product of objects is merely the cartesian product of alphabets. and the projections are given by the pointwise lifting of projections by $(-)^\omega$. Given two machines

$$\begin{array}{rcl} \mathcal{M} & = & (Q_\mathcal{M}, q^\iota_\mathcal{M}, \partial_\mathcal{M}) \quad : \quad A \to B \quad \text{and} \\ \mathcal{N} & = & (Q_\mathcal{N}, q^\iota_\mathcal{N}, \partial_\mathcal{N}) \quad : \quad A \to C \end{array}$$

the pairing is implemented as

$$\langle \mathcal{M}, \mathcal{N} \rangle \quad = \quad (Q_\mathcal{M} \times Q_\mathcal{N}, (q^\iota_\mathcal{M}, q^\iota_\mathcal{N}), \partial_{\langle \mathcal{M}, \mathcal{N} \rangle}) \quad : \quad A^\omega \to B^\omega \times C^\omega$$

where $\partial_{\langle \mathcal{M}, \mathcal{N} \rangle}$ is defined as the composition of

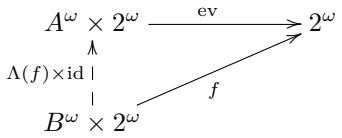
$$A \times (Q_\mathcal{M} \times Q_\mathcal{N}) \xrightarrow{\quad d \quad} (A \times Q_\mathcal{M}) \times (A \times Q_\mathcal{N}) \xrightarrow{\partial_\mathcal{M} \times \partial_\mathcal{N}} (B \times Q_\mathcal{M}) \times (C \times Q_\mathcal{N})$$

with the obvious isomorphism $(B \times Q_\mathcal{M}) \times (C \times Q_\mathcal{N}) \cong (B \times C) \times (Q_\mathcal{M} \times Q_\mathcal{N})$, taking $d = \langle \langle \pi_1, \pi_1 \circ \pi_2 \rangle, \langle \pi_1, \pi_2 \circ \pi_2 \rangle \rangle$. It is then straightforward to check that $[\![\langle \mathcal{M}, \mathcal{N} \rangle]\!]$ is the unique causal function satisfying the expected universal property. □

Since $(-)^\omega$ reflects cartesian products, we shall sometimes abusively write $A^\omega \times B^\omega$ for the cartesian product in Mealy which is formally defined as $(A \times B)^\omega$ in the sequel.

Proposition 2.1.5. Mealy *is not cartesian-closed.*

Proof. Suppose that $\mathcal{M}$ has an exponential object $(2^\omega)^{2^\omega}$, i.e. that there exists a finite alphabet A, some evaluation map $\mathrm{ev} : A^\omega \times 2^\omega \to 2^\omega$ such that, for every B and $f : B^\omega \times 2^\omega \to 2^\omega$, there exists a unique $\Lambda(f)$ such that the following commute.



In particular, it means this must be true when B^ω is the terminal object. Instantiating the universal property above and recalling that the set of infinite words 2^ω is isomorphic to the set of morphisms $1^\omega \to 2^\omega$ in Mealy, this means that for every $f : 2^\omega \to 2^\omega$ there is a unique word $w \in A^\omega$ such that, for every $x \in 2^\omega$, we have $\mathrm{ev}(\langle w, x \rangle) = f(x)$.

Suppose that it is the case. It means that we have a Mealy machine $\mathcal{E} = (Q, q^\iota, \partial) : A \times 2 \to 2$ implementing ev. Let $f = \mathbf{cons}^n_0$, for $n \geq |Q|$. By the universal property, there is a word $w \in A^\omega$ such that $\mathrm{ev}(\langle w, x \rangle) = \pi_2 \circ \partial^*(\langle w, x \rangle) = f(x)$ for all $x \in 2^\omega$. Define $\underline{k} \in 2^\omega$ by setting $\underline{k}(m) = 1$ if and only if $m = k$. For every distinct $k < k' \leq n$, we have $f(\underline{k})(n+k) \neq f(\underline{k'})(n+k)$ while $f(\underline{k})(m) = f(\underline{k'})(m)$, for each $m < n+k$. By definition of ∂^*, this must mean that $\partial^*(\langle w, \underline{k} \rangle)(m) \neq \partial^*(\langle w, \underline{k'} \rangle)(m)$ for $m \in [\![k', n+k-1]\!]$. Then, since

$$\partial^*(\langle w, \underline{k} \rangle)(n) = f(\underline{k})(n) = 0 = f(\underline{k'})(n) = \partial^*(\langle w, \underline{k'} \rangle)(n)$$

we must have $\pi_1(\partial^*(\langle w, \underline{k} \rangle)(n))$ pairwise distinct when $k \in [\![0, n]\!]$. This means that $|Q| > n$, which is a contradiction. □

A crucial fact we shall use later on when considering the composition of finite-state strategies in games is that Mealy machines are closed under a *guarded parametric fixpoint operator*. This fixpoint operator is essentially adapted from guarded λ-calculus [7] and corresponds intuitively to a definition using a feedback loop: when defining a Mealy machine, since the output alphabet is finite, one may without loss of generality suppose that the internal state of the machine recalls the last output and make the next transition depend on that output. This is formalized by the next lemma.

Lemma 2.1.6. Mealy *has guarded parametric fixpoints in the following sense: for any alphabet A, B, for any letter $b \in B$, there is a unique functional*

$$\mathbf{fix}_b : [A^\omega \times B^\omega, B^\omega]_{\mathsf{Mealy}} \to [A^\omega, B^\omega]_{\mathsf{Mealy}}$$

such that, for any finite-state causal $f : A^\omega \times B^\omega \to B^\omega$, we have

$$\mathbf{fix}_b(f) = f \circ \langle \mathrm{id}, \mathbf{cons}_b \circ \mathbf{fix}_b(f) \rangle \qquad (*)$$

Proof. Let $\mathcal{M} = (Q, q^\iota, \partial) : A \times B \to B$ be a Mealy machine and $b_0 \in B$. $\mathbf{fix}_{b_0}(\mathcal{M}) = (Q \times B, (q^\iota, b_0), \partial_{\mathbf{fix}_{b_0}(\mathcal{M})})$ has the following transition function:

$$\partial_{\mathbf{fix}_{b_0}(\mathcal{M})}((q, b), a) = (\partial(q, (a, b)), \pi_2(\partial(q, (a, b))))$$

We can check that $\mathbf{fix}_{b_0}(\mathcal{M})$ satisfies.

$$\partial^*_{\mathbf{fix}_{b_0}(\mathcal{M})} = \partial^* \circ \langle \mathrm{id}, \mathbf{cons}_b \circ \pi_2 \circ \partial^*_{\mathbf{fix}_{b_0}(\mathcal{M})} \rangle$$

This establishes that $\mathbf{fix}_{b_0}$ satisfying equation $(*)$ exists. As for uniqueness, the unicity of h such that

$$h = f \circ \langle \mathrm{id}, \mathbf{cons}_b \circ h \rangle \qquad (*)$$

is given by showing that the induced family of functions $A^n \to B$ □

This fixpoint construction is slightly confused by the necessary addition of an initial letter b to the **fix** combinator, which does not appear to be a genuine fixpoint combinator! This can be remedied by considering a notion of "productive" causal function occurring naturally when composing Mealy machines.

Definition 2.1.7. *An* eager *causal function $f : A^\omega \to B^\omega$ is a function such that $f(u)_n = f(v)_n$ whenever $u_i = v_i$ for every $i < n$.*

Example 2.1.8. *A typical eager function is $\mathbf{cons}_a$ for some $a \in A$.*

Lemma 2.1.9. *For any causal function $h : A^\omega \times C^\omega \to B^\omega$ and eager causal $f : B^\omega \to C^\omega$, there exists a unique causal function $s : A^\omega \to B^\omega$ such that*

$$s = h \circ \langle \mathrm{id}, f \circ s \rangle$$

Furthermore, if h and f are finite-state, then s is also finite-state.

It is useful to note that the degenerate case of Lemma 2.1.9 where $A = 1$ corresponds to the definition of definition of a single infinite word by recursion. In that case, the statement simplifies considerably, as the intermediate alphabet C no longer needs to be introduced.

Corollary 2.1.10. *Given an eager causal function $f : A^\omega \to A^\omega$, there is a unique word w such that $f(w) = w$.*

2.1.2 A term syntax for Mealy machines

It turns out that the morphisms in Mealy can be generated by taking memoryless functions, *guarded parametric fixpoints* and closing under composition. The objective of this section is to make this observation formal by giving a term language for f.s. causal functions and an inductive congruence relation coinciding with the equality in the semantics.

Concretely, it means that the morphisms of the category Mealy may be generated by the grammar $\mathtt{t}, \mathtt{u} ::= \mathtt{u} \circ \mathtt{t} \mid f^\omega \mid \mathbf{fix}_{b_0}(\mathtt{t})$, where f ranges over finite functions between alphabets and b_0 is an element of some alphabet. In the sequel we consider only terms which are well-typed according to the three typing rules in Figure 2.1

We could have an effective interpretation of this term syntax into *machines* thanks to Lemmas 2.1.1 and 2.1.6. Let us also write $[\![\mathtt{t}]\!]$ for the underlying finite-state denoted by the term $\mathtt{t}$.

Lemma 2.1.11. *For every Mealy machine $\mathcal{M} = (Q, q^\iota, \partial) : A^\omega \to B^\omega$ and $b \in B$, we have*

$$[\![\mathcal{M}]\!] = [\![\pi_1^\omega \circ \mathbf{fix}_{(b, q^\iota)}((\partial \circ (\mathrm{id} \times \pi_2))^\omega)]\!]$$

$$\frac{f : A \to B \quad \text{in } \mathbf{FinSet}_{\geq \mathbf{1}}}{f^\omega : A^\omega \to B^\omega} \qquad \frac{\mathtt{t} : A^\omega \to B^\omega \qquad \mathtt{u} : B^\omega \to C^\omega}{\mathtt{u} \circ \mathtt{t} : A^\omega \to B^\omega} \qquad \frac{\mathtt{t} : A^\omega \times B^\omega \to B^\omega \qquad b_0 \in B}{\mathbf{fix}_{b_0}(\mathtt{t}) : A^\omega \to B^\omega}$$

$$\frac{i \in \{1,2\}}{\pi_i : A_1^\omega \times A_2^\omega \to A_i^\omega} \qquad \frac{t : A^\omega \to B^\omega \qquad u : A^\omega \to C^\omega}{\langle u, t\rangle : A^\omega \to B^\omega \times C^\omega} \qquad \frac{a \in A}{\mathbf{cons}_a : A^\omega \to A^\omega} \qquad \frac{}{\mathrm{id} : A^\omega \to A^\omega}$$

Figure 2.1: Typed term syntax for Mealy machines.

Proof. There is a simulation from the machine obtained by interpreting the syntax thanks to Lemmas 2.1.1 and 2.1.6, namely[1]

$$\mathcal{M}' = (B \times Q, (b, q^\iota), \partial') : A^\omega \to B^\omega \text{ with } \partial'(a,(b,q)) = \partial(a,q)$$

to $\mathcal{M}$ induced by the second projection on states.

(Note that this illustrate that the syntax does not readily interpret to representation of *minimal* Mealy machines for a given finite-state causal function) □

While this is enough syntax to define arbitrary morphisms, it is helpful to consider additional constructs in order to discuss the equational theory of such terms. We thus consider additionally consider:

- a pairing $\langle \mathtt{t}, \mathtt{u}\rangle$ construct and projections π_1 and π_2 corresponding to the cartesian structure. By Lemma 2.1.4, projections are given by memoryless morphisms. On the other hand, while they do preserve memoryless morphisms, pairings $\langle \mathtt{t}, \mathtt{u}\rangle$ are memoryless memoryless if and only if $\mathtt{t}$ and $\mathtt{u}$ are. A concrete syntactic representation of $\langle t, u\rangle$ in terms of the three basic syntactic constructions may be computed by combining Lemma 2.1.11 and 2.1.4, but there is a direct syntactic way by recursion over t and u, which produces a term of linear size.
- terms implementing the morphisms $\mathbf{cons}_a$, which is helpful to characterize the guarded fixpoint operator. It may be implemented as $\pi_2^\omega \circ \mathbf{fix}_{(a,a)}((\mathrm{id} \times \pi_1)^\omega)$.

These additional constructions are also typed; we also give the derived typing rules on the second line of Figure 2.1. We are now ready to give a sensible equational theory over typed terms.

Definition 2.1.12. *Let $\equiv$ be the least congruence relation over terms satisfying the clauses presented in Figure 2.2. Being a congruence means that $\equiv$ should also satisfy the following*

$$\frac{\mathtt{t} \equiv \mathtt{u}}{\mathbf{fix}_{b_0}(\mathtt{t}) \equiv \mathbf{fix}_{b_0}(\mathtt{u})} \qquad \frac{\mathtt{t} \equiv \mathtt{t}' \qquad \mathtt{u} \equiv \mathtt{u}'}{\mathtt{u} \circ \mathtt{t} \equiv \mathtt{u}' \circ \mathtt{t}'} \qquad \frac{\mathtt{t} \equiv \mathtt{t}' \qquad \mathtt{u} \equiv \mathtt{u}'}{\langle \mathtt{u}, \mathtt{t}\rangle \equiv \langle \mathtt{u}', \mathtt{t}'\rangle}$$

It is easy to check that $\equiv$ is sound with respect to the interpretation $[\![-]\!]$ of terms as f.s. causal functions.

Theorem 2.1.13 (Soundness)**.** *Letting $\equiv$ be the smallest congruence including the clauses of Figure 2.2. For arbitrary Mealy terms $\mathtt{t}$ and $\mathtt{u}$, we have*

$$\mathtt{t} \equiv \mathtt{u} \qquad \Rightarrow \qquad [\![\mathtt{t}]\!] = [\![\mathtt{u}]\!]$$

Proof. Straightforward induction on the derivation of $\mathtt{t} \equiv \mathtt{u}$. □

The converse is also provable, although the proof is more involved. Because it is not required for the sequel, so we only give an outline. The full argument is rather elementary, but several technicalities arise; we thus refer the interested reader to a full formalization of this proof we carried out in the proof assistant Coq [55].

Theorem 2.1.14 (Completeness)**.** *Letting $\equiv$ be the smallest congruence including the clauses of Figure 2.2. For arbitrary Mealy terms $\mathtt{t}$ and $\mathtt{u}$, we have*

$$[\![\mathtt{t}]\!] = [\![\mathtt{u}]\!] \qquad \Rightarrow \qquad t \equiv u$$

Proof sketch. The general proof strategy goes as follows:

[1] Up to obvious isomorphism.

Categorical structure

$$\begin{array}{lcl} \mathrm{id} \circ f & \equiv & f \\ f \circ \mathrm{id} & \equiv & f \\ (f \circ g) \circ h & \equiv & f \circ (g \circ h) \end{array}$$

Cartesian products

$$\begin{array}{lcl} \pi_1 \circ \langle f, g \rangle & \equiv & f \\ \pi_2 \circ \langle f, g \rangle & \equiv & g \\ \langle \pi_1, \pi_2 \rangle & \equiv & \mathrm{id} \end{array}$$

Inclusion $(-)^\omega : \mathbf{FinSet} \to \mathsf{Mealy}$

$$\begin{array}{lcl} f^\omega \circ g^\omega & \equiv & (f \circ g)^\omega \\ \pi_1^\omega & \equiv & \pi_1 \\ \pi_2^\omega & \equiv & \pi_2 \end{array}$$

Guarded fixpoints

$$\begin{array}{lcl} \mathbf{fix}_b(f) & \equiv & f \circ \langle \mathrm{id}, \mathbf{cons}_b \circ \mathbf{fix}_b(f) \rangle \\ f^\omega \circ \mathbf{cons}_a & \equiv & \mathbf{cons}_{f(a)} \circ f^\omega \end{array}$$

Uniqueness of guarded fixpoints

$$\frac{h \equiv f \circ \langle \mathrm{id}, \mathbf{cons}_b \circ \mathbf{fix}_b(f) \rangle}{h \equiv \mathbf{fix}_b(f)}$$

Figure 2.2: The equational theory of finite-state causal functions.

- First, one may internalize Lemma 2.1.11 by showing that for every term $\mathtt{t} : A^\omega \to B^\omega$, there exists an alphabet C, and a function $f : A \times (B \times C) \to (B \times C)$ such that $\mathtt{t}' \equiv \pi_2 \circ \mathbf{fix}_{(b,c)}(f^\omega)$ for arbitrary $(b, c) \in B \times C$. This is done by induction over t and requires to derive a number of naturality lemmas concerning **fix** and $\equiv$ from the unicity axiom. Let us for instance mention the nesting of fixpoints

$$\mathbf{fix}_{b_0}(\mathbf{fix}_{b_1}(\mathtt{t})) \equiv \mathbf{fix}_{(b_0,b_1)}(\langle \mathrm{id}, \mathrm{id} \rangle \circ \mathtt{t} \circ \langle \langle \pi_1, \pi_1 \circ \pi_2 \rangle, \pi_2 \circ \pi_2 \rangle$$

- Then, one may reduce the problem to the completeness for equality of fixpoints of terms $\mathbf{fix}_b(\mathtt{t}) \equiv \mathbf{fix}_b(\mathtt{u})$ with $[\![\mathtt{t}]\!]$ and $[\![\mathtt{u}]\!]$ memoryless. Formally (and leaving alphabets implicit), it means that for any quadruple $(f_1^\omega, f_2^\omega, g_1^\omega, g_2^\omega)$ of memoryless terms and constants a and b, there exists a constant c and memoryless terms v^ω and w^ω such that

$$[\![f_1^\omega \circ \mathbf{fix}_a(f_2^\omega)]\!] = [\![g_1^\omega \circ \mathbf{fix}_b(g_2^\omega)]\!] \quad \Rightarrow \quad [\![\mathbf{fix}_c(v^\omega)]\!] = [\![\mathbf{fix}_c(w^\omega)]\!]$$

  and

$$\mathbf{fix}_c(v^\omega) \equiv \mathbf{fix}_c(w^\omega) \quad \Rightarrow \quad f_1^\omega \circ \mathbf{fix}_a(\mathtt{f}_2^\omega) \equiv \mathtt{g}_1^\omega \circ \mathbf{fix}_b(g_2^\omega)$$

- Finally, define $\mathsf{Reach}(f, b)$ for arbitrary functions $f : \Sigma \times \Gamma \to \Gamma$ and $b \in \Gamma$ as the least set containing b and such that, if $b' \in \mathsf{Reach}(f, b)$ and $a \in \Sigma$, then $f(a, b') \in \mathsf{Reach}(f, b)$. Then it is straightforward to check that, for arbitrary $f, g : \Sigma \times \Gamma \to \Gamma$, if the set $X = \mathsf{Reach}(f, b)$ coincide with $\mathsf{Reach}(g, b)$ and $f\big|_{\Sigma \times X} = g\big|_{\Sigma \times X}$ if and only if $[\![\mathbf{fix}_b(f^\omega)]\!] = [\![\mathbf{fix}_b(g^\omega)]\!]$. This characterization allow to show that $\mathbf{fix}_b(f^\omega) \equiv \mathbf{fix}_b(g^\omega)$ by considering explicitly the map of alphabet $i : X \to \Gamma$ induced by the inclusion $X \subseteq \Gamma$ and an arbitrary retract $r : \Gamma \to X$; one shows that $\mathbf{fix}_b(f^\omega) \equiv i^\omega \circ \mathbf{fix}_b((r \circ f \circ (\mathrm{id} \times i))^\omega)$ within the equational theory thanks to the unicity of fixpoints. The aforementioned characterization then tells us that $r \circ f \circ (\mathrm{id} \times i) = r \circ g \circ (\mathrm{id} \times i)$, which allows to conclude.

□

2.2 Rephrasing MSO(ω) as a first-order equational theory of streams

The objective of this section is to show that the classical theory $\mathsf{MSO}(\omega)$ may be viewed as a multi-sorted first-order theory of equality between streams allowing term formers for every f.s. functions, which we dub FOM. Once the equivalence between $\mathsf{MSO}(\omega)$ and FOM is firmly established, we shall abandon the official definition of $\mathsf{MSO}(\omega)$ in our quest for a Curry-Howard account of Church's

synthesis. While this might appear as a rather frivolous aesthetic concern, there are several advantages to moving from $\mathsf{MSO}(\omega)$ to FOM. For one, having terms for every Mealy machine allows for having a system where every potential witness is implicitly given using the $\exists$-intro rule of natural deduction. Without such terms, the alternative would be to encode their existence in the axiomatization[2]. This move also stresses that the only basic objects we are interested in from a semantic perspectives are really infinite words A^ω seen as streams. Finally, the term language of FOM is also a better starting point to suggest higher-order extensions.

We first give the formal definition of FOM as a multi-sorted first-order logic. Then, we proceed to show how to interpret $\mathsf{MSO}(\omega)$ into FOM and vice-versa at the semantic level. Lastly, we show that we may adapt Siefkes' axiomatization of $\mathsf{MSO}(\omega)$ to FOM and get a complete axiomatization of the latter [3].

Formally speaking, the exact details of the equivalence between $\mathsf{MSO}(\omega)$ and FOM are not necessary to read subsequent chapter; only the definition of the language FOM and the existence of a recursive complete axiomatization thereof are needed.

2.2.1 Formal preliminaries

Multi-sorted first-order logic We briefly review the basic formalism of multi-sorted first-order logic with terms and relations in order to fix some notations.

Definition 2.2.1. *A signature $\Sigma = (\mathcal{S}, \mathcal{T}, \mathcal{R})$ for many-sorted logic consists of:*

- *A set $\mathcal{S}$ of base sorts τ, σ.*
- *A set $\mathcal{T}$ of constant symbols $\mathtt{t}$ together with arities, i.e. to each constant symbol is attached a non-empty list of sorts $(\tau_1, \dots, \tau_k; \sigma)$.*
- *A set $\mathcal{R}$ of predicate symbols together with arities, i.e to each predicate symbol is attached a list of sorts $(\tau_1, \dots, \tau_k)$.*

The set of terms of sort $(\tau_1, \dots, \tau_k; \sigma)$ is defined by simultaneous induction, assuming that they each come implicitely with an ordered set of k variables $x_1, \dots, x_k$ of respective sort $\tau_1, \dots, \tau_k$:

- *a variable x_i is a term of arity $(\tau_1, \dots, \tau_k; \tau_i)$*
- *for every term $\mathtt{t}(y_1, \dots, y_n)$ of arity $(\sigma_1, \dots, \sigma_n; \sigma)$ and terms $\mathtt{u}_i(x_1, \dots, x_k)$ of respective arities $(\tau_1, \dots, \tau_k; \sigma_i)$ for $1 \leq i \leq n$, there is a term $\mathtt{t}(\mathtt{u}_1(x_1, \dots, x_k), \dots, \mathtt{u}_n(x_1, \dots, x_k))$ of arity $(\tau_1, \dots, \tau_k; \sigma)$.*

Substitution of terms and α-equivalence are then defined as usual. Given a term $\mathtt{t}$ of arity $(\tau_1, \dots, \tau_k; \sigma)$, a variable of sort τ_m for $1 \leq m \leq k$ and a term $\mathtt{u}$ of arity $(\tau_1, \dots, \tau_{m-1}, \tau_{m+1}, \dots \tau_k; \tau_m)$, write $\mathtt{t}[\mathtt{u}/x]$ for the substituted term of arity $(\tau_1, \dots, \tau_{m-1}, \tau_{m+1}, \dots \tau_k; \sigma)$.

Given a multisorted signature Σ, we may define the language $\mathsf{FO}_=(\Sigma)$ of first-order formulas with equality over Σ.

Definition 2.2.2. *Given an arbitrary signature Σ the language of* first-order logic of equality *over Σ ($\mathsf{FO}_=(\Sigma)$) is defined as follows:*

$$\varphi, \psi ::= \quad \mathtt{t} = \mathtt{u} \mid R(\mathtt{t_1}, \dots, \mathtt{t_k}) \mid \bot \mid \top \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \varphi \Rightarrow \psi \mid \forall y^B \varphi(y^B) \mid \exists y^B \varphi(y^B)$$

where

- *$\mathtt{t}$, $\mathtt{u}$ are terms of a common arity $(\tau_1, \dots, \tau_m; \sigma)$ over Σ*
- *$\mathtt{t_i}$ is a term of arity $(\tau_1, \dots, \tau_m; \sigma_i)$ over Σ*
- *R is a relation symbol of arity $(\sigma_1, \dots, \sigma_k)$.*

[2] We took such an approach in [56] where we stuck to the official language of $\mathsf{MSO}(\omega)$ as a subsystem of second-order arithmetic. While it gave a rather nice characterization of the admissible instances of the instance of comprehensions of $\mathsf{MSO}(\omega)$ which still allowed to extract synchronous functions, sticking to a language close to $\mathsf{MSO}(\omega)$ had another drawback besides necessitating the usual automata-theoretic encoding of the notion of synchronous transducers: extracting terms for the more natural restriction of comprehension axiom required non-elementary complexity. Even then, we needed to work with a purely relational variant of $\mathsf{MSO}(\omega)$.

[3] Said axiomatization mostly arise as a translation of Siefkes' axiomatization of $\mathsf{MSO}(\omega)$ as a subsystem of second-order arithmetic, and is thus arguably not too elegant with respect to the language of FOM. Moreover the existence of some complete recursive axiomatization FOM is trivial since the logic may be shown to be decidable without going through $\mathsf{MSO}(\omega)$.

The arity of a formula φ is the ordered list $(\tau_1, \dots, \tau_k)$ of the sort of the free variables occuring in φ. Substitution and α-renaming are defined as usual by recursion over the formula. A formula with no free variables is henceforth called a sentence*.*

While more general notions of model for the language of $\mathsf{FO}_=(\Sigma)$ encompassing constructive semantics is going to be given in Chapter 5, we only need the basic notion of *Tarski model* for multi-sorted signatures Σ for now. Given a Tarski model M over some signature Σ and a $\mathsf{FO}_=(\Sigma)$ sentence φ, we write $M \models \varphi$ when M satisfies φ. Two Tarski models M and M' over Σ are *elementarily equivalent* if for every sentence φ of $\mathsf{FO}_=(\Sigma)$, we have $M \models \varphi$ if and only if $M' \models \varphi$. We write $M \equiv M'$ when it is the case.

A *theory* over a signature Σ is a set of $\mathsf{FO}_=(\Sigma)$ sentences closed under deduction.

Definition of $\mathsf{MSO}(\omega)$ For the rest of this chapter, we regard $\mathsf{MSO}(\omega)$ as a multi-sorted first order logic. This is done by considering a signature with two sorts: a sort ι of individuals and a sort $\iota \to o$ of one-place predicates. There are only two terms constructors, namely $\dot{\mathsf{Z}}$ of sort $(\cdot; \iota)$ and $\dot{\mathsf{S}}$ of sort $(\iota; \iota)$ and an additional predicate $\dot{\mathsf{In}}(\mathtt{t}^\iota, X^{\iota \to o})$ intended to mean that $\mathtt{t}$ satisfies the predicate X. As is customary with MSO, we use lowercase variables to denote individuals in MSO formula and reserve uppercase for one-place predicates, so we may omit superscripts in quantifiers and formulas.

The standard model of $\mathsf{MSO}(\omega)$, which we call $\mathfrak{M}_{\mathsf{MSO}}$, is given by taking:

$$\begin{array}{llll} \mathfrak{M}_{\mathsf{MSO}}(\iota) = \mathbb{N} & \mathfrak{M}_{\mathsf{MSO}}(\iota \to o) = \mathcal{P}(\mathbb{N}) & \text{for sorts} \\ \mathfrak{M}_{\mathsf{MSO}}(\dot{\mathsf{Z}}) = 0 & \mathfrak{M}_{\mathsf{MSO}}(\dot{\mathsf{S}}) = n \mapsto n+1 & \text{for terms} \\ \mathfrak{M}_{\mathsf{MSO}}(\dot{\mathsf{In}}) = \{(n, X) \in \mathbb{N} \times \mathcal{P}(\mathbb{N}) \mid n \in X\} & & \text{for the membership relation} \end{array}$$

The theory $\mathsf{MSO}(\omega)$ is the set sentences of sentences satisfied by $\mathfrak{M}_{\mathsf{MSO}}$.

Definition of FOM The language of FOM is the language of $\mathsf{FO}_=(\Sigma_{\mathsf{Mealy}})$, taking Σ_{Mealy} to be the signature $(\mathcal{S}_{\mathsf{Mealy}}, \mathcal{T}_{\mathsf{Mealy}})$ such that

- $\mathcal{S}_{\mathsf{Mealy}}$ be the set of strictly positive natural numbers. By abuse of notation, we identify the sort n with the non-empty alphabet $\{0, \dots, n-1\}$ and rather use directly alphabets for sorts.
- there is a constant $\dot{\mathcal{M}}$ of sort $(A_1, \dots, A_k; B)$ in $\mathcal{T}_{\mathsf{Mealy}}$ for each Mealy machine

$$\mathcal{M} : A_1^\omega \times \cdots \times A_k^\omega \to B^\omega$$

The *standard model* $\mathfrak{M}^{\mathsf{Mealy}}$ of FOM is given by mapping:

- a sort A to the set A^ω of infinite words over A.
- a term $\mathtt{t}$ of arity $(A_1, \dots, A_n; B)$, that is, a Mealy machine, to the underlying f.s. causal function $A_1^\omega \times \cdots \times A_n^\omega \to B^\omega$.

The standard model is our default notion of model for $\mathsf{FO}_=(\mathsf{Mealy})$; most often, we merely write $\models_\rho \varphi$ to mean $\mathfrak{M}^{\mathsf{Mealy}} \models_\rho \varphi$. The theory FOM is set of $\mathsf{FO}_=(\mathsf{Mealy})$ sentences satisfied by $\mathfrak{M}^{\mathsf{Mealy}}$.

2.2.2 Translation from $\mathsf{MSO}(\omega)$ to FOM

Now, we want to show that $\mathsf{MSO}(\omega)$ and FOM are equivalent. To even just spell out what we mean by that, we need the classical notion of (multisorted) first-order interpretation.

Definition 2.2.3. *Given multi-sorted signatures Σ and Σ', an first-order interpretation of Σ into Σ' is given by*

- *a map $\tau \mapsto \overline{\tau}^*$ mapping sorts of Σ to tuples of sorts of Σ'.*
- *for every sort τ of Σ, a $\mathsf{FO}_=(\Sigma')$ formula $\mathrm{dom}^*_\tau(\overline{x}^{\overline{\tau}})$.*
- *for every atomic formula of $\mathsf{FO}_=(\Sigma)$ (i.e., relations of Σ and equality, possibly with terms) $R(\overline{\mathtt{t}(\overline{x})})$, a formula $R^*_{\overline{t}}(\overline{\overline{x}})$ of of $\mathsf{FO}_=(\Sigma')$, where each subtuple of free variables $\overline{x}$ in the output correspond to a single variable of the input.*

$$
\begin{array}{lcllcl}
R(\overline{\mathtt{t}(\overline{\mathtt{x}})})^* & = & R^*_{\overline{\mathtt{t}}}(\overline{x}) & \top^* & = & \top \\
\bot^* & = & \bot & (\varphi \Rightarrow \psi)^* & = & \varphi^* \Rightarrow \psi^* \\
(\varphi \wedge \psi)^* & = & \varphi^* \wedge \psi^* & (\varphi \vee \psi)^* & = & \varphi^* \vee \psi^* \\
(\forall x\ \varphi)^* & = & \forall \overline{x}^{\overline{\tau}^*}.\mathrm{dom}^*_\tau(\overline{x}) \Rightarrow \varphi^* & (\exists x\ \varphi)^* & = & \exists \overline{x}^{\overline{\tau}^*}.\mathrm{dom}^*_\tau(\overline{x}) \wedge \varphi^*
\end{array}
$$

Figure 2.3: Map of $\mathsf{FO}_=$ formulas induced by an interpretation $(-)^*$.

An interpretation $(-)^*$ of Σ into Σ' inductively gives rise to maps $\varphi \mapsto \varphi^*$, taking a formula φ over $\mathsf{FO}_=(\Sigma)$ to another formula φ^* over $\mathsf{FO}_=(\Sigma')$; the precise inductive definition, which can be summed up as "commute over every logical connective", is given in Figure 2.3. Note that this map is sound with respect to deduction if and only if the equality predicate for sort τ is mapped to a partial equivalence relation over dom^*_τ. We call such interpretations *sound*. Sound interpretations of Σ into Σ' extend to a maps $M \mapsto M^*$ taking as input a model of $\mathsf{FO}_=(\Sigma')$ and outputting a model M^* of $\mathsf{FO}_=(\Sigma)$ in the obvious way (i.e., sort τ of Σ is interpreted as the set of tuples in $\overline{\tau}^*$ satisfying dom^*_τ in M). Finally, note that interpretations compose, and that the maps of models induced by a composition of two interpretation is the same, up to isomorphism, as the composition of the induced maps of models of the induced interpretation.

The equivalence between $\mathsf{MSO}(\omega)$ and FOM will thus manifest in the form of interpretations between the respective languages of $\mathsf{MSO}(\omega)$ and FOM preserving, up to elementary equivalence, their standard model.

Lemma 2.2.4. *There are interpretations $(-)^{\dagger\bullet}$ and $(-)^*$ such that*

$$\mathfrak{M}_{\mathsf{FOM}} \equiv \mathfrak{M}^*_{\mathsf{MSO}} \qquad \mathfrak{M}_{\mathsf{MSO}} \equiv \mathfrak{M}^{\dagger\bullet}_{\mathsf{FOM}}$$

The rest of this subsection is devoted to giving a high-level description of the interpretations involved in Lemma 2.2.4.

First, we notice that the whole of the language of FOM is not going to be necessary to interpret $\mathsf{MSO}(\omega)$. We call FOM_2 the fragment of FOM where the only sort allowed is 2. This means that quantification are only allowed over words in 2^ω and that terms may only have sort $(2, \dots, 2; 2)$. Its standard model $\mathfrak{M}_{\mathsf{FOM}_2}$ is obtained by the obvious restriction of $\mathfrak{M}_{\mathsf{FOM}}$.

In the other direction, it is easier to first give an interpretation $(-)^\dagger$ of FOM into FOM_2 and then an interpretation $(-)^\bullet$ of FOM_2 into $\mathsf{MSO}(\omega)$. The interpretation of FOM into $\mathsf{MSO}(\omega)$ is then obtained as the composition of $(-)^\dagger$ and $(-)^\bullet$.

From $\mathsf{MSO}(\omega)$ to FOM_2 At the level of sorts, $(-)^*$ maps both the sort of individual ι and sets $\iota \to o$ to the sort 2^ω. The basic idea is that we have the classical isomorphism $2^\omega \simeq \mathcal{P}(\mathbb{N})$ and that the characteristic function $\mathbb{N} \to \mathcal{P}(\mathbb{N})$ is used to represent natural numbers. The other component of the interpretation $(-)^*$ are then defined using auxiliary terms and predicates of FOM given in Figure 2.4.

We take $\mathrm{dom}^*_\iota(x)$ to be the predicate $x \in \mathbb{N}$. At the level of relations, we first give a translation of terms $\mathtt{t}^*$ compatible with substitution. It is thus determined by $\dot{\mathsf{Z}}^*$, $\dot{\mathsf{S}}^*$ and its trivial action on variables. This allow to simply put

$$(\dot{\mathsf{In}}(\mathtt{t}, X))^* := \dot{\mathsf{In}}^*(\mathtt{t}^*, X) \qquad (\mathtt{t} = \mathtt{u})^* := \mathtt{t}^* = \mathtt{u}^*$$

It is straightforward to check that this interpretation gives us the elementary equivalence

$$\mathfrak{M}_{\mathsf{MSO}} \equiv \mathfrak{M}^*_{\mathsf{FOM}}$$

From FOM to FOM_2 There are several way to go about this, and the details are rather unsurprising: one essentially uses the fact that alphabets of FOM_2 are arbitrarily large and that any alphabet may be suitably interpreted in a larger alphabet.

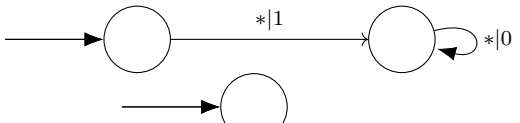
At the level of sorts, we map an alphabet $A = \{a_1, \dots, a_{|A|}\}$ the tuple $(2, \dots, 2)$ of size $|A|$. Then, consider the singleton map $\eta_A : A \to 2^A$ which maps a letter $a \in A$ to the characteristic function of $\{a\}$. The basic idea is that a word $w \in A^\omega$ should be regarded as the word $\eta_A \circ w \in (2^A)^\omega$ in the interpretation. For every sort A, there is a function $c^A : 2^A \to 2^A$ such that $c^A \circ c^A = c^A$ and $c^A(\eta_A(a)) = \eta_A(a)$; fix a choice of tuple of terms $\overline{\mathsf{c}}^A$ implementing such functions in order to define

$$\mathrm{dom}^\dagger_A(\overline{x}) = \bigwedge_{a \in A} \mathsf{c}^A_a(\overline{x}) = x_a$$

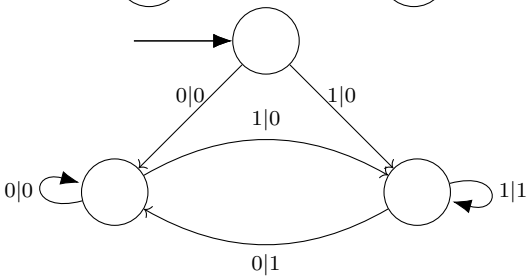
$$n \in \mathbb{N} \quad := \quad \mathbb{N}_\infty(n) =_{2^\omega} 1^\omega \wedge \neg n =_{2^\omega} 0^\omega \quad \text{for } n \text{ of sort } 2^\omega$$

and $\dot{\mathsf{In}}^*(n,x) \quad := \quad \mathtt{in}(n,x) =_{2^\omega} 1^\omega \quad \text{for } n, x \text{ of sort } 2^\omega$

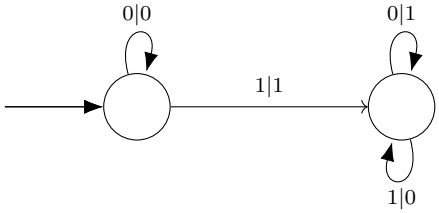
$\dot{\mathsf{Z}} = 10^\omega : 1^\omega \to 2^\omega$



$\dot{\mathsf{S}} = \mathbf{cons}_0 : 2^\omega \to 2^\omega$



$\mathbb{N}_\infty : 2^\omega \to 2^\omega$



$\mathtt{in} = (\Rightarrow)^\omega : 2^\omega \to 2^\omega$

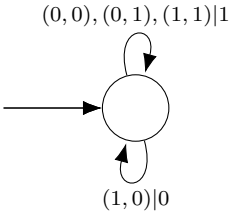


Figure 2.4: Interpretation of basic MSO terms and predicates in FOM.

For every f.s. causal function $f : A^\omega \to B^\omega$, it is rather straightforward to check that there exists a (non-canonical) function $\widetilde{f} : (2^A)^\omega \to (2^B)^\omega$ such that $\widetilde{f} \circ c^A = \widetilde{f}$ and $c^B \circ \widetilde{f} = \widetilde{f}$. Indeed, if $f = [\![\mathcal{M}]\!]$ for a Mealy machine $\mathcal{M} = (Q, q^\iota, \partial) : A^\omega \to B^\omega$, any Mealy machine $\widetilde{\mathcal{M}} = (Q, q^\iota, \widetilde{\partial})$ where $\pi_1(\widetilde{\partial}(\eta_A(a), q)) = c^B(\pi_1(\partial(a, q)))$ and $\pi_2(\widetilde{\partial}(\eta_A(a), q)) = \pi_2(\partial(a, q))$ implements $\widetilde{f}$. Fix such a choice of lifts at the level of Mealy machines. This determines a corresponding lift $\overline{\mathtt{t}}^\dagger$ at the level of terms $\mathtt{t}$, which then allows to translate the basic equality predicates by setting

$$(\mathtt{t} =_B \mathtt{u})^\dagger \quad = \quad \bigwedge_{b \in B} \mathtt{t}_b^\dagger =_2 \mathtt{u}_b^\dagger$$

It is then easy to check that this interpretation preserves the standard model up to elementary equivalence.

$$\mathfrak{M}_{\mathsf{FOM}} \quad \equiv \quad \mathfrak{M}^\dagger_{\mathsf{FOM}_2}$$

From FOM_2 to $\mathsf{MSO}(\omega)$ At the level of sort, the unique sort 2^ω of FOM_2 is simply interpreted as the sort $\iota \to o$ of $\mathsf{MSO}(\omega)$; $\mathrm{dom}^\bullet_{2^\omega}(\mathrm{x})$ is the trivial formula $\top$. We now need to give the interpretation of the equality predicate. This is done by adapting an usual pattern encapsulated by the following statement (see e.g. [71, §5.3]).

Lemma 2.2.5. *Say that a MSO formula $\varphi(X_1, \dots, X_k, n)$ represents a function $f : (2^k)^\omega \to 2^\omega$ if for every tuple of words $w_i \in 2^\omega$ and integer n $(\rho, n) \in (2^k)^\omega \times n$*

$$\mathfrak{M}_{\mathsf{MSO}} \models \varphi(w_1, \dots, w_k, n) \qquad \Leftrightarrow \qquad f(w_1 \times \cdots \times w_k) = n$$

For every finite-state function $f : (2^k)^\omega \to 2^\omega$, there is a MSO formula $\chi_f(X_1, \dots, X_k, n^\iota)$ representing f.

Proof. Let $f : (2^p)^\omega \to 2^\omega$ be induced by a Mealy machine $\mathcal{M}$. Without loss of generality, we can assume the state set of $\mathcal{M}$ to be of the form 2^q. Then f is represented by a formula of the form

$$\delta[\overline{X}, x] \quad = \quad \forall \overline{Q}, Y. \mathsf{I}(\overline{Q}) \quad \wedge \forall t \mathsf{H}(\overline{Q}, \overline{X}, Y, t) \implies Y(x) \tag{2.1}$$

The sequence of outputs of $\mathcal{M}$ is coded by the predicate variables Y, sequence of state is coded by the tuple of predicate variables $\overline{Q} = Q_1, \dots, Q_q$, Moreover, since $\mathcal{M}$ is deterministic, we can assume the formula $I(\overline{Q})$ to be of the form $\bigwedge_{1 \leq i \leq q} [Q_i(0) \Leftrightarrow \mathsf{B}_i]$ with each $\mathsf{B}_i \in \{\top, \bot\}$, and

$$\mathsf{I}(\overline{Q}) \; = \; \bigwedge_{1 \leq i \leq q} [Q_i(t) \Leftrightarrow \mathsf{B}_i] \qquad \mathsf{H}(\overline{Q}, \overline{X}, \overline{Y}, \overline{Q}, t) \quad = \quad \begin{pmatrix} \big(t \in Y \Leftrightarrow \mathsf{O}[\overline{t \in Q}, \overline{t \in X}]\big) & \wedge \\ \bigwedge_{1 \leq i \leq q} \big(\dot{\mathsf{S}}(t) \in Q_i \Leftrightarrow \mathsf{D}_i[\overline{t \in Q}, \overline{t \in X}]\big) & \end{pmatrix}$$

for some propositional formulas $\mathsf{O}[-,-], \overline{\mathsf{D}}[-,-]$ corresponding to the transition function of the underlying Mealy machine. □

We may then complete the definition of $(-)^\bullet$ by setting

$$(\mathtt{t}(\overline{x}) = \mathtt{u}(\overline{x}))^\bullet \quad := \quad \forall n^\iota. \chi_{[\![\mathtt{t}]\!]}(\overline{x}, n) \Leftrightarrow \chi_{[\![\mathtt{u}]\!]}(\overline{x}, n)$$

and Lemma 2.2.5 allows to show the desired elementary equivalence.

$$\mathfrak{M}_{\mathsf{FOM}} \quad \equiv \quad \mathfrak{M}^\bullet_{\mathsf{MSO}}$$

2.2.3 A complete axiomatization of FOM

We recall Siefkes' complete axiomatization of $\mathsf{MSO}(\omega)$ in Figure 2.5. This axiomatization is rather elegant as the axioms are exactly those of classical second-order arithmetic restricted to the language of $\mathsf{MSO}(\omega)$. By encoding these axioms into FOM and an appropriate scheme establishing correspondence with the composite translation $(-)^{\bullet *}$, we obtain a complete axiomatization of FOM_2, which is finally shown to extend to a complete axiomatization of FOM.

The target axiomatization of FOM is given in Figure 2.6. The first three are natural extension of the pure equational theory of the term language, while the other are less elegant addition to ensure completeness: the induction and the comprehension axioms of $\mathsf{MSO}(\omega)$ are encoded and atomic equalities are forced to be equivalent to their encoding in $\mathsf{MSO}(\omega)$ (notice that we use the translation $(-)^* : \mathsf{MSO}(\omega) \to \mathsf{FOM}$ in order to spell out the last axiom).

Since we rely on this translation, our first order of business is to make sure that $(-)^*$ is compatible with deduction, i.e., that $\mathsf{MSO}(\omega) \vdash \varphi$ implies that $\mathsf{FOM} \vdash \varphi$.

$\forall n\, m.\dot{\mathsf{S}}(n) = \dot{\mathsf{S}}(m) \Rightarrow n = m$ $\qquad$ $\forall n.\dot{\mathsf{S}}(n) \neq \dot{\mathsf{Z}}$

$\exists X.\forall n.n \in X \Leftrightarrow \varphi(n)$ $\qquad$ $\varphi(\dot{\mathsf{Z}}) \wedge (\forall n.\varphi(n) \Rightarrow \varphi(\dot{\mathsf{S}}(n))) \Rightarrow \forall n.\varphi(n)$

Figure 2.5: Siefkes' axiomatization of $\mathsf{MSO}(\omega)$.

Lemma 2.2.6. *Let $\overline{\varphi}$ and ψ by $\mathsf{MSO}(\omega)$ formulas with first-order variables included in $\{x_1, \ldots, x_k\}$. If the sequent $\overline{\varphi} \vdash \psi$ is derivable in $\mathsf{MSO}(\omega)$, then $\overline{\varphi^*}, x_1 \in \mathbb{N}, \ldots, x_k \in \mathbb{N} \vdash \psi^*$ is derivable in FOM.*

Proof. We formally proceed by induction over the derivation; all logical rules are straightforward as the translation commute with every propositional connective. The only contentious point concerns axioms and the rules for the existential quantification over integers. The elimination rule of $\exists$ does not pose any particular problem, but the introduction rule for integers requires to show the following

Claim. *Let $\mathtt{t}$ be a term of sort ι of $\mathsf{MSO}(\omega)$ whose set of free variables is included in $\{x\}$ (note that such a term has at most one variable of sort ι). Then, $\mathsf{FOM} \vdash x \in \mathbb{N} \Rightarrow \mathtt{t}^* \in \mathbb{N}$.*

Proof. By induction over the term $\mathtt{t}$.

- If $\mathtt{t}$ is the variable x, then this is trivial.
- For $\dot{\mathsf{Z}}$, we have $\dot{\mathsf{Z}}^* = 10^\omega$. Note that $[\![\mathbb{N}_\infty(0^\omega)]\!] = [\![1^\omega]\!]$ in the semantics, so $\mathsf{FOM} \vdash \mathbb{N}_\infty(1^\omega) = 1^\omega$. We also have $10^\omega = \mathbf{cons}_1(0^\omega) \neq \mathbf{cons}_0(0^\omega) = 0^\omega$ through the third axiom of FOM, so $\dot{\mathsf{Z}}^* \in \mathbb{N}$.
- Otherwise, for the successor case, it suffices to prove that $\mathsf{FOM} \vdash \forall x^{2^\omega}.x \in \mathbb{N} \Rightarrow \mathbf{cons}_0(x) \in \mathbb{N}$. Reasoning in FOM assume that $\mathbb{N}_\infty(x) = 1^\omega$ and $x \neq 0^\omega$. First we show $\mathbb{N}_\infty(\mathbf{cons}_0(x)) = 1^\omega$. We first have as axiom $\forall x^{2^\omega}\ \mathbb{N}_\infty(\mathbf{cons}_0(x)) = \mathbf{cons}_1(\mathbb{N}_\infty(x))$. Instantiating on x, we may then use Leibniz' rule to deduce $\mathbb{N}_\infty(\mathbf{cons}_0(x)) = \mathbf{cons}_1(1^\omega) = 1^\omega$. Thus we now only have to show that $\mathbf{cons}_0(x) \neq 0^\omega$; to this end, assume the contrary. By injectivity of $\mathbf{cons}_0$, we would deduce that $x = 0^\omega$, contradicting our hypothesis.

□

It remains to show that the translation of all axioms of $\mathsf{MSO}(\omega)$ are derivable in FOM in order to conclude.

- The translation of the injectivity of successor is

  $$\forall n^{2^\omega}.n \in \mathbb{N} \Rightarrow \forall m^{2^\omega}.n \in \mathbb{N} \Rightarrow \mathbf{cons}_0(n) = \mathbf{cons}_0(m)$$

  is easily derived from the more general axiom stating that $\mathbf{cons}_a$ is injective of FOM.
- Similarly, the translation of the axiom of non-confusion is

  $$\forall n^{2^\omega}.n \in \mathbb{N} \Rightarrow \mathbf{cons}_0(n) \neq 10^\omega$$

  is derived from the third axiom of FOM.
- The translation of the comprehension and induction axioms are axioms of FOM.

□

We now want to derive the completeness of the axiomatization FOM_2 using the completeness of Siefkes' axiomatization of $\mathsf{MSO}(\omega)$ thanks to the following result.

Lemma 2.2.7. *Let φ be a FOM_2 formula. Then, FOM proves that*

$$\varphi \quad \Leftrightarrow \quad \varphi^{\bullet *}$$

Proof. Proceed by induction over φ.

- If φ is an atomic equality $\mathtt{t}(\overline{x}) = \mathtt{u}(\overline{x})$, then FOM needs to show that

  $$\mathtt{t}(\overline{x}) = \mathtt{u}(\overline{x}) \Leftrightarrow \left(\forall n.\ \chi_{[\![t]\!]}(\overline{x}, n) \Leftrightarrow \chi_{[\![u]\!]}(\overline{x}, n)\right)^*$$

  which is precisely the last axiom of FOM.

$\forall x_1^{A_1^\omega} \dots x_n^{A_n^\omega}.\mathtt{t}(x_1,\dots,x_n) = \mathtt{u}(x_1,\dots,x_n)$ when $[\![\mathtt{t}]\!] = [\![\mathtt{u}]\!]$

$\forall x^{A^\omega}\ \mathbf{cons}_a(x) = \mathbf{cons}_a(y) \Rightarrow x = y$ where $a \in A$

$\forall x^{A^\omega}\, y^{A^\omega}\ \mathbf{cons}_a(x) \neq \mathbf{cons}_b(y)$ where $a, b \in A$ with $a \neq b$

$\varphi(\dot{\mathsf{Z}}) \wedge (\forall x^{2^\omega}.x \in \mathbb{N} \wedge \varphi(x) \Rightarrow \varphi(\dot{\mathsf{S}}(x))) \Rightarrow \forall x^{2^\omega}\ x \in \mathbb{N} \Rightarrow \varphi(x)$

$\exists x^{2^\omega} \forall n^{2^\omega}.\ n \in \mathbb{N} \Rightarrow (\varphi(n) \Leftrightarrow \dot{\mathsf{In}}(n,x))$ where x does not occur in φ

$\forall x_1^{2^\omega} \dots x_n^{2^\omega}.\mathtt{t}(x_1,\dots,x_n) = \mathtt{u}(x_1,\dots,x_n) \Leftrightarrow \big(\forall n.\ \chi_{[\![t]\!]}(x_1,\dots,x_n,n) \Leftrightarrow \chi_{[\![u]\!]}(x_1,\dots,x_n,n)\big)^*$

Figure 2.6: Axioms of FOM

- Otherwise, both translations $(-)^*$ and $(-)^\bullet$ commute on all connectives, so it is straightforward to show the equivalence form the induction hypothesis.

□

At this point, we can show that FOM_2 is complete.

Lemma 2.2.8. *The axiomatization is complete for* FOM_2*: for any* FOM_2 *sentence* φ*, we have*

$$\mathfrak{M}_{\mathsf{FOM}} \models \varphi \qquad \Leftrightarrow \qquad \mathsf{FOM} \vdash \varphi$$

Proof. Let φ be such a FOM_2 sentence. The equivalence is obtained as follows.

$\mathfrak{M}_{\mathsf{FOM}} \models \varphi$	$\Leftrightarrow$	$\mathfrak{M}_{\mathsf{MSO}} \models \varphi^\bullet$	since $\mathfrak{M}_{\mathsf{FOM}_2} \equiv \mathfrak{M}^\bullet_{\mathsf{MSO}}$
	$\Leftrightarrow$	$\mathsf{MSO} \vdash \varphi^\bullet$	by soundness and completeness of $\mathsf{MSO}(\omega)$
	$\Leftrightarrow$	$\mathsf{FOM} \vdash \varphi^{\bullet *}$	by Lemma 2.2.6
	$\Leftrightarrow$	$\mathsf{FOM} \vdash \varphi$	by Lemma 2.2.7

□

Now, we want to extend this completeness result to the whole language of FOM; we do so by showing that the elementary equivalence $\mathfrak{M}_{\mathsf{FOM}} \equiv \mathfrak{M}^\dagger_{\mathsf{FOM}_2}$ may be internalized within the axiomatic version of FOM.

Lemma 2.2.9. *Let* $\varphi(x_1,\dots,x_k)$ *be a* FOM *formula, where the* x_i *are the free variables of respective sort* A_i^ω*. Then we have*

$$\mathsf{FOM} \vdash \varphi(\overline{x}) \Leftrightarrow \varphi^\dagger((\pi_1 \circ \eta_{A_1})^\omega(x_1),\dots,(\pi_{|A_1|} \circ \eta_{A_1})^\omega(x_1),\dots)$$

.

Proof. The proof goes by induction over φ; most cases are trivial, save for the base case of a term equality $\mathtt{t}(\overline{x}) = \mathtt{u}(\overline{x})$. Let $(A_1,\dots,A_k;B)$ be the arity of $\mathtt{t}$ and $\mathtt{u}$. In such a case, we need to show that FOM proves the equivalence

$$\widetilde{\mathtt{t}}((\pi_1 \circ \eta_{A_1})^\omega(x_1),\dots) = \widetilde{\mathtt{u}}((\pi_1 \circ \eta_{A_1})^\omega(x_1),\dots) \quad \Leftrightarrow \quad \mathtt{t}(x_1,\dots) = \mathtt{u}(x_1,\dots)$$

For any alphabet B, there is a function $r_B : 2^B \to B$ such that $r_B \circ \eta_B(a) = a$ for every letter $a \in B$. The key to proving the equivalence is the equality

$$r_B^\omega(\widetilde{\mathtt{t}}((\pi_1 \circ \eta_{A_1})^\omega(x_1),\dots)) = \mathtt{t}(x_1,\dots,x_k)$$

which is universally true and thus an axiom of FOM because the lifting $\widetilde{\mathtt{t}}$ was chosen so that we have

$$\widetilde{\mathtt{t}}((\pi_1 \circ \eta_{A_1})^\omega(x_1),\dots)) = \eta_B(\mathtt{t}(x_1,\dots,x_k))$$

holds; postcomposing by r_B^ω on both sides allow to conclude. □

Hence, we may deduce that FOM is complete.

Theorem 2.2.10. *For every formula* φ *of* FOM*,* $\mathsf{FOM} \vdash \varphi$ *if and only if* $\mathfrak{M}_{\mathsf{FOM}} \models \varphi$*. In particular, for every sentence* φ*,* $\mathsf{FOM} \vdash \varphi$ *or* $\mathsf{FOM} \vdash \neg\varphi$*.*

2.3 Church's synthesis problem in FOM

Since FOM has a term language which is extensionally complete for f.s. causal function, admits essentially the same translation to automata as $\mathsf{MSO}(\omega)$, and is *complete*, we may rephrase the Büchi-Landweber exclusively in terms of provability in FOM and refer to its term language to discuss finite-state machines.

Theorem 2.3.1 (Büchi-Landweber)**.** *There exists an algorithm taking as input a* FOM *formula* $\varphi(x^{A^\omega}, y^{B^\omega})$ *and outputs either:*

- *a code of a Mealy machine* $\mathcal{M}$ *implementing a f.s. causal function* $\mathtt{t}(x)$ *such that*

$$\forall x^{A^\omega}\ \varphi(x, \mathtt{t}(x))$$

- *a code of a Mealy machine implementing an eager f.s. causal function* $\mathtt{t}(y)$ *such that*

$$\forall y^{B^\omega}\ \neg\varphi(\mathtt{t}(y), y)$$

Note that the second alternative implies that there is no f.s. causal function $\mathtt{t}(x)$ *such that* $\forall x^{A^\omega}\ \varphi(x, \mathtt{t}(x))$ *holds.*

From this point on, we shall use this version of the Büchi-Landweber theorem when necessary.

Chapter 3

A notion of realizability for Monadic Second-Order Logic MSO over ω

The logic $\mathsf{MSO}(\omega)$ discussed in the introduction is a classical system where entailments between formulas only imply inclusion of the languages determined by their Tarskian semantics. In particular, it does not allow for effective witness extraction: from a proof of statement $\forall n \in \mathbb{N} \exists m \in \mathbb{N}\ \varphi(n, m)$ in Peano arithmetic, there is no way to extract a recursive function $f : \mathbb{N} \to \mathbb{N}$ such that $\varphi(n, f(n))$ holds[1]. By foregoing excluded middle, constructive logics admit richer semantics where the interpretation of proofs allow for such extraction to take place.

The goal of this section is to give a Curry-Howard interpretation of Church's synthesis problem. Concretely speaking, we give a constructive theory SFOM which

- may be seen as a subsystem of $\mathsf{MSO}(\omega)$ in terms of provability.
- is as expressive as $\mathsf{MSO}(\omega)$ through a double-negation translation.
- has a strong extraction property, i.e., from a proof of $\vdash \exists y^B \varphi(x^A, y^B)$ may be computed (in linear time) the code of a f.s. function $\mathtt{t}(x)$ such that $\forall x^A \varphi(x, \mathtt{t}(x))$ classically holds[2].
- is complete with respect to Church's synthesis, i.e., if there exists a code of a f.s. function $\mathtt{t}(x)$ such that $\forall x^A \varphi(x, \mathtt{t}(x))$ holds, then $\mathsf{SFOM} \vdash \exists y^B \varphi^{\neg\neg}(x, \mathtt{t}(x))$.

The most important property might be the strong witnessing property. This is achieved by giving a realizability model for SFOM based on a refinement of the classical automata-theoretic translation of $\mathsf{MSO}(\omega)$ by using *simulation* instead of mere language inclusion when discussing entailment. This constitutes the most important departure from usual treatment of $\mathsf{MSO}(\omega)$. The other results follow from more basic considerations appealing to Büchi's decidability theorem and Siefkes' theorem (for FOM) as blackboxes.

We first give the definition and axiomatization of SFOM and show it admits a double-negation translation relating it to FOM in Section 3.1. Then we explicitate the translation of SFOM formulas to automata and the companion realizability model in Section 3.2. We then finally wrap up by deriving soundness and completeness with respect to synthesis in Section 3.3.

This chapter is meant as a counterpart to our article [56] which featured the same realizability model. The crucial difference between [56] and the current setting is the language of the logic: while we have taken the opportunity to move from $\mathsf{MSO}(\omega)$ to FOM to ease the presentation, the constructive theory of [56] retains the language and the trappings of $\mathsf{MSO}(\omega)$. While this complexifies the presentation, it also means that [56] contains some additional results pertaining to the representation of Mealy machines as $\mathsf{MSO}(\omega)$ formulas which are not reproduced in this thesis.

[1] Note that it is possible when φ is Σ^0_1; the proof goes through a conservativity argument over constructive arithmetic.

[2] Let us mention that we are cheating slightly here; the representation of the function itself is not polynomially bounded in the size of the proof if we insist on representing the Mealy machines as graphs. However, computing a term or any bit of the expanded representation may be done in linear times.

$$\frac{}{\overline{\varphi}, \varphi \vdash \varphi} \qquad \frac{\overline{\varphi} \vdash \psi \qquad \overline{\varphi}, \psi \vdash \varphi}{\overline{\varphi} \vdash \varphi} \qquad \frac{\overline{\varphi} \vdash \varphi \qquad \overline{\varphi} \vdash \neg\varphi}{\overline{\varphi} \vdash \bot}$$

$$\frac{\overline{\varphi} \vdash \varphi \qquad \overline{\varphi} \vdash \psi}{\overline{\varphi} \vdash \varphi \wedge \psi} \qquad \frac{\overline{\varphi} \vdash \varphi \wedge \psi}{\overline{\varphi} \vdash \varphi} \qquad \frac{\overline{\varphi} \vdash \varphi \wedge \psi}{\overline{\varphi} \vdash \psi}$$

$$\frac{\overline{\varphi} \vdash \varphi[\mathtt{t}/x]}{\overline{\varphi} \vdash \exists x^a \varphi} \qquad \frac{\overline{\varphi}, \varphi \vdash \psi \qquad \overline{\varphi} \vdash \exists x^A \varphi}{\overline{\varphi} \vdash \psi} \ (x^A \text{ not free in } \overline{\varphi}, \psi)$$

$$\frac{}{\overline{\varphi} \vdash \mathtt{t} = \mathtt{t}} \qquad \frac{\overline{\varphi} \vdash \phi(\mathtt{t}) \qquad \overline{\varphi} \vdash \mathtt{t} = \mathtt{u}}{\overline{\varphi} \vdash \phi(\mathtt{u})}$$

Figure 3.1: Natural deduction for first-order logic with equalities.

$\mathtt{t}(x_1, \ldots, x_n) = \mathtt{u}(x_1, \ldots, x_n)$	when $[\![\mathtt{t}]\!] = [\![\mathtt{u}]\!]$
$\neg(\mathbf{cons}_a(x) = \mathbf{cons}_a(y) \wedge \neg x = y)$	where $a \in A$ and x, y of sort A^ω
$\neg\mathbf{cons}_a(x) = \mathbf{cons}_b(y)$	where $a, b \in A$ with $a \neq b$ at sort A^ω
$\neg\neg\exists x^{2^\omega} \neg\exists n^{2^\omega}.\ n \in \mathbb{N} \wedge \neg\big(\varphi(n) \Leftrightarrow \dot{\mathsf{In}}(n, x)\big)$	where x does not occur in φ
$\neg\big(t = u \wedge \exists n\ (n \in \mathbb{N} \wedge \neg(\chi_{[\![t]\!]}(n) \Leftrightarrow \chi_{[\![u]\!]}(n))^*)\big)$	
$\neg\big(\neg t = u \wedge \neg\exists n\ (n \in \mathbb{N} \wedge \neg(\chi_{[\![t]\!]}(n) \Leftrightarrow \chi_{[\![u]\!]}(n))^*)\big)$	
where $\varphi \Leftrightarrow \psi$ denotes $\neg(\neg\varphi \wedge \psi) \wedge \neg(\varphi \wedge \neg\psi)$	

Figure 3.2: Additional axioms of SFOM

3.1 The logical system

3.1.1 Definition of SFOM

Formally speaking, the deduction system SFOM is defined as follows:

- The language is the same language as FOM: first-order logic of infinite words, with a term for every f.s. synchronous function.

- The proof rules are those of intuitionistic natural deduction for our set of connectives as presented in Figure 3.1, augmented with double-negation elimination for atomic formulas

$$\frac{\bar{\varphi} \vdash \neg\neg\mathtt{t} = \mathtt{u}}{\bar{\varphi} \vdash \mathtt{t} = \mathtt{u}}$$

  and a rule corresponding respectively to weakened induction.

$$\frac{\bar{\varphi} \vdash \phi(0) \qquad \bar{\varphi}, n \in \mathbb{N}, \phi(n) \vdash \phi(\dot{\mathsf{S}}(n))}{\bar{\varphi}, n \in \mathbb{N} \vdash \neg\neg\phi(n)}$$

- Finally, are added the basic axioms collected in Figure 3.2. These correspond to axioms of FOM as seen in Figure 2.6 and are seen to be readily equivalent. To stress that SFOM does *not* admit universal quantifications or implications, we formulate those explicitly in terms of our limited set of connectives. In particular, axioms with free variables are used to simulate prenex universal quantifications. One crucial point is the adoption of a double-negated comprehension scheme.

3.1.2 Relating FOM and SFOM

We first note that SFOM proves less theorems than FOM.

Lemma 3.1.1. *If* $\mathsf{SFOM} \vdash \varphi$*, then* $\mathsf{FOM} \vdash \varphi$*.*

Proof. Via a straightforward induction over the proof derivation. Most proof rules of SFOM are proof rules of FOM. Only elimination of double-negation for equalities needs to be explicitly shown admissible, which is straightforward since FOM is classical. Then, all of the axioms of SFOM are axioms of FOM with possible additional double-negations, and thus theorems of FOM. □

As is typical with constructive logic, this does not mean that SFOM is less expressive than FOM. Typically, provability in classical logic and constructive logic are related using a double-negation translation $\varphi \mapsto \varphi^{\neg\neg}$. The theorem then states that φ is provable classically if and only if $\varphi^{\neg\neg}$ is provable constructively. The key idea is that, since double-negation elimination is admissible for negated formulas, adding recursively double-negations everywhere allow to reason as in classical logic. From the point of view of constructiveness, a negated formula also have a proof-irrelevant semantics following the slogan "negation kills computational content" of intuitionistic realizability. Therefore, while a witness may be effectively extracted from a constructive proof of $\vdash \exists x\ \varphi$, a proof of $\vdash \neg\neg\exists x\ \varphi$ conveys little information.

Before investigating double-negation translation, it is useful to isolate those formulas with no computational content; anticipating on their automata-theoretic interpretation in the next Section, we call them *deterministic*.

Definition 3.1.2. *The* deterministic *formulas of* SFOM *are generated by the following grammar.*

$$\delta, \delta' ::= \mathtt{t} = \mathtt{u} \mid \delta \wedge \delta' \mid \neg\varphi$$

In particular, note that any negated formula is deterministic, which vindicate the usual slogan "negation kills computational content" from Kleene's realizability.

Lemma 3.1.3. *In* SFOM*, the following rule is admissible for every deterministic formula* δ*.*

$$\frac{}{\varphi, \neg\neg\delta \vdash \delta}$$

Proof. By induction over the formula δ:

- if the formula is an equality, this is an axiom of SFOM.
- if the formula is a conjunct $\delta_1 \wedge \delta_2$, cut the following proof of $\neg\neg(\delta_1 \wedge \delta_2) \vdash \neg\neg\delta_i$ for $i = 1, 2$ with the induction hypothesis.

$$\dfrac{\dfrac{\dfrac{}{\neg\neg(\delta_1 \wedge \delta_2)\,,\, \neg\delta_i \vdash \neg\neg(\delta_1 \wedge \delta_2)} \qquad \dfrac{\dfrac{\dfrac{}{\neg\neg(\delta_1 \wedge \delta_2)\,,\, \neg\delta_i\,,\, \delta_1 \wedge \delta_2 \vdash \delta_1 \wedge \delta_2}}{\neg\neg(\delta_1 \wedge \delta_2)\,,\, \neg\delta_i\,,\, \delta_1 \wedge \delta_2 \vdash \delta_i}}{\neg\neg(\delta_1 \wedge \delta_2)\,,\, \neg\delta_i\,,\, \delta_1 \wedge \delta_2 \vdash \bot}}{\neg\neg(\delta_1 \wedge \delta_2)\,,\, \neg\delta_i \vdash \bot}}{\neg\neg(\delta_1 \wedge \delta_2) \vdash \neg\neg\delta_i}$$

- if the formula is a negation $\neg\varphi$, cut with the proof of triple-negation elimination.

$$\dfrac{\dfrac{\dfrac{}{\neg\neg\neg\varphi\,,\, \varphi \vdash \neg\neg\neg\varphi} \qquad \dfrac{\dfrac{\dfrac{}{\neg\neg\neg\varphi\,,\, \varphi\,,\, \neg\varphi \vdash \neg\varphi} \qquad \dfrac{\dfrac{}{\neg\neg\neg\varphi\,,\, \varphi\,,\, \neg\varphi \vdash \varphi}}{\neg\neg\neg\varphi\,,\, \varphi\,,\, \neg\varphi \vdash \bot}}{\neg\neg\neg\varphi\,,\, \varphi \vdash \neg\neg\varphi}}{\neg\neg\neg\varphi\,,\, \varphi \vdash \bot}}{\neg\neg\neg\varphi \vdash \neg\varphi}$$

□

Since the language of FOM does not feature universal quantifications, we can actually use a radically simpler version of double-negation translation: simply double-negate the formula under consideration.

Lemma 3.1.4. $\mathsf{FOM} \vdash \varphi$ *if and only if* $\mathsf{SFOM} \vdash \neg\neg\varphi$.

Proof. By Lemma 3.1.1, if $\mathsf{SFOM} \vdash \neg\neg\varphi$, then $\mathsf{FOM} \vdash \neg\neg\varphi$. Then, since double-negation elimination is admissible in FOM, we have $\mathsf{FOM} \vdash \varphi$. Conversely, the proof goes by induction on SFOM derivations.

We show that if $\overline{\varphi} \vdash \varphi$ is derivable in FOM, then $\overline{\varphi} \vdash \neg\neg\varphi$ is derivable in SFOM. This amounts to showing that for every FOM rule of the form

$$\frac{(\overline{\varphi}_i \vdash \varphi_i)_{i\in I}}{\overline{\psi} \vdash \psi}$$

the following rule is admissible in SFOM:

$$\frac{(\overline{\varphi}_i \vdash \neg\neg\varphi_i)_{i\in I}}{\overline{\psi} \vdash \neg\neg\psi}$$

We implicitly use the admissibility of *weakening* in SFOM, *i.e.* the admissibility of the rule

$$\frac{\overline{\varphi} \vdash \varphi}{\overline{\varphi}, \psi \vdash \varphi}$$

The propositional rules may be treated exactly as in the usual proof of Glivenko's theorem for propositional logic, and it is folklore that Glivenko's theorem extends to existential quantifications (see e.g. [40, Prop. 10.3]). It remains to deal with the axioms of FOM.

Induction We need to show that

$$\frac{\overline{\varphi} \vdash \neg\neg\phi(0) \qquad \overline{\varphi}, n \in \mathbb{N}, \phi(n) \vdash \neg\neg\phi(\dot{\mathsf{S}}(n))}{\overline{\varphi} \vdash \neg\neg\phi(n)}$$

where n^{2^ω} is not free in $\overline{\varphi}$. The induction scheme of SFOM can be instantiated on $\neg\neg\phi(n)$

$$\frac{\overline{\varphi} \vdash \neg\neg\phi(0) \qquad \overline{\varphi}, n \in \mathbb{N}, \neg\neg\phi(n) \vdash \neg\neg\phi(\dot{\mathsf{S}}(n))}{\overline{\varphi} \vdash \neg\neg\neg\neg\phi(n)}$$

and be cut with the proof of $\neg\neg\neg\neg\phi(n) \vdash \neg\neg\phi(n)$. To conclude, it then suffices to show that the rule

$$\frac{\overline{\varphi}, n \in \mathbb{N}, \phi(n) \vdash \neg\neg\phi(\dot{\mathsf{S}}(n))}{\overline{\varphi}, n \in \mathbb{N}, \neg\neg\phi(n) \vdash \neg\neg\phi(\dot{\mathsf{S}}(n))}$$

is derivable in intuitionistic propositional logic.

Elimination of Equality We have to show that the following rule is admissible in SMSO:

$$\frac{\overline{\varphi} \vdash \neg\neg\varphi(\mathtt{t}) \qquad \overline{\varphi} \vdash \neg\neg\mathtt{t} = \mathtt{u}}{\overline{\varphi} \vdash \neg\neg\varphi(\mathtt{u})}$$

Since $\mathtt{t} = \mathtt{u}$ is deterministic, by cutting the right premise with the deterministic double-negation elimination rule of SFOM, we are left with deriving the following in SFOM:

$$\frac{\overline{\varphi} \vdash \neg\neg\varphi(\mathtt{t}) \qquad \overline{\varphi} \vdash \mathtt{t} = \mathtt{u}}{\overline{\varphi} \vdash \neg\neg\varphi(\mathtt{u})}$$

But this is an instance of the rule of elimination of equality.

Other Axioms of FOM The comprehension axiom scheme of SFOM

$$\neg\neg\exists x^{2^\omega} \neg\exists n^{2^\omega}.\ n \in \mathbb{N} \wedge \neg\big(\varphi(n) \Leftrightarrow \dot{\mathsf{In}}(n, x)\big)$$

is exactly the comprehension axiom of FOM with an additional outer double-negation. The other axioms coincide with those of FOM.

□

3.2 The realizability model

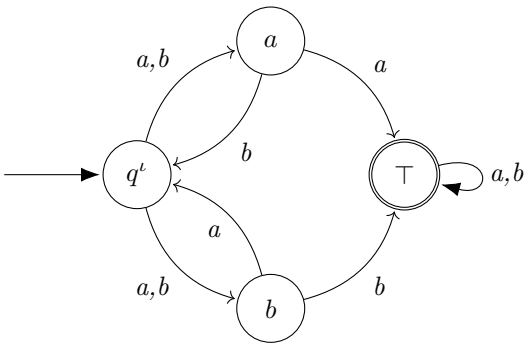
The design of SFOM and its model is guided by the classical automaton translation of Theorem 1.1.5. The basic conceit behind SFOM is that a proof $\varphi \vdash \psi$ not only serves as a witness of the inclusion of languages

$$\{\rho \mid \mathfrak{M}^{\mathsf{FOM}} \models_\rho \varphi\} \;=\; \mathcal{L}(\mathcal{A}_\varphi) \quad \subseteq \quad \mathcal{L}(\mathcal{A}_\psi) \;=\; \{\rho \mid \mathfrak{M}^{\mathsf{FOM}} \models_\rho \psi\}$$

but also ensures that there exists a suitable *simulation* between $\mathcal{A}_\varphi$ and $\mathcal{A}_\psi$. Calling respectively Q_φ and Q_ψ the state-spaces of $\mathcal{A}_\varphi$ and $\mathcal{A}_\psi$ and A their input alphabet, a simulation will be in effect a f.s. causal function $A^\omega \times Q_\varphi^\omega \to Q_\psi^\omega$ mapping accepting runs of $\mathcal{A}_\varphi$ over w to accepting runs of $\mathcal{A}_\psi$ over w. Of course, this result will be effective in the sense that one may compute [3] a simulation from a SFOM proof.

If one is concerned with provability of a single formula $\vdash \varphi$ rather than a sequent, then this means considering simulations from a trivial one-state automaton accepting the universal language to $\mathcal{A}_\varphi$. In effect, such simulations are thus causal functions $A^\omega \to Q_\varphi^\omega$ taking a word to an accepting run (this means in particular that $\mathcal{L}(\mathcal{A}_\varphi) = A^\omega$). Those are not sufficient to give a semantics for SFOM, but provide a quick way of understanding why the suggested above semantics is not degenerate.

Example 3.2.1. *Consider the following non-deterministic Büchi automaton $\mathcal{A}$ over the alphabet $\{a, b\}$.*



For any word $w \in A^\omega$, $q^\iota, w_1, \top, \top, \ldots$ is an accepting run, so $\mathcal{L}(\mathcal{A}) = A^\omega$ However, there is no f.s. causal function $f : A^\omega \to Q^\omega$ such that $f(w)$ is an accepting run of $\mathcal{A}$ over w.

Indeed, fix such a f.s. causal function $f : A^\omega \to Q^\omega$ and consider the function $h : Q \to A$ such that $h(q^\iota) = h(b) = h(\top) = a$ and $h(a) = b$, and extend it to the memoryless function $h^\omega : Q^\omega \to A^\omega$. Then, we can consider the eager function

$$g = h^\omega \circ \mathbf{cons}_{q^\iota} \circ f : A^\omega \to A^\omega$$

By Corollary 2.1.10, there is a unique word $w \in A^\omega$ such that $g(w) = w$.

Then, we show that $\mathbf{cons}_{q^\iota} \circ f(w)$ is not an accepting run to derive a contradiction. To this end, it is sufficient to show that $f(w)_n \neq \top$ for every $n \in \mathbb{N}$. For $n = 0$, it is immediate as $f(w)_0 \in \{a, b\}$ in order to be compatible with $\mathcal{A}$. For $n + 1$, we have a case distinction: either $f(w)_n = q^\iota$, in which case we also have $f(w)_{n+1} \in \{a, b\}$. Otherwise, $f(w)_n = a$ or b. Then $w_{n+1} = g(w)_{n+1} = h((\mathbf{cons}_{q^\iota}(f(w)))_{n+1}) = h(f(w)_n)$. By definition of h, we have $h(f(w)_n) \neq f(w)_n$, which means that we necessarily have $f(w)_{n+1} = q^\iota$.

In this definition, the state space of the automaton plays a crucial rôle. However, there might be many more guiding functions $A^\omega \to Q^\omega$ than actual resolution of determinisms, even for quite intricate predicates. Typically, as we shall use an interpretation based on McNaughton's theorem, complemented automata $\neg\mathcal{A}$ will have huge state space but no meaningful non-deterministic behaviour. For this reason among others, we consider a notion of *uniform automata* which will prove more convenient in interpreting SFOM sequent.

Definition 3.2.2. *A* uniform automaton *over alphabet A is a tuple $\mathcal{A} = (Q, q^\iota, U, \delta, \Omega) : A$ such that*

- Q is a finite set of states.

[3] In fact, in linear time if one adopts a term language for Mealy machines featuring pairing, projections and composition. Otherwise, this extraction procedure may produce machines with a state-space in the input derivation.

- $q^\iota \in Q$ *is the initial state.*

- U *is a finite set of* moves.

- $\delta : A \times Q \times U \to Q$ *is a transition function.*

- $\Omega \subseteq Q^\omega$ *is an acceptance conditions.*

A run of the automaton over a word $w \in A^\omega$ is a sequence of states $q \in Q^\omega$ such that there exists $u \in U^\omega$ with $q_0 = q^\iota$ and $q_{n+1} = \delta(w_n, q_n, u_n)$. A run q is accepting if and only if $q \in \Omega$.

As before, the language recognized by $\mathcal{A}$ is the set of words w such there exists an accepting run over w.

A uniform automaton is called Büchi/parity/Muller according to the same criteria as in Definition 1.1.2.

A uniform automaton is called deterministic *if the set of moves U is a singleton.*

Uniform non-deterministic automata and non-deterministic automata recognize the same languages. From a non-deterministic automaton (Q, I, Δ, Ω), one may build the uniform automaton $(Q + \{q^\iota, \bot\}, q^\iota, Q, \delta', \Omega')$ with

$$\begin{array}{lcl}
\delta(a, \mathsf{inr}(\bot), r) & = & \mathsf{inr}(\bot) \\
\delta(a, \mathsf{inr}(q^\iota), r) & = & \begin{cases} \mathsf{inl}(r) & \text{if there exists } q \in I \text{ such that } (q,a,r) \in \Delta \\ \mathsf{inr}(\bot) & \text{otherwise} \end{cases} \\
\delta(a, \mathsf{inl}(q), r) & = & \begin{cases} \mathsf{inl}(r) & \text{if } (q,a,r) \in \Delta \\ \mathsf{inr}(\bot) & \text{otherwise} \end{cases} \\
\\
\Omega' & = & \{q \in (Q + \{q^\iota, \bot\})^\omega \mid \exists q' \in Q^\omega . q' \in \Omega \wedge \forall n > 0 . q_n = \mathsf{inl}(q'_n)\}
\end{array}$$

Conversely, given a uniform automaton $(Q, q^\iota, U, \delta, \Omega)$, the non-deterministic automaton $(Q, \{q^\iota\}, \Delta', \Omega)$ with $\Delta' = \{(q, a, r) \in Q \times A \times Q \mid \exists u \in U \ \delta(a, q, u) = r\}$ recognizes the same language. Similar maps can also be defined for deterministic uniform automata and deterministic automata. Observe that the complexity of the acceptance condition (Büchi, parity or Muller) is not affected by this translation. In the sequel, we shall re-use this fact together with McNaughton's theorem (Theorem 1.1.6).

Proposition 3.2.3. *For every uniform Muller automaton $\mathcal{A} : A$, there is a Muller automaton recognizing $\mathcal{L}(\mathcal{A})$ and conversely, for every Muller automaton $\mathcal{B} : A$, there is a uniform Muller automaton recognizing $\mathcal{L}(\mathcal{B})$.*

Now that we have established that uniform automata are not so different from the classical notion, we can now give a convenient phrasing of the notion of simulation between uniform automata.

Definition 3.2.4. *Let $\mathcal{A} = (Q_\mathcal{A}, q^\iota_\mathcal{A}, \delta_\mathcal{A}, U, \Omega_\mathcal{A}) : A$ and $\mathcal{B} = (Q_\mathcal{B}, q^\iota_\mathcal{B}, \delta_\mathcal{B}, V, \Omega_\mathcal{B}) : A$ be uniform automata over a common alphabet A. A* simulation $\mathcal{A} \to \mathcal{B}$ *is a f.s. synchronous function $f : (A \times U)^\omega \to V^\omega$ such that, for every word $w \in A^\omega$ and $u \in U^\omega$, the unique sequences $q \in Q^\omega_\mathcal{A}$ and $r \in Q^\omega_\mathcal{B}$ such that*

$$\begin{array}{lll} q_0 = q^\iota_\mathcal{A} & & q_{n+1} = \delta_\mathcal{A}(w_n, q_n, u_n) \\ r_0 = q^\iota_\mathcal{B} & & r_{n+1} = \delta_\mathcal{B}(w_n, r_n, f(\langle w, u\rangle)_n) \end{array}$$

we have $q \in \Omega_\mathcal{A} \Rightarrow r \in \Omega_\mathcal{B}$.

We write $\mathcal{A} \Vdash f : \mathcal{B}$ (which is informally read as "f realizes $\mathcal{A} \vdash \mathcal{B}$" when f is a simulation from $\mathcal{A}$ to $\mathcal{B}$. Sometimes, we write $\mathcal{A} \Vdash \mathcal{B}$ to mean that there exists some f such that $\mathcal{A} \Vdash f : \mathcal{B}$.

Simulations $\mathcal{A} \Vdash \mathcal{B}$ strictly refine inclusions of languages $\mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$: if there exists a simulation $\mathcal{A} \to \mathcal{B}$, then $\mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$ in the general case. However, the notion trivializes as expected when $\mathcal{B}$ is deterministic.

Lemma 3.2.5. *Let $\mathcal{A}$ and $\mathcal{B}$ be uniform automata over a common alphabet A. If $\mathcal{B}$ is deterministic, then there exists a (necessarily unique) simulation $\mathcal{A} \to \mathcal{B}$ if and only if $\mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$.*

Proof. Since $\mathcal{B}$ is deterministic, a simulation $f : \mathcal{A} \to \mathcal{B}$ has codomain 1, so there is at most one such map. Then the equivalence is straightforward. □

Crucially, simulations between automata compose. In fact, they may be arranged into a category Aut_A

Lemma 3.2.6. *Given an alphabet A, the category of uniform Muller automata and simulations Aut_A is given by the following data:*

- **Objects:** *objects are uniform Muller automata over the designated alphabet $\mathcal{A} : A$.*
- **Morphisms:** *morphisms from $\mathcal{A}$ to $\mathcal{B}$ are f.s. causal function f such that $\mathcal{A} \Vdash f : \mathcal{B}$.*
- **Composition:** *given f.s causal functions f and g such that $\mathcal{A} \Vdash f : \mathcal{B}$ and $\mathcal{B} \Vdash g : \mathcal{C}$, the composite is $h = f \circ \langle \pi_1, g \rangle$. It is straightforward to check that $\mathcal{A} \Vdash h : \mathcal{C}$.*

Associativity of composition is straightforward[4]. This fact will readily provide us with the interpretation of the cut rule from logic.

$$\frac{\mathcal{A} \Vdash f : \mathcal{B} \qquad \mathcal{B} \Vdash g : \mathcal{C}}{\mathcal{A} \Vdash f \circ \langle \pi_1, g \rangle : \mathcal{C}}$$

The treatment of conjunction can also be expressed as a categorical property.

Lemma 3.2.7. *Given Muller automata*

$$\begin{array}{rcl} \mathcal{A} & = & (Q_{\mathcal{A}}, q^{\iota}_{\mathcal{A}}, U, \delta_{\mathcal{A}}, [\mathcal{F}_{\mathcal{A}}]_{\infty}) \ : \ A \\ \mathcal{B} & = & (Q_{\mathcal{B}}, q^{\iota}_{\mathcal{B}}, V, \delta_{\mathcal{B}}, [\mathcal{F}_{\mathcal{B}}]_{\infty}) \ : \ A \end{array}$$

define the conjunction automaton as $\mathcal{A} \wedge \mathcal{B} = (Q_{\mathcal{A}} \times Q_{\mathcal{B}}, I_{\mathcal{A}} \times I_{\mathcal{B}}, \Delta_{\mathcal{A} \wedge \mathcal{B}}, [\mathcal{F}_{\mathcal{A} \wedge \mathcal{B}}]_{\infty})$ with

$$\begin{array}{rcl} \delta_{\mathcal{A} \wedge \mathcal{B}}(a, (q, r), (u, v)) & = & (\delta_{\mathcal{A}}(a, q, u), \delta_{\mathcal{B}}(a, r, v)) \\ \mathcal{F}_{\mathcal{A} \wedge \mathcal{B}} & = & \{X \mid \pi_1(X) \in \mathcal{F}_{\mathcal{A}} \wedge \pi_2(X) \in \mathcal{F}_{\mathcal{B}}\} \end{array}$$

The automaton $\mathcal{A} \wedge \mathcal{B}$ satisfies the following:

- *$\mathcal{L}(\mathcal{A} \wedge \mathcal{B}) = \mathcal{L}(\mathcal{A}) \cap \mathcal{L}(\mathcal{B})$.*
- *If $\mathcal{A}$ and $\mathcal{B}$ are both deterministic, so is $\mathcal{A} \wedge \mathcal{B}$.*
- *Finally, $\mathcal{A} \wedge \mathcal{B}$ is the cartesian product of $\mathcal{A}$ and $\mathcal{B}$ in Aut_A.*

Proof. The first two points are standard, so we focus on the last. First we need to provide projections. They are given as

$$\pi_{\mathcal{A}} : A \times (U \times V) \xrightarrow{\pi_2} U \times V \xrightarrow{\pi_1} U$$

$$\pi_{\mathcal{B}} : A \times (U \times V) \xrightarrow{\pi_2} U \times V \xrightarrow{\pi_2} V$$

Clearly, it is then easy to check that

$$\mathcal{A} \wedge \mathcal{B} \Vdash \pi_{\mathcal{A}} : \mathcal{A} \qquad \mathcal{A} \wedge \mathcal{B} \Vdash \pi_{\mathcal{B}} : \mathcal{B}$$

Finally, we need to check that $\mathcal{A} \wedge \mathcal{B}$ equipped with those projections have the suitable universal property: for any automaton $\mathcal{C} = (Q_{\mathcal{C}}, q^{\iota}_{\mathcal{C}}, W, \delta_{\mathcal{C}}, [\mathcal{F}_{\mathcal{C}}]_{\infty}) : A$ and simulations

$$\mathcal{C} \Vdash f : \mathcal{A} \qquad \mathcal{C} \Vdash g : \mathcal{B}$$

there should exist a unique f.s. causal $h : A \times W \to U \times V$ such that $\pi_1 \circ h = f$ and $\pi_2 \circ h = g$. Since $U \times V$ is a cartesian product, h is uniquely determined to be the pairing $\langle f, g \rangle$. Then it can be checked that we have indeed

$$\mathcal{C} \Vdash \langle f, g \rangle : \mathcal{A} \wedge \mathcal{B}$$

□

As usual, the cartesian structure allow to interpret the natural deduction rules for introducing negation and conjunction.

$$\frac{\mathcal{A} \Vdash f : \mathcal{B}_1 \wedge \mathcal{B}_2}{\mathcal{A} \Vdash \pi_i \circ f : \mathcal{B}_i} \qquad \frac{\mathcal{A} \Vdash f : \mathcal{B} \qquad \mathcal{A} \Vdash g : \mathcal{C}}{\mathcal{A} \Vdash \langle f, g \rangle : \mathcal{B} \wedge \mathcal{C}}$$

We now may write $\mathcal{A}_1, \ldots, \mathcal{A}_n \Vdash f : \mathcal{B}$ as a shorthand for $\mathcal{A}_1 \wedge \cdots \wedge \mathcal{A}_n \Vdash f : \mathcal{B}$.

Similarly the existential quantification is handled by adapting the classical automaton construction[5]. In order to characterize the computational content pertaining to $\exists$, we first need to make precise how substitution by finite-state causal functions works.

[4] Although not technically needed here since if unconcerned with cut-elimination.

[5] Rather than defining the abstract structure needed for categorical logic, we unpack the technical ingredients here. The categorical setting for first-order logic will be presented later, and the interested reader will notice that we define here the substitution functor and simple sums.

Definition 3.2.8. *Given a uniform Muller automaton $\mathcal{A} = (Q_\mathcal{A}, q^\iota_\mathcal{A}, U, \delta_\mathcal{A}, [\mathcal{F}]_\infty) : B$ and a Mealy machine $\mathcal{M} = (Q_\mathcal{M}, q^\iota_\mathcal{M}, \delta_\mathcal{M}) : A^\omega \to B^\omega$, define the substituted automaton $\mathcal{M}^*\mathcal{A} = (Q_\mathcal{A} \times Q_\mathcal{M}, (q^\iota_\mathcal{A}, q^\iota_\mathcal{M}), U, \delta_{\mathcal{M}^*\mathcal{A}}, [\mathcal{F}_{\mathcal{M}^*\mathcal{A}}]_\infty)$ with*

$$\begin{array}{lcl} \pi_2(\delta_{\mathcal{M}^*\mathcal{A}}(a,(q,r)),u) & = & \pi_2(\delta_\mathcal{M}(a,r)) \\ \pi_1(\delta_{\mathcal{M}^*\mathcal{A}}(a,(q,r)),u) & = & \delta_\mathcal{A}(\pi_1(\delta_\mathcal{M}(a,r)),q,u) \\ X \in \mathcal{F}_{\mathcal{M}^*\mathcal{A}} & \Leftrightarrow & \pi_1(X) = \{q \mid (q,r) \in X\} \in \mathcal{F} \end{array}$$

Since every f.s. causal function corresponds to a unique minimal Mealy machine, we shall some times be sloppy and allow ourselves to write $f^*\mathcal{A}$ for the corresponding subsituted automaton. The language recognized by the subsituted automaton corresponds formally to the following.

Lemma 3.2.9. *For every uniform Muller automaton $\mathcal{A} : B$ and f.s. causal function $f : A^\omega \to B^\omega$, we have*

$$\mathcal{L}(f^*\mathcal{A}) = \{x \in A^\omega \mid f(x) \in \mathcal{L}(\mathcal{A})\}$$

As a straightforward corollary, this establishes the soundness of the usual substitution scheme for the classical semantics. Given that f is taken to be f.s. causal, it is also readily check that it is validated for the realizability semantics

$$\frac{\mathcal{A} \Vdash g : \mathcal{B}}{f^*\mathcal{A} \Vdash g \circ (f \times \mathrm{id}) : f^*\mathcal{B}}$$

In particular, the f.s. causal function may be taken to be a projection $\pi_1 : A \times B \to B$, and the substitution operation $\pi_1^*\mathcal{A}$ for $\mathcal{A} : B$ amounts to adding a dummy stream variable to the formula corresponding to $\pi_1^*\mathcal{A}$.

Lemma 3.2.10. *Given a uniform automaton $\mathcal{A} = (Q_\mathcal{A}, q^\iota_\mathcal{A}, U, \delta_\mathcal{A}, [\mathcal{F}]_\infty) : A \times B$, define the projection automaton $\exists_{\pi_2}\mathcal{A} := (Q_\mathcal{A}, q^\iota_c A, U \times A, \delta_{\exists_{\pi_2}\mathcal{A}}, [\mathcal{F}]_\infty) : B$ with*

$$\delta_{\exists_{\pi_2}\mathcal{A}}(b, q, (u, a)) = \delta_\mathcal{A}((a, b), q, u)$$

The automaton $\exists_{\pi_2}\mathcal{A}$ satisfies the following:

- $\mathcal{L}(\exists_{\pi_2}\mathcal{A}) = \{b \in B^\omega \mid \exists a \in A^\omega \ \langle a, b\rangle \in \mathcal{L}(\mathcal{A})\}$
- *For any f.s. causal $f : B^\omega \to U^\omega$ and $g : B^\omega \to A^\omega$, we have $\langle f, g\rangle \Vdash \mathcal{A}$ if and only if $f \Vdash \langle g, \mathrm{id}\rangle^*\mathcal{A}$.*

This construction thus implements the usual existential quantification at the level of language, but also has a familiar constructive semantics: a proof is a pair of a witness together with another proof that the witness is valid. In order to show that this interpretation is sound with respect to natural deduction, the following two lemmas are required; the proofs are also straightforward to check.

Lemma 3.2.11. *Let $\mathcal{A} : B$, $\mathcal{B} : A \times B$ and $\mathcal{C} : B$ be uniform Muller automata with respective sets of moves U, V and W. For every $f : B \times (U \times (V \times A)) \to W$ such that*

$$\mathcal{A} \wedge \exists_{\pi_2}\mathcal{B} \Vdash f : \mathcal{C}$$

we have

$$\pi_2^*\mathcal{A} \wedge \mathcal{B} \Vdash f' : \pi_2^*\mathcal{C}$$

where f' is the following composite, where m is the only natural permutation of coordinates available

$$(A \times B) \times (U \times V) \xrightarrow{\quad m \quad} B \times (U \times (V \times A)) \xrightarrow{\quad f \quad} W$$

Lemma 3.2.12. *Let $\mathcal{A} : A$ and $\mathcal{B} : A \times B$ be Muller automata and $f : A^\omega \to B^\omega$ finite-state, causal. Then, if g is such that $\mathcal{A} \Vdash g : \langle \mathrm{id}, f\rangle^*\mathcal{B}$, then*

$$\mathcal{A} \Vdash \langle g, f \circ \pi_1\rangle : \exists_{\pi_2}\mathcal{B}$$

These two lemmas correspond respectively to the following proof rules,

$$\frac{\mathcal{A} \wedge \exists_{\pi_2}\mathcal{B} \Vdash \mathcal{C}}{\pi_2^*\mathcal{A} \wedge \mathcal{B} \Vdash \pi_2^*\mathcal{C}} \qquad \frac{\mathcal{A} \Vdash \langle \mathrm{id}, f\rangle^*\mathcal{B}}{\mathcal{A} \Vdash \exists_{\pi_2}\mathcal{B}}$$

Finally, come the non-trivial question of interpreting negation. A more common approach in realizability is to first give a semantics for the arrow $\Rightarrow$ and falsity $\bot$. While the usual automata-theoretic translation $\bot_A = (1, *, \emptyset, *, [\emptyset]_\infty) : A$ for the latter may be rather unproblematically reused, the former actually cannot be encoded in all generality because the category Mealy is not cartesian-closed.

Therefore, we give a singular negation connective on automata. Following a customary automata-theoretic translation, we implement $\neg\mathcal{A}$ in two steps: we first determinize and then negate.

Lemma 3.2.13. *Let $\mathcal{A} = (Q, q^\iota, U, \delta, [\mathcal{F}]_\infty) : A$ be a uniform Muller automaton. There exists a deterministic uniform Muller automaton $\neg\mathcal{A} : A$ such that $\mathcal{L}(\neg\mathcal{A}) = A^\omega \setminus \mathcal{L}(\mathcal{A})$*

Proof.
- We first use a determinization procedure $\mathcal{A} \mapsto ?\mathcal{A}$ to get a Muller automaton accepting the same language by combining McNaughton's theorem (Theorem 1.1.6) and Proposition 3.2.3. The specifics of the determinzation procedure are rather unimportant as long as the set of moves of the resulting uniforma automaton $?\mathcal{A}$ is 1 and $\mathcal{L}(\mathcal{A}) = \mathcal{L}(?\mathcal{A})$.
- Then we consider the operation of negating the acceptance condition $\mathcal{A} \mapsto \mathcal{A}^\perp$. If $\mathcal{A}$ is deterministic, this ensures that $\mathcal{L}(\mathcal{A}^\perp) = A^\omega \setminus \mathcal{L}(\mathcal{A})$ and that $\mathcal{A}^\perp$ remains deterministic. $\neg\mathcal{A}$ is then set to be $(?\mathcal{A})^\perp$.

□

In order to show that this choice of negation is sound with respect to the deduction rules, we exploit Lemma 3.2.5, i.e. the fact that when $\mathcal{B}$ is deterministic, we have the equivalence

$$\mathcal{A} \Vdash \mathcal{B} \qquad \text{if and only if} \qquad \mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$$

Thus the rules of negation are also sound at the level of simulations, i.e.

$$\frac{\mathcal{A}, \mathcal{B} \Vdash \bot}{\mathcal{A} \Vdash \neg\mathcal{B}} \qquad \frac{\mathcal{A} \Vdash \bot}{\mathcal{A} \Vdash \mathcal{B}}$$

This implies in particular that, for uniform automata, we have $\mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$ if and only if $\mathcal{A} \Vdash ?\mathcal{B}$.

Remark. *We can relate our semantics to the notion of* good-for-games *automata from [28]. If $\mathcal{A} : A$ is a classical automaton and $\mathcal{A}^* : A$ is its uniform version obtained through Proposition 3.2.3, then $\mathcal{A}$ is good-for-games if and only if $?\mathcal{A}^* \Vdash \mathcal{A}^*$.*

It is also worth noting that the determinization construction is equivalent to double negation at the level of simulations, i.e.

Proposition 3.2.14. *For any alphabet A and uniform Muller automaton $\mathcal{A} : A$, there is a unique isomorphism in Aut_A between $?\mathcal{A}$ and $\neg\neg\mathcal{A}$. Furthermore, if $\mathcal{A}$ was already deterministic, then $\mathcal{A}$ is a unique isomorphism between $\mathcal{A}$ and $?\mathcal{A}$.*

3.3 Soundness and completeness with respect to Church's synthesis

Now that we have basic proof-theoretic facts about SFOM and a notion of simulation of automata, we are ready to show that SFOM is sound and complete with respect to Church's synthesis.

For soundness, we first define a translation $[\![-]\!]$ from FOM formulas of sort A to uniform automata over A.

$$\begin{array}{lcll} [\![\mathcal{M}(x) = \mathcal{N}(x)]\!] & = & \langle \mathcal{M}, \mathcal{N} \rangle^* \mathcal{E} & \\ [\![\varphi \wedge \psi]\!] & = & [\![\varphi]\!] \wedge [\![\psi]\!] & \\ [\![\exists x^A\ \varphi]\!] & = & \exists_\pi [\![\varphi]\!] & \text{where } \pi \text{ is the relevant projection.} \\ [\![\neg\varphi]\!] & = & (?[\![\varphi]\!])^\perp & \end{array}$$

where $\mathcal{E}$ is the deterministic automaton

$$\mathcal{E} = (\{0,1\}, 1, \delta_\mathcal{E}, [\mathcal{P}(\{1\})]_\infty) : A \times A$$

$$\begin{array}{lll} \text{with} & \delta_\mathcal{E}((a,a),1) = 1 & \\ & \delta_\mathcal{E}((a,a'),1) = 0 & \text{if } a \neq a' \\ & \delta_\mathcal{E}((a,a'),0) = 0 & \end{array}$$

recognizing the diagonal language $\{\langle w, w \rangle \in (A \times A)^\omega\}$.

Remark. *The translation from formulas to automata is naturally restricted to the connectives* $\exists$, $\wedge$ *and* $\neg$. *In the context of constructive logic, this restriction is not as innocent as with classical logic:* $\neg\forall x\, \neg\varphi(x)$ *is possibly strictly weaker than* $\exists x\, \varphi(x)$. *As we shall see later, the intended model for* SFOM *may also arise as a generic construction from categorical logic, a variant of the* simple fibration *over the category* Mealy*; this construction allow to interpret the full set of first-order connectives only when the base category is cartesian-closed, which is not the case of* Mealy.

While formulas are mapped to automata as with usual interpretation of MSO, the crucial point is that proofs are mapped to *simulations*. In particular, this means the level of non-determinism in the interpretation of a formula has an impact on derivability. Deterministic formulas as given in Definition 3.1.2 are mapped to deterministic uniform automata; considering Lemma 3.2.5, this justifies that slogan "negation kills computational content" from realizability also applies to our setting. Aggregating the Lemmas in Section 3.2, one may derive the following soundness theorem via a straightforward induction.

Theorem 3.3.1. *There is a linear-time function taking as input a derivation* $\varphi_1, \dots, \varphi_k \vdash \phi$ *in* SFOM *and outputting a term* $\mathtt{t}$ *such that* $[\![\varphi_1]\!] \wedge \cdots \wedge [\![\varphi_k]\!] \Vdash [\![\mathtt{t}]\!] : [\![\phi]\!]$.

Proof. It suffices to show that every rule and axiom of SFOM is adequate with respect to our realizability interpretation in order to conclude by induction over the derivation. The rules of introduction of $\exists$ is admissible by Lemma 3.2.12 and elimination is handled by Lemma 3.2.11. Similarly, the rules for conjunction are sound because conjunction correspond to cartesian products in the category of automata and simulations (Lemma 3.2.7). Now, the conclusion of the remaining proof rules are all of the shape $\overline{\varphi} \vdash \delta$ with δ deterministic; therefore, by Lemma 3.2.5, it suffices to show that there is an inclusion of language $\bigcap_{i=1}^{k} \mathcal{L}([\![\varphi_i]\!]) \subseteq \mathcal{L}([\![\delta]\!])$. Since simulations refine inclusions, all the premises give rise to similar inclusions; it then suffices to check that the rule are then valid for the classical semantics FOM, which is easy. □

This allow to derive the crucial witnessing property that allows extraction of Mealy machines from proofs of existential statements.

Corollary 3.3.2. *Given a proof of* $\vdash \exists y^B \varphi(x^A, y^B)$ *in* SFOM*, one may output a term* $\mathtt{t}$ *such that, for every* $w \in A^\omega$, $\mathfrak{M}^{\mathsf{FOM}} \models \varphi(w, [\![t]\!](w))$ *holds.*

Proof. Calling U the set of moves of $[\![\varphi(x,y)]\!]$, by Theorem 3.3.1, there exists a f.s. synchronous map $f : A^\omega \to (B \times U)^\omega$ such that $\Vdash f : [\![\exists y^{B^\omega} \varphi(x,y)]\!]$ holds. Taking $\mathtt{t}$ any term of arity $(A^\omega; B^\omega)$ such that $[\![\mathtt{t}]\!] = f$, this means that $\Vdash \pi_2 \circ f : [\![\varphi(x, \mathtt{t}(x))]\!]$. Since simulations refine inclusions, we have $[\![\varphi(x), \mathtt{t}(x)]\!] = A^\omega$, and therefore the results hold. □

Remark. *Note that the state-space of a Mealy machine interpreting* $[\![\mathtt{t}]\!]$ *has no reason to be linear in the size of* $\mathtt{t}$*, but is only bounded by an exponential: the size of the state space of either composition or pairing of two Mealy machines* $\mathcal{M}$ *and* $\mathcal{N}$ *is obtained by multiplying the size of the state spaces of* $\mathcal{M}$ *and* $\mathcal{N}$.

Corollary 3.3.2 admits the following converse, thanks to the double-negation translation of FOM in SFOM. This constitute *completeness with respect to Church's synthesis*. Note that this is shown solely from proof-theoretic considerations derived from Section 3.1.

Theorem 3.3.3. *Let* $\varphi(x^{A^\omega}, y^{B^\omega})$ *be a* FOM *formula such that there exists a f.s. synchronous function* $f : A^\omega \to B^\omega$ *such that* $\mathfrak{M}^{\mathsf{FOM}} \models \varphi(w, f(w))$ *for every* $w \in A^\omega$. *Then,* SFOM $\vdash \exists y^{B^\omega} \neg\neg\varphi(x,y)$.

Proof. Let $\mathtt{t}$ be term of sort $(A^\omega; B^\omega)$ such that $[\![t]\!] = f$. Then FOM $\vdash \varphi(x, \mathtt{t}(x))$ by completeness of FOM with respect to its standard model. Then, by Lemma 3.1.4, we have SFOM $\vdash \neg\neg\varphi(x, \mathtt{t}(x))$. Then, using a $\exists$-intro rule, we have the result SFOM $\vdash \exists y^{B^\omega} \neg\neg\varphi(x,y)$. □

Chapter 4

Extension to alternating automata

In the previous chapter, we defined SFOM, a constructive subsystem of FOM and a companion realizability-like model, where formulas are interpreted as (uniform) non-deterministic Muller automata and proofs as Mealy machines, regarded as a particular kind of simulations between the underlying automata. An interesting aspect of this model is that the interpretation of formulas into automata matches the classical interpretation of $\mathsf{MSO}(\omega)$ into automata; the difference lies at the level of the interpretation of proofs, which are no longer mere language inclusions, but simulations whose type depends on the non-determinism of the underlying automata.

While non-deterministic automata are sufficient to translate every $\mathsf{MSO}(\omega)$ formula in a sound way, these are not the only device able to recognize ω-regular languages. A natural extension is given by alternating automata over infinite words, which generalize both non-deterministic automata and their dual, *universal automata*. The main object of this chapter is to describe LSFOM, another formalism FOM together with a realizability-like model generalizing the previous one by incorporating alternating word automata. In particular, formal proof trees are interpreted as a notion of simulation generalizing the one present in the previous chapter. This presents an additional difficulty as this generalized notion of simulation will not enable to interpret the structural rule of *contraction* $\varphi \to \varphi \wedge \varphi$ in the general case. For this reason, LSFOM will be based on first-order intuitionistic multiplicative linear logic. SFOM also comes with a polarity system extending the distinction between non-deterministic and deterministic formulas of SFOM, as well as exponential modalities restricted to polarized formulas, accounted for by (co)determinization at the semantic level.

From the perspective of linear logic, this model is interesting because of a number of peculiarities it shares with models of linear logic based on Gödel's Dialectica interpretation [21]. Among other things, it is *not* a model of classical linear logic, but it features propositional connectives $\otimes$ and $\parr$ distributing over one another (in the sense of linearly distributive categories [**?**]) and, as we shall see much later on, retracts of the map $\varphi \to (\varphi \multimap \bot) \multimap \bot$. On top of these characteristics, it should also be noted that the notion of quantification here runs counter the intuition of witnesses being given sequentially one after the other: a realizer for a formula $\exists x^{A^\omega} \forall y^{B^\omega}.\varphi(x,y)$ must give some witness for x, but the letter x_n this witness may depend on the letters y_k for $k < n$.

From an automata-theoretic perspective, it should be stressed LSFOM formulas may be interpreted as automata. These formulas come with a natural polarity system which allowing to constrain their interpretation to be e.g. deterministic, non-deterministic or universal. In particular, the polarity system, beyond its role at the level of provability, can be seen as a way of constraining the translation to be correct with respect to the classical semantics of the formula (i.e., when translating the linear connectives of SFOM to the usual connectives of FOM). As a result, various translations of FOM into SFOM may be regarded as various ways of implementing Büchi's theorem using basic automata-theoretic constructions *and* determinization. It should be stressed that, similarly to SFOM, LSFOM does not say anything about the fine combinatorics behind the automata theoretic constructions such as determinization; in the interpretation of formulas as automata, determinization is used as a black box.

This chapter is meant as a counterpart to the article [58] where the same realizability model was presented for a theory very similar to LSFOM. The material presented here is essentially the same. However, when describing the realizability model, the discussion will remain informal and the full proofs will be deferred to Chapter 6 which treats a higher-order extension of the model.

4.1 The theory LSFOM

Automata and polarities We now present the logic LSFOM. Since the end syntax includes a notion of *polarized exponentials*, we define by mutual induction the syntax of polarized formulas before giving the full-fledged syntax of LSFOM. Since we need to discuss polarity early, it might be useful for the reader familiar with automata-theoretic interpretations to know into what kind of automata a formula might end up being interpreted.

Definition 4.1.1. *An* alternating uniform automaton *over alphabet A is a tuple*

$$\mathcal{A} = (Q, q^\iota, U, X, \delta, \Omega) : A$$

such that

- *Q is a finite set of states.*
- *$q^\iota \in Q$ is the initial state.*
- *U is a finite non-empty set of* P*-moves.*
- *X is a finite non-empty set of* O*-moves.*
- *$\delta : A \times Q \times U \times X \to Q$ is a transition function.*
- *$\Omega \subseteq Q^\omega$ is an acceptance conditions.*

The crucial difference with uniform deterministic automata is that now, it is not sufficient to guess an accepting run by providing some $u \in U$ for every transition to establish that a word is in the language, but now one needs to show that it is possible to do so for any choice of $x \in X$ by some opponent O. Acceptance of a word is thus formalized as the existence of a winning strategy in an *acceptance game*.

Definition 4.1.2. *A* P*-strategy is an* eager[1] *causal map $s : X^\omega \to U^\omega$. A* P*-strategy together with a stream $x \in X^\omega$ defines a* play *$\langle s(x), x\rangle \in (U \times X)^\omega$. A play induces a unique sequence sequence of states $q \in Q^\omega$ such that $q_0 = q^\iota$ and $q_{n+1} = \delta(w_n, q_n, u_n, x_n)$. A play is accepting if and only if the corresponding sequence of states $(q_n)_{n\in\mathbb{N}}$ lies in Ω.*

The language recognized by $\mathcal{A}$ is the set of words $w \in A^\omega$ such there exists a P*-strategy s such that all plays $\langle s(x), x\rangle$ are accepting. Write $\mathcal{L}(\mathcal{A})$ for the set of words accepted by $\mathcal{A}$.*

A uniform automaton is called Büchi/parity/Muller according to the same criteria as in Definition 1.1.2.

From now on, when speaking about uniform automata, we rather mean the more general notion given in Definition 4.1.1 rather than the non-deterministic case. The important advantage of this uniform notion is that, much like with the non-deterministic case, it allows to speak of the deterministic/non-deterministic/universal subcases at the level of moves.

Definition 4.1.3. *A uniform automaton $\mathcal{A} = (Q, q^\iota, U, X, \delta, \Omega) : A$ is said to be:*

- non-deterministic *if $X \simeq 1$.*
- universal *if $U \simeq 1$.*
- deterministic *if $U \simeq X \simeq 1$.*

When designing operators on uniform automata meant to be correct with respect to the semantics of underlying MSO formulas, some may easily be done without using complementation or determinization procedures, depending on the nature of the underlying automaton:

- language recognized by non-deterministic Muller automata are easily shown to be closed under union, intersection and projection.
- dually, universal automata are easily closed under union, intersection and coprojection.
- deterministic automata are easily closed under complement, intersection and union but not quantifications.

These intuitions may guide the reader as the polarity system where *positive* formulas will correspond to non-deterministic automata in the semantics and *negative* formulas to universal automata. This means in particular that there will be formulas which are both positive and negative corresponding to deterministic automata, and more general unpolarized formulas corresponding to general alternating automata.

[1] In the sense of Definition 2.1.7, which means that the value of $s(x)_n$ depends only the x_i for $i < n$.

$$
\begin{array}{rcl}
\varphi^{\pm}, \psi^{\pm} & ::= & \mathbf{I} \mid \bot \mid \mathtt{t} = \mathtt{u} \mid !\varphi^{-} \mid ?\varphi^{+} \mid \varphi^{\pm} \otimes \psi^{\pm} \mid \varphi^{\pm} \parr \psi^{\pm} \mid \varphi^{\pm} \multimap \psi^{\pm} \\
\varphi^{+}, \psi^{+} & ::= & \varphi^{\pm} \mid \exists x^{A^{\omega}}.\varphi^{+} \mid \varphi^{+} \otimes \psi^{+} \mid \varphi^{+} \parr \psi^{+} \mid \varphi^{-} \multimap \psi^{+} \mid !\varphi^{+} \\
\varphi^{-}, \psi^{-} & ::= & \varphi^{\pm} \mid \forall x^{A^{\omega}}.\varphi^{-} \mid \varphi^{-} \otimes \psi^{-} \mid \varphi^{-} \parr \psi^{-} \mid \varphi^{+} \multimap \psi^{-} \mid ?\varphi^{-} \\
\\
\varphi, \psi & ::= & \varphi^{+} \mid \varphi^{-} \mid \exists x^{A^{\omega}}.\varphi \mid \forall x^{A^{\omega}}.\varphi \mid \varphi \otimes \psi \mid \varphi \parr \psi \mid \varphi \multimap \psi
\end{array}
$$

Figure 4.1: Formulas of LSFOM

The formal system LSFOM Formulas of LSFOM are given inductively by the grammar of Figure 4.1, where φ^{+} refers to *positive formulas*, φ^{-} to *negative formulas* and $\varphi^{\pm}$ to deterministic formulas. As for FOM and SFOM, the atomic formulas consist only of equalities between terms of the same sort and quantifications are sorted. The main connectives are those of classical multiplicative linear logic with multisorted first-order quantifications:

- $\otimes$ is the multiplicative conjunction, the linear counterpart to $\wedge$. If φ and ψ are of polarity p, so is $\varphi \otimes \psi$.

- $\parr$ is the multiplicative disjunction, the linear counterpart to $\vee$.

- $\multimap$ is the linear implication, the counterpart to $\to$. $\varphi \multimap \psi$ is polarized only when φ and ψ are of opposite polarities. In particular, linear negation defined as $- \multimap \bot$ inverts polarity.

- $\exists x^{A^{\omega}}.\varphi$, if polarized, is necessarily positive. Furthermore, this enforces that φ should also be positive. Similarly, $\forall x^{A^{\omega}}.\varphi$, if polarized, is necessarily negative.

As is customary, we write $\varphi \multimap\!\!\circ\, \psi$ for the formula $(\varphi \multimap \psi) \otimes (\psi \multimap \varphi)$ and say that φ and ψ are (linearly) equivalent when $\varphi \multimap\!\!\circ\, \psi$ is derivable.

As such, this polarity system is more liberal than most of those found in linear systems such as LLP for instance [44]. The only reason we have to offer comes from the correspondence with automata, rather than proof-theoretic considerations closely related to linear logic.

The main technical reason why we need to introduce polarized formulas are the exponential modalities ! and ?, which are not defined for general LSFOM formulas. The main reason for this lack of a definition is that, to our knowledge, there is no computationally easy interpretation of general ! or ? modalities corresponding to *dealternation*. While it is known how to dealternate infinite word automata, the difficulty lies in interpreting the promotion rule of linear logic. A solution is investigated in the more general setting of tree automata for ! in [61], but this option complicates the interpretation of proofs in the realizability model significantly; we elect not to adapt it here.

As for deduction in LSFOM, it is carried out in the sequent calculus presented in Figure 4.2 augmented with the axioms presented in Figure 4.3. This sequent calculus is a straightforward extension of the calculus for *Full Intuitionistic Multiplicative Linear Logic* (FIMLL) presented in [34], with rules for the exponential modalities, first-order quantifications, and equalities. The system departs from usual sequent calculus for classical logic in the following ways:

- As heralded earlier, the system is linear and the structural rules of contraction and weakening may only apply to formulas under a suitable exponential modality.

- As in *classical* multiplicative linear logic, a sequent formally consists of two lists of legal LSFOM formulas. Unlike intuitionistic linear logic, the right-hand side sequents may be arbitrarily large and not of size at most one. The reason we do not get classical multiplicative linear logic is because this restriction is reinstated at the level of the left rule for $\multimap$ and right rule for $\forall$. This means in particular that $((\varphi \multimap \bot) \multimap \bot) \multimap \varphi$ is not derivable and that we do not have $\varphi \parr \psi \;\multimap\!\!\circ\; ((\varphi \multimap \bot) \otimes (\psi \multimap \bot)) \multimap \bot$ in general. The only relation we retain between $\parr$ and $\otimes$ is the distributive law $\varphi \otimes (\psi \parr \psi') \multimap (\varphi \otimes \psi) \parr \psi'$.

- All formulas appearing in Figure 4.2 are assumed to be syntactically correct LSFOM formulas as given by the grammar in Figure 4.1. In particular, every formula appearing under an exponential modality is necessarily polarized. This is the reason why we refrain from baptizing this proof system as something like "full first-order multiplicative exponential linear logic with equalities".

The axioms presented in Figure 4.3 fall into two categories: general axiom schemes related to polarized formulas and axioms translated from FOM (i.e., the system of axioms presented in Figure 2.6). The latter serve to embed FOM in LSFOM thanks to a translation $(-)^L$ we detail in Figure 4.4. The former, while also playing an decisive rôle in embedding FOM, is of more importance. It essentially states that polarized formulas are stable under double linear negation and that positive (respectively negative) formulas are stable under ! (respectively ?). As a consequence, one may reason in the deterministic fragment of LSFOM as in classical logic. We collect the relevant de Morgan dualities in the following proposition.

Proposition 4.1.4. *The following linear equivalences are derivable in* LSFOM *for all formulas with the displayed polarities, taking $p \in \{+,-\}$ to be some polarity and writing $\overline{p}$ for its opposite.*

$$\begin{array}{rcl} \bot \multimap \bot & \multimap & \mathbf{I} \\ (\varphi^p \otimes \psi^p) \multimap \bot & \multimap & (\varphi^p \multimap \bot) \parr (\psi^p \multimap \bot) \\ (?\exists x^{A^\omega}.\varphi^\pm) \multimap \bot & \multimap & !\forall x^{A^\omega}.\varphi^\pm \multimap \bot \\ \varphi^{\overline{p}} \multimap \psi^p & \multimap & (\varphi^{\overline{p}} \multimap \bot) \parr \psi^p \end{array} \qquad \begin{array}{rcl} \mathbf{I} \multimap \bot & \multimap & \bot \\ (\varphi^p \parr \psi^p) \multimap \bot & \multimap & (\varphi^p \multimap \bot) \otimes (\psi^p \multimap \bot) \\ (!\forall x^{A^\omega}.\varphi^\pm) \multimap \bot & \multimap & ?\exists x^{A^\omega}.\varphi^\pm \multimap \bot \end{array}$$

Moreover, we have the following linear entailments.

$$\begin{array}{rcl} \varphi^+ & \multimap & \mathbf{I} \\ \varphi_1^+ \otimes \varphi_2^+ & \multimap & \varphi_i^+ \end{array} \qquad \begin{array}{rcl} \bot & \multimap & \varphi^- \\ \varphi_i^- & \multimap & \varphi_1^- \parr \varphi_2^- \end{array}$$

Proof. We do not spell out all the proofs in full here, but let us treat the equivalence between $(!\forall x^{A^\omega}.\varphi^\pm) \multimap \bot$ and $?\exists x^{A^\omega}.\varphi^\pm \multimap \bot$ by way of example. The right-to-left implication is obtained as a routine derivation in intuitionistic linear logic.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi^\pm \vdash \varphi^\pm}}{\forall x^{A^\omega}.\varphi^\pm \vdash \varphi^\pm} \quad \dfrac{}{\bot \vdash}}{\varphi^\pm \multimap \bot, \forall x^{A^\omega}.\varphi^\pm) \vdash}}{\varphi^\pm \multimap \bot, !\forall x^{A^\omega}.\varphi^\pm) \vdash}}{\exists x^{A^\omega}.\varphi^\pm \multimap \bot, !\forall x^{A^\omega}.\varphi^\pm) \vdash}}{?\exists x^{A^\omega}.\varphi^\pm \multimap \bot, !\forall x^{A^\omega}.\varphi^\pm) \vdash}}{?\exists x^{A^\omega}.\varphi^\pm \multimap \bot, !\forall x^{A^\omega}.\varphi^\pm) \vdash \bot}}{?\exists x^{A^\omega}.\varphi^\pm \multimap \bot \vdash (!\forall x^{A^\omega}.\varphi^\pm) \multimap \bot}$$

The left-to-right implication on the other hand makes explicit use of the additional axioms $?\varphi^\pm \multimap \varphi^\pm$ together with the extended right rule for $\multimap$ in presence of exponential contexts.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi^\pm \vdash \varphi^\pm}}{\varphi^\pm \vdash ?\varphi^\pm}}{\varphi^\pm \vdash ?\varphi^\pm, \bot}}{\vdash ?\varphi^\pm, \varphi^\pm \multimap \bot} \quad \dfrac{}{\varphi^\pm \vdash \varphi}}{?\varphi^\pm \multimap \varphi^\pm \vdash \varphi^\pm, \varphi^\pm \multimap \bot}}{\vdash ?\varphi^\pm \multimap \varphi^\pm}}{\vdash \varphi^\pm, \varphi^\pm \multimap \bot}}{\vdash \varphi^\pm, \exists x^{A^\omega}.\varphi^\pm \multimap \bot}}{\vdash \varphi^\pm, ?\exists x^{A^\omega}.\varphi^\pm \multimap \bot}}{\vdash \forall x^{A^\omega}.\varphi^\pm, ?\exists x^{A^\omega}.\varphi^\pm \multimap \bot}}{\vdash !\forall x^{A^\omega}.\varphi^\pm, ?\exists x^{A^\omega}.\varphi^\pm \multimap \bot} \quad \dfrac{}{\bot \vdash}}{(!\forall x^{A^\omega}.\varphi^\pm) \multimap \bot \vdash ?\exists x^{A^\omega}.\varphi^\pm \multimap \bot}$$

□

Remark. *Since the axioms in Figure 4.3 imply that our positive formulas are "stable" under ! and that, dually, negative are stable under ?, means that the following generalized weakening and contraction rules are derivable in* SFOM*.*

$$\dfrac{\overline{\varphi} \vdash \overline{\varphi'}}{\overline{\varphi}, \psi^+ \vdash \overline{\varphi'}} \qquad \dfrac{\overline{\varphi} \vdash \overline{\varphi'}}{\overline{\varphi} \vdash \psi^-, \overline{\varphi'}}$$

$$\dfrac{\overline{\varphi}, \psi^+, \psi^+ \vdash \overline{\varphi'}}{\overline{\varphi}, \psi^+ \vdash \overline{\varphi'}} \qquad \dfrac{\overline{\varphi} \vdash \psi^-, \psi^-, \overline{\varphi'}}{\overline{\varphi} \vdash \psi^-, \overline{\varphi'}}$$

$$\frac{}{\varphi \vdash \varphi} \qquad \frac{\overline{\varphi} \vdash \gamma, \overline{\varphi}' \qquad \overline{\psi}, \gamma \vdash \overline{\psi}'}{\overline{\varphi}, \overline{\psi} \vdash \overline{\varphi}', \overline{\psi}'} \qquad \frac{\overline{\varphi}, \varphi, \psi, \overline{\psi} \vdash \overline{\varphi}'}{\overline{\varphi}, \psi, \varphi, \overline{\psi} \vdash \overline{\varphi}'} \qquad \frac{\overline{\varphi} \vdash \overline{\varphi}', \varphi, \psi, \overline{\psi}'}{\overline{\varphi} \vdash \overline{\varphi}', \psi, \varphi, \overline{\psi}'}$$

$$\frac{\overline{\psi} \vdash \overline{\psi}'}{\overline{\psi}, !\varphi \vdash \overline{\psi}'} \qquad \frac{\overline{\psi}, !\varphi, !\varphi \vdash \overline{\psi}'}{\overline{\psi}, !\varphi \vdash \overline{\psi}'} \qquad \frac{\overline{\varphi}, \varphi \vdash \overline{\varphi}'}{\overline{\varphi}, !\varphi \vdash \overline{\varphi}'} \qquad \frac{!\overline{\varphi} \vdash \varphi, ?\overline{\psi}}{!\overline{\varphi} \vdash !\varphi, ?\overline{\psi}}$$

$$\frac{\overline{\psi} \vdash \overline{\psi}'}{\overline{\psi} \vdash ?\varphi, \overline{\psi}'} \qquad \frac{\overline{\psi} \vdash ?\varphi, ?\varphi, \overline{\psi}'}{\overline{\psi} \vdash ?\varphi, \overline{\psi}'} \qquad \frac{\overline{\varphi} \vdash \varphi, \overline{\varphi}}{\overline{\varphi} \vdash ?\varphi, \overline{\varphi}} \qquad \frac{!\overline{\varphi}, \varphi \vdash ?\overline{\psi}}{!\overline{\varphi}, ?\varphi \vdash ?\overline{\psi}}$$

$$\frac{}{\vdash \mathbf{I}} \qquad \frac{\overline{\varphi}, \varphi, \psi \vdash \overline{\varphi}'}{\overline{\varphi}, \varphi \otimes \psi \vdash \overline{\varphi}'} \qquad \frac{\overline{\varphi} \vdash \varphi, \overline{\varphi}' \qquad \overline{\psi} \vdash \psi, \overline{\psi}'}{\overline{\varphi}, \overline{\psi} \vdash \varphi \otimes \psi, \overline{\varphi}', \overline{\psi}'}$$

$$\frac{\overline{\varphi} \vdash \varphi, \overline{\varphi}' \qquad \overline{\psi}, \psi \vdash \overline{\psi}'}{\overline{\varphi}, \overline{\psi}, \varphi \multimap \psi \vdash \overline{\varphi}', \overline{\psi}'} \qquad \frac{\overline{\varphi}, \varphi \vdash \psi}{\overline{\varphi} \vdash \varphi \multimap \psi} \qquad \frac{!\overline{\varphi}, \varphi \vdash \psi, ?\overline{\psi'}}{!\overline{\varphi} \vdash \varphi \multimap \psi, ?\overline{\psi'}}$$

$$\frac{}{\bot \vdash} \qquad \frac{\overline{\varphi}, \varphi \vdash \overline{\varphi}' \qquad \overline{\psi}, \psi \vdash \overline{\psi}'}{\overline{\varphi}, \overline{\psi}, \varphi \parr \psi \vdash \overline{\varphi}', \overline{\psi}'} \qquad \frac{\overline{\varphi} \vdash \varphi, \psi, \overline{\varphi}'}{\overline{\varphi} \vdash \varphi \parr \psi, \overline{\varphi}'}$$

$$\frac{\overline{\varphi}, \varphi[\mathtt{t}/x] \vdash \overline{\varphi}'}{\overline{\varphi}, \forall x^{A^\omega}.\varphi \vdash \overline{\varphi}'} \qquad \frac{\overline{\varphi} \vdash \varphi}{\overline{\varphi} \vdash \forall z^{A^\omega}.\varphi} \qquad \frac{!\overline{\varphi} \vdash \varphi, ?\overline{\varphi'}}{!\overline{\varphi} \vdash \forall z^{A^\omega}.\varphi, ?\overline{\varphi'}}$$

$$\frac{\overline{\varphi}, \varphi \vdash \overline{\varphi}'}{\overline{\varphi}, \exists z^{A^\omega}.\varphi \vdash \overline{\varphi}'} \qquad \frac{\overline{\varphi} \vdash \varphi[\mathtt{t}/X], \overline{\varphi}'}{\overline{\varphi} \vdash \exists x^{A^\omega}.\varphi, \overline{\varphi}'}$$

$$\frac{}{\overline{\varphi} \vdash \mathtt{t} = \mathtt{t}} \qquad \frac{\overline{\varphi} \vdash \phi(\mathtt{t}) \qquad \overline{\varphi} \vdash \mathtt{t} = \mathtt{u}}{\overline{\varphi} \vdash \phi(\mathtt{u})}$$

Figure 4.2: The Deduction Rules of LSFOM (where A is an alphabet, z^{A^ω} a variable fresh for $\overline{\varphi}, \overline{\varphi'}$ in each rule mentioning it).

These rules actually subsume the relevant structural rules given in Figure 4.2 and could have been used instead. These were in fact the original rules given in our original paper [58].

Translation of FOM into LSFOM A translation from the classical FOM formulas to LSFOM formulas is given in Figure 4.4. This translation is not a usual embedding of classical logic into (intuitionistic) linear logic, such as a double negation translation followed by Girard's translation of intuitionistic logic in linear logic using the decomposition $\neg\varphi \equiv !\varphi \multimap \bot$. One reason for this is that, depending on the choice of double negation translation, this may not even make sense due to our restricted exponentials and a polarity mismatch. The real reason is that the additional polarity axioms of 4.3 allow for a much simpler translation $(-)^L$ given in Figure 4.4. The main invariant that is kept and allow to reason "as in FOM" is the following.

Lemma 4.1.5. *For every* FOM *formula φ, its translation φ^L is deterministic.*

Lemma 4.1.5 together with our previous remarks thus allow us to show the following.

Lemma 4.1.6. *If* $\mathsf{FOM} \vdash \varphi$, *then* $\mathsf{LSFOM} \vdash \varphi^L$.

Proof. By induction over a potential derivation of $\overline{\varphi} \vdash \psi$ in FOM, we show that $\overline{\varphi^L} \vdash \psi^L$ is derivable in LSFOM. Given that we have taken a presentation based on natural deduction in Figure 3.1 and that structural rules may be applied freely as all formulas under consideration are deterministic, this amounts to showing that sequent calculus is conservative over natural deduction which is standard. The additional rule allowing classical logic

$$\frac{\overline{\varphi}, \neg\psi \vdash \bot}{\overline{\varphi} \vdash \psi}$$

amounts to double-negation elimination, which is given by linear double-negation elimination over deterministic formulas. Finally, one has to consider the axioms of FOM, given in Figure 2.6. It is

Polarity axioms

$$\begin{array}{ll}
\varphi^+ \multimap\!\!\!\!\circ\; !\varphi^+ & \text{(where } \varphi^+ \text{ is positive)} \\
?\varphi^- \multimap\!\!\!\!\circ\; \varphi^- & \text{(where } \varphi^- \text{ is negative)} \\
(\varphi^p \multimap \bot) \multimap \bot \multimap\!\!\!\!\circ\; \varphi^p & \text{with } p \in \{+,-,\pm\} \text{ (i.e., } \varphi \text{ is polarized)}
\end{array}$$

FOM axioms

$$\begin{array}{ll}
\forall x_1^{A_1^\omega} \ldots \forall x_n^{A_n^\omega}.\mathtt{t}(x_1,\ldots,x_n) = \mathtt{u}(x_1,\ldots,x_n) & \text{when } [\![\mathtt{t}]\!] = [\![\mathtt{u}]\!] \\
\forall x^{A^\omega} y^{A^\omega}.\mathbf{cons}_a(x) = \mathbf{cons}_a(y) \multimap x = y) & \text{where } a \in A \text{ and } x, y \text{ of sort } A^\omega \\
\forall x^{A^\omega} y^{A^\omega}.\mathbf{cons}_a(x) = \mathbf{cons}_b(y) \multimap \bot & \text{where } a, b \in A \text{ with } a \neq b
\end{array}$$

$$\begin{array}{ll}
\varphi(\dot{\mathsf{Z}}) \otimes \big(!\forall x^{2^\omega}.\ [x \in \mathbb{N} \otimes \varphi^\pm(x)] \multimap \varphi^\pm(\dot{\mathsf{S}}(x))\big) \quad \multimap\!\!\!\!\circ \quad !\forall x^{2^\omega}.\ x \in \mathbb{N} \multimap \varphi^\pm(x))) & \\
?\exists x^{2^\omega} !\forall n^{2^\omega}.\ n \in \mathbb{N} \multimap \big(\varphi^\pm(n) \multimap\!\!\circ\; \dot{\mathsf{In}}(n,x)\big) & \text{where } x \text{ does not occur in } \varphi \\
t = u \quad \multimap\!\!\circ \quad \Big(\forall n^{2^\omega}.n \in \mathbb{N} \quad \multimap \quad \chi^L_{[\![t]\!]}(n) \multimap\!\!\circ\; \chi^L_{[\![u]\!]}(n)\Big) &
\end{array}$$

Figure 4.3: Axioms of LSFOM (where $n \in \mathbb{N}$ is defined as $\mathbb{N}_\infty(n) = 1^\omega \otimes (n = 0^\omega \multimap \bot)$ and $\mathbb{N}_\infty$, $\dot{\mathsf{Z}}$, $\dot{\mathsf{S}}$ and $\dot{\mathsf{In}}$ as in Figure 2.4.)

rather easy to see that they are in one-to-one correspondence with those of LSFOM. Also note that the restriction of the induction and comprehension schemes to deterministic formulas in Figure 4.3 is unproblematic since $(-)^L$ only produces deterministic formulas. □

Once again, $(-)^L$ is not the only syntactic embedding of FOM into LSFOM. We sketch below two alternatives.

Translating SFOM to FOM It is possible to give the following translation of SFOM formulas $(-)^{LS}$ into LSFOM preserving derivability.

$$\begin{array}{rclcrcl}
(\mathtt{t} = \mathtt{u})^{LS} & := & \mathtt{t} = \mathtt{u} & & (\varphi \wedge \psi)^{LS} & := & \varphi^{LS} \otimes \psi^{LS} \\
(\neg\varphi)^{LS} & := & (?\varphi^{LS}) \multimap \bot & & (\exists x^{A^\omega}.\varphi)^{LS} & := & \exists x^{A^\omega}.\varphi^{LS}
\end{array}$$

Here, the crucial invariant is that a formula φ^{LS} is necessarily *positive*, and thus subject to contraction and weakening on the left. This allows to prove that SFOM $\vdash \varphi$ implies LSFOM $\vdash \varphi^{LS}$, a statement analogous to Lemma 4.1.6. Together with Lemma 3.1.4, this shows that FOM $\vdash \varphi$ implies LSFOM $\vdash (\neg\neg\varphi)^{LS}$, which provides us an alternative (less efficient) way of embedding FOM in LSFOM. This does not matter very much in the end, as it may be noted that for every FOM formula φ, LSFOM shows that φ^L, $?\varphi^{LS}$ and $(\neg\neg\varphi)^{LS}$ are equivalent.

Double-negation and Girard's translation Finally, let us note that there is a way of making a double-negation translation followed by Girard's translation work, provided the double-negation translation allows for universal quantification in its target, so that $(\exists x^{A^\omega}.\varphi)^{\neg\neg} = \neg\forall x^{A^\omega}.\neg\varphi^{\neg\neg}$. Dubbing $(-)^{\neg\neg G}$ the resulting translation FOM $\to$ LSFOM, we would have the clauses

$$\begin{array}{rclcrcl}
(\mathtt{t} = \mathtt{u})^{\neg\neg G} & := & \mathtt{t} = \mathtt{u} & & (\varphi \wedge \psi)^{\neg\neg G} & := & \varphi^{\neg\neg G} \otimes \psi^{\neg\neg G} \\
(\neg\varphi)^{\neg\neg G} & := & (!\varphi^{\neg\neg G}) \multimap \bot & & (\exists x^{A^\omega}.\varphi)^{\neg\neg G} & := & !(\forall x^{A^\omega}.!\varphi^{\neg\neg G} \multimap \bot) \multimap \bot \\
(\varphi \Rightarrow \psi)^{\neg\neg G} & := & \varphi^{\neg\neg G} \multimap \psi^{\neg\neg G} & & (\varphi \vee \psi)^{\neg\neg G} & := & !((!\varphi^{\neg\neg G} \multimap \bot) \otimes (!\psi^{\neg\neg G} \multimap \bot)) \multimap \bot \\
(\forall x^{A^\omega}.\varphi)^{\neg\neg G} & := & \forall x^{A^\omega}.\varphi^{\neg\neg G} & &
\end{array}$$

Here, the natural polarity invariant this time is that $\varphi^{\neg\neg G}$ is always negative because of the optimized translation of $\forall$. Once again a straightforward induction over φ shows that φ^L and $!\varphi^{\neg\neg G}$ are equivalent according to LSFOM.

4.2 The realizability model

We now turn to the automata interpretation of LSFOM. Similar as to what was done in Section 3.2, we are going to describe several automata theoretic constructions corresponding to the various

$$
\begin{array}{rcl@{\qquad}rcl}
(\mathtt{t} = \mathtt{u})^L & := & \mathtt{t} = \mathtt{u} & (\varphi \wedge \psi)^L & := & \varphi^L \otimes \psi^L \\
(\neg\varphi)^L & := & \varphi^L \multimap \bot & (\exists x^{A^\omega}.\varphi)^L & := & ?\exists x^{A^\omega}.\varphi^L \\
(\varphi \vee \psi)^L & := & \varphi^L \parr \psi^L & (\varphi \Rightarrow \psi)^L & := & \varphi^L \multimap \psi^L \\
(\forall x^{A^\omega}.\varphi)^L & := & !\forall x^{A^\omega}.\varphi^L & & &
\end{array}
$$

Figure 4.4: The translation $(-)^L$ of FOM into LSFOM.

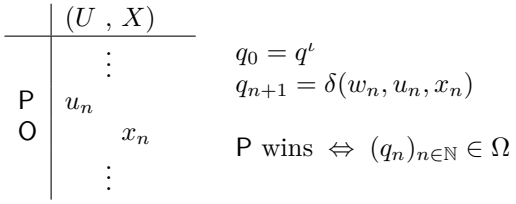


Figure 4.5: Acceptance game for $(Q, q^\iota, U, X, \delta, \Omega) : A$ over $w \in A^\omega$.

connectives of LSFOM and their behaviour both with respect to recognized languages and an extended notion of simulation between automata, which once again refines language inclusion. Those properties will then imply the soundness of FOM with respect to simulations: if $\varphi \multimap \psi$ is provable, then there is a simulation between the underlying automata.

The main difference is that basic constructions made on automata may not always behave nicely with respect to the recognized languages, but they will always be sound for deduction in LSFOM. However, it will also be clear that they behave nicely at the level of languages when considering automata arising as the interpretation of polarized formulas.

This section does not contain complete proofs of soundness and is mostly meant to convey intuitions. In particular, we will only keep a rather high-level description of the simulations between automata for now. The full proofs for an extended higher-order setting are postponed to Chapter 6.

Before defining simulations, or rather, simulation games, notice that acceptance of a word by an alternating uniform automaton $(Q, q^\iota, U, X, \delta, \Omega) : A$ (Definition 4.1.1) is defined in terms of a game-like scenario pictured in Figure 4.5. Given a word $w \in A^\omega$, we may imagine that two players P and O play an infinite game: at each round $n \in \mathbb{N}$, P plays a move $u_n \in U$ and O answers with $x_n \in X$. This yields two sequences $(u_n)_{n\in\mathbb{N}}$ and $(x_n)_{n\in\mathbb{N}}$. Together with w, they yield a run $(q_n)_{n\in\mathbb{N}}$ in the automaton. Say that P wins if and only if $(q_n)_{n\in\mathbb{N}} \in \Omega$. Then it is clear that Definition 4.1.1 says that w is accepted if and only if P has a winning strategy in this acceptance game.

Now, the proofs of LSFOM will be interpreted as winning strategies in a *simulation game* between two automata over the same alphabet pictured in Figure 4.6.

Definition 4.2.1. *Given two uniform automata*

$$\mathcal{A} = (Q_\mathcal{A}, q^\iota_\mathcal{A}, U, X, \delta_\mathcal{A}, \Omega_\mathcal{A}) : A \quad \textit{and} \quad \mathcal{B} = (Q_\mathcal{B}, q^\iota_\mathcal{B}, V, Y, \delta_\mathcal{B}, \Omega_\mathcal{B}) : A$$

define the simulation game between P *and* O *as the game where* P *and* O *play as follow at round* $n \in \mathbb{N}$*:*

- O *plays a letter* $a_n \in A$ *and a move* $u_n \in U$*.*
- P *answers with a move* $v_n \in V$*.*
- O *answers with a move* $y_n \in Y$*.*
- P *concludes the round by a move* $x_n \in X$*.*

A play may be seen as a sequence $\langle a, u, x, v, y\rangle \in (A \times U \times X \times V \times Y)^\omega$*. We say that* P *is winning if and only if whenever* $\langle u, x\rangle$ *is an accepting play over* a *in* $\mathcal{A}$*,* $\langle v, y\rangle$ *is an accepting play over* a *in* $\mathcal{B}$*.*

If such a winning strategy exists in a simulation game from $\mathcal{A} : A$ *to* $\mathcal{B} : A$*, write* $\mathcal{A} \Vdash \mathcal{B}$*.*

This simulation game departs from the aforementioned acceptance game in two essential ways:

- First, since two automata $\mathcal{A} : A$ and $\mathcal{B} : A$ are involved, a winning strategy for P is now chiefly be concerned with building an accepting run in $\mathcal{B}$ using an accepting run of $\mathcal{A}$ as input.

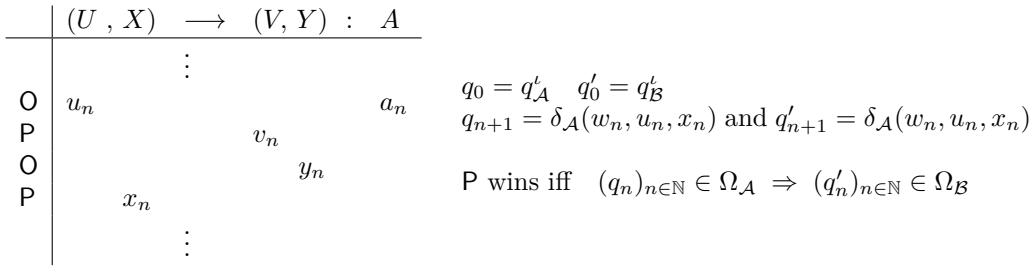


Figure 4.6: Simulation game between $\mathcal{A} : A$ and $\mathcal{B} : A$

- Second, the word $w \in A^\omega$ over which $\mathcal{A}$ and $\mathcal{B}$ run not be known in advance by P. It is rather gradually revealed by O.

In concrete terms, a P-strategy in the aforementioned game can be seen as a pair of sequences of functions $(f_n, F_n)_{n\in\mathbb{N}}$ with the following types.

$$f_n : A^{n+1} \times U^{n+1} \times X^n \to V \qquad F_n : A^{n+1} \times U^{n+1} \times X^{n+1} \to Y^{n+1}$$

There are, of course, highly uncomputable such sequences in the wild; to remedy this, note that these sequences induce a canonical causal function $(A \times U \times X)^\omega \to (V \times Y)^\omega$; the converse is not quite true, but this datum still characterizes the strategy. We say that the strategy is *finite-state* if this function is. We may also call winning P-strategies simulations for short in the sequel. For the remainder of this section, we shall not define formally combinators for strategies in simulation games and leave that for Chapter 6. While Chapter 6 does not nominally prove that the strategies interpreting proof rules are finite-state as it deals with generalized higher-order strategies, the subsequent discussion in Chapter 7 explains how the constructions detailed in Chapter 6 restricted to the current setting actually produce finite-state strategies.

One appeal of simulation games is their tight connexion to the games involved in the Büchi-Landweber theorem (Theorem 2.3.1. In particular, a simple reduction shows that those games are also determined in finite memory.

Lemma 4.2.2. *There exists an algorithm taking as input uniform automata $\mathcal{A}$ and $\mathcal{B}$ and returning a finite-state winning strategy for either* P *or* O *in the simulation game between $\mathcal{A}$ and $\mathcal{B}$.*

While this connexion is interesting, let us note that we do not rely on Lemma 4.2.2 to build P-strategies corresponding to the interpretation of proofs.

Now, let us turn to the relationship between simulations and the languages recognized by uniform automata.

Lemma 4.2.3. *Let $\mathcal{A}, \mathcal{B} : A$ be uniform alternating automata. We always have*

$$\mathcal{A} \Vdash \mathcal{B} \quad \Rightarrow \quad \mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$$

Proof. It is rather straightforward from the design of the simulation game that, if an input word $w \in A^\omega$ is fixed, the winning P-strategy in the simulation game can be leveraged to turn a winning strategy in the acceptance game of w by $\mathcal{A}$ into a winning P-strategy in the acceptance game of w by $\mathcal{B}$. □

As with the particular case of uniform non-deterministic automata, the converse does not hold in general, but it can be recovered in the particular case where the automata $\mathcal{A}$ and $\mathcal{B}$ have the suitable polarity.

Lemma 4.2.4. *Let $\mathcal{A}$ be a non-deterministic uniform automaton and $\mathcal{B}$ be uniform universal automaton over the same alphabet A. Then we have*

$$\mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B}) \quad \Leftrightarrow \quad \mathcal{A} \Vdash \mathcal{B}$$

Proof. Note that in that case, there is a unique P-strategy in the simulation game. It is straightforward to check that it is winning if and only $\mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$. □

Another essential aspect that we need to cover before defining the operation analogous to the connectives is composition of winning strategies in simulation games. This is important to have a sound interpretation of the axiom and cut rules of LSFOM which may be informally be transcribed as follows in the semantics

$$\frac{}{\mathcal{A} \Vdash \mathcal{A}} \qquad \frac{\mathcal{A} \Vdash \mathcal{B} \qquad \mathcal{B} \Vdash \mathcal{C}}{\mathcal{A} \Vdash \mathcal{C}}$$

For the rest of this section, fix the following notations for the automata $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$.

$$\begin{array}{rcl} \mathcal{A} & = & (Q_{\mathcal{A}},\ q^{\iota}_{\mathcal{A}},\ U,\ X,\ \delta_{\mathcal{A}},\ \Omega_{\mathcal{A}}) \ : \ A \\ \mathcal{B} & = & (Q_{\mathcal{B}},\ q^{\iota}_{\mathcal{B}},\ V,\ Y,\ \delta_{\mathcal{B}},\ \Omega_{\mathcal{B}}) \ : \ A \\ \mathcal{C} & = & (Q_{\mathcal{C}},\ q^{\iota}_{\mathcal{C}},\ W,\ Z,\ \delta_{\mathcal{C}},\ \Omega_{\mathcal{C}}) \ : \ A \end{array}$$

Lemma 4.2.5. *For every automata $\mathcal{A} : A$, there is a simulation $\mathcal{A} \Vdash \mathcal{A}$. For every automata $\mathcal{A}, \mathcal{B}, \mathcal{C} : A$ and simulations $\mathcal{A} \Vdash \mathcal{B}$ and $\mathcal{B} \Vdash \mathcal{C}$, we may compute a simulation $\mathcal{A} \Vdash \mathcal{C}$.*

Proof sketch. The constructions of those simulations follow well-known patterns in *game semantics* [1, 32] The simulation $\mathcal{A} \Vdash \mathcal{A}$ corresponds to a copycat strategy that may be pictured as follows

	$(U\ ,\ X)$	$\longrightarrow$	$(U,\ X)$	:	A
			$\vdots$		
O	u_n				a_n
P			u_n		
O				x_n	
P		x_n			
			$\vdots$		

On the other hand, $\mathcal{A} \Vdash \mathcal{C}$ corresponds to simulating both strategies $\mathcal{A} \Vdash \mathcal{B}$ and $\mathcal{B} \Vdash \mathcal{C}$ over an extended board and hiding the interaction, materialized below as the middle column.

	$(U\ ,\ X)$	$\longrightarrow$	$(V,\ Y)$	$\longrightarrow$	$(W,\ Z)$	:	A
			$\vdots$				
O	u_n						a_n
			v_n				
P					w_n		
O						z_n	
			y_n				
O		x_n					
			$\vdots$				

□

Now, we are ready to discuss the logical connectives.

Propositional connectives Linear conjunction $\mathcal{A} \otimes \mathcal{B}$ and disjunction $\mathcal{A} \parr \mathcal{B}$ will be interpreted by a standard constructions over non-deterministic/universal automata with state-space of size $|Q_{\mathcal{A}}| \times |Q_{\mathcal{B}}|$.

Remark. *We could have also considered the additive variant of the construction where the state space is proportional to $|Q_{\mathcal{A}}| + |Q_{\mathcal{B}}|$ and which generalizes to alternating automata. This option is natural and seems to be a natural step toward interpreting the additive connectives $\oplus$ and & of linear logic. These constructions however are rather cumbersome with our rather rigid notion of uniform alternating automata; with some effort we could have a* weak *version of & without altering our definition.*

Definition 4.2.6. *Define the multiplicative conjunction automaton $\mathcal{A} \otimes \mathcal{B} : A$ and the disjunction automaton $\mathcal{A} \parr \mathcal{B} : A$ as follows.*

$$\begin{array}{rcl} \mathcal{A} \otimes \mathcal{B} & := & (Q_{\mathcal{A}} \times Q_{\mathcal{B}},\ (q^{\iota}_{\mathcal{A}}, q^{\iota}_{\mathcal{B}}),\ U \times V,\ X \times Y,\ \{\langle q, q' \rangle \mid q \in \Omega_{\mathcal{A}} \wedge q' \in \Omega_{\mathcal{B}}\}) \ : \ A \\ \mathcal{A} \parr \mathcal{B} & := & (Q_{\mathcal{A}} \times Q_{\mathcal{B}},\ (q^{\iota}_{\mathcal{A}}, q^{\iota}_{\mathcal{B}}),\ U \times V,\ X \times Y,\ \{\langle q, q' \rangle \mid q \in \Omega_{\mathcal{A}} \vee q' \in \Omega_{\mathcal{B}}\}) \ : \ A \end{array}$$

Define the associated unit automata

$$\mathbf{I} := (1, *, 1, 1, *, 1^{\omega}) : A \qquad\qquad \bot := (1, *, 1, 1, *, \emptyset) : A$$

Note that if $\mathcal{A}$ and $\mathcal{B}$ are Muller automata, so are $\mathcal{A} \otimes \mathcal{B}$ and $\mathcal{A} \parr \mathcal{B}$. Furthermore if both $\mathcal{A}$ and $\mathcal{B}$ are non-deterministic (resp. universal), so are $\mathcal{A} \otimes \mathcal{B}$ and $\mathcal{A} \parr \mathcal{B}$. The automata corresponding to the units are deterministic.

As announced, at the level of languages, we have the expected equalities.

Lemma 4.2.7. *For every automata $\mathcal{A}, \mathcal{B} : A$, we have*

$$\mathcal{L}(\mathcal{A} \otimes \mathcal{B}) = \mathcal{L}(\mathcal{A}) \cap \mathcal{L}(\mathcal{B}) \qquad \text{and} \qquad \mathcal{L}(\mathcal{A} \parr \mathcal{B}) = \mathcal{L}(\mathcal{A}) \cup \mathcal{L}(\mathcal{B})$$

Proof sketch. Let us concentrate on the case $\mathcal{A} \otimes \mathcal{B}$. If $w \in \mathcal{L}(\mathcal{A}) \cap \mathcal{L}(\mathcal{B})$, it means that we have winning strategies in the relevant acceptance games in both $\mathcal{A}$ and $\mathcal{B}$; they can easily be paired into a winning strategy for the acceptance of w in $\mathcal{A} \otimes \mathcal{B}$. Conversely, if $w \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$, there is a winning strategy for the acceptance game over w in $\mathcal{A} \otimes \mathcal{B}$. Fixing an arbitrary $y \in Y$, this can be turned into a winning strategy over w in $\mathcal{A}$ by pretending that opponent constantly plays y on the non-existent board corresponding to $\mathcal{B}$. □

At the level of simulations, we only require a modicum of structure to interpret sequents. Indeed, as a sequent $\overline{\varphi} \vdash \overline{\varphi'}$ is to be thought of as a simulation $\bigotimes \overline{[\![\varphi]\!]} \Vdash \parr \overline{[\![\varphi']\!]}$ in the semantics, it means that $\square \in \{\otimes, \parr\}$ should carry a symmetric monoidal structure and corresponding unit $J \in \{\bot, \mathbf{I}\}$[2]

- if $\mathcal{A} \Vdash \mathcal{B}$ and $\mathcal{A}' \Vdash \mathcal{B}'$, then $\mathcal{A} \square \mathcal{A}' \Vdash \mathcal{B} \square \mathcal{B}'$.
- we have $\mathcal{A} \square (\mathcal{B} \square \mathcal{C}) \Vdash (\mathcal{A} \square \mathcal{B}) \square \mathcal{C}$ and vice-versa.
- we have $\mathcal{A} \square J \Vdash \mathcal{A}$ and vice-versa.
- and finally, $\mathcal{A} \square \mathcal{B} \Vdash \mathcal{B} \square \mathcal{A}$.

These properties are completely straightforward to check. On top of that, since we are interpreting *full* intuitionistic linear logic, there should be a canonical distributive law

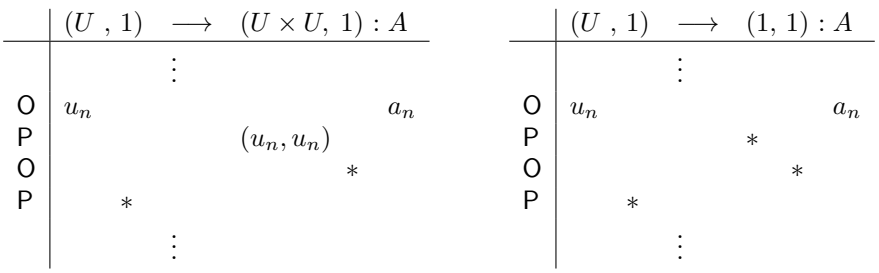
$$\mathcal{A} \otimes (\mathcal{B} \parr \mathcal{C}) \Vdash (\mathcal{A} \otimes \mathcal{B}) \parr \mathcal{C}$$

which is not much harder to check (if ignoring the spurious parentheses, the underlying automata have the same state-spaces, same moves, and there is an inclusion of acceptance conditions). The properties above are enough to guarantee that the basic left/right rules for $\mathbf{I}, \bot, \otimes$ and $\parr$ are interpreted in a sound way.

Before moving on, we are also ready to discuss the soundness of the generalized contraction and weakening rules. Recall that in LSFOM, contraction and weakening are tied to polarity restrictions which translate to restriction on the underlying automata interpretation. The reason behind this is that the following holds.

Lemma 4.2.8. *If $\mathcal{A} : A$ is a non-deterministic automaton, there are canonical simulations $\mathcal{A} \Vdash \mathcal{A} \otimes \mathcal{A}$ and $\mathcal{A} \Vdash \mathbf{I}$. Dually, if it is universal, there are canonical simulations $\mathcal{A} \parr \mathcal{A} \Vdash \mathcal{A}$ and $\bot \Vdash \mathcal{A}$.*

Proof sketch. Consider the case where $\mathcal{A}$ is non-deterministic. Then, the P-strategy in the simulation game from $\mathcal{A} \otimes \mathcal{A}$ to $\mathcal{A}$ duplicates O-moves as pictured below (where we confuse $1 \times 1 \simeq 1$ and $X \simeq 1$). Furthermore, there is a unique simulation $\mathcal{A} \Vdash \mathbf{I}$.



The universal case is entirely dual. □

Now we discuss the linear implication $- \multimap -$. Contrarily to most of the other operations discussed here, we are not aware of it occurring before in the automata-theoretic literature.

[2]We do not mention the usual coherence conditions for now, as they are not needed to interpret sequents. These are only alluded to in later chapters.

Definition 4.2.9. *Given automata $\mathcal{A}, \mathcal{B} : A$, define the automaton $\mathcal{A} \multimap \mathcal{B} : A$ as follows*

$$\mathcal{A} \multimap \mathcal{B} := (Q_{\mathcal{A}} \times Q_{\mathcal{B}}, (q^\iota_{\mathcal{A}}, q^\iota_{\mathcal{B}}), V^U \times X^{U\times Y}, U \times Y, \delta_{\mathcal{A}\multimap\mathcal{B}}, \Omega_{\mathcal{A}\multimap\mathcal{B}}) : A$$

$$\begin{array}{ll} \textit{with} & \delta_{\mathcal{A}\multimap\mathcal{B}}(a,(f,F),(u,y)) = (\delta_{\mathcal{A}}(a,u,F(u,y)), \delta_{\mathcal{B}}(a,f(u),y)) \\ \textit{and} & \Omega_{\mathcal{A}\multimap\mathcal{B}} = \{\langle q, q'\rangle \in (Q_{\mathcal{A}} \times Q_{\mathcal{B}})^\omega \mid q \in \Omega_{\mathcal{A}} \Rightarrow q' \in \Omega_{\mathcal{B}}\} \end{array}$$

Note that if $\mathcal{A}$ and $\mathcal{B}$ are Muller automata, then $\mathcal{A} \multimap \mathcal{B}$ is a Muller as well. If $\mathcal{A}$ is universal and $\mathcal{B}$ non-deterministic, $\mathcal{A} \multimap \mathcal{B}$ is non-deterministic, and dually, if $\mathcal{A}$ is non-deterministic and $\mathcal{B}$ universal, $\mathcal{A} \multimap \mathcal{B}$ is universal.

The rationale for the above definition, which is directly inspired from the definition of of the arrows in Dialectica categories [21], can be seen as the attempt to cram a simulation game within a single automaton without modifying the P-strategy. To wit, put side-by-side rounds of the simulation games from $\mathcal{A}$ to $\mathcal{B}$ and from $\mathbf{I}$ to $\mathcal{A} \multimap \mathcal{B}$.

	$(U\ ,\ X)$	$\longrightarrow$	$(V,\ Y)$	$:$	A
		$\vdots$			
O	u_n				a_n
P			v_n		
O				y_n	
P	x_n				
		$\vdots$			

	$(1\ ,\ 1)$	$\to$	$(V^U \times X^{U\times Y},$	$U\ \times Y)$	$:$	A
			$\vdots$			
O	$*$					a_n
P			f_n	F_n		
O					u_n	y_n
P	$*$					
			$\vdots$			

At the level of O, the game in $\mathcal{A} \multimap \mathcal{B}$ is actually more lenient than the vanilla simulation game, as it allows them to play their round knowing the strategy of P. This is not an issue as our notion of strategy is only concerned with P-strategies. For P, as they must move first in the right hand-side game, they are allowed to play functions that anticipate on the moves that opponent should have originally played in the left-hand side game: f_n corresponds to the move v_n which should be made after O provided u_n and F_n to x_n, which depends on both u_n and y_n. This dynamic is accordingly reflected at the level of the transition function $\delta_{\mathcal{A}\multimap\mathcal{B}}$.

In order to make the rules of LSFOM sound, one has to check that the following, corresponding to the monoidal closure of the category of uniform automata and simulations, holds.

Lemma 4.2.10. *If there is a simulation $\mathcal{A} \otimes \mathcal{B} \Vdash \mathcal{C}$, then there is a simulation $\mathcal{A} \Vdash \mathcal{B} \multimap \mathcal{C}$. Furthermore, there is a canonical simulation $(\mathcal{A} \multimap \mathcal{B}) \otimes \mathcal{A} \Vdash \mathcal{B}$.*

Proof sketch. For the first statement, the case $\mathcal{A} = \mathbf{I}$ is informally discussed above. Seeing that there is a one-to-one correspondence between simulations $\mathcal{A} \otimes \mathcal{B} \Vdash \mathcal{C}$ and $\mathcal{A} \Vdash \mathcal{B} \multimap \mathcal{C}$ does not take much more conceptual effort. This also implies the second half of the statement, but it is also instructive to picture concretely the strategy corresponding to $(\mathcal{A} \multimap \mathcal{B}) \otimes \mathcal{A} \Vdash \mathcal{B}$ as follows

	$(V^U \times X^{U\times Y},$	$U\ \times Y)$	$\otimes$	$(U\ ,\ X)$	$\longrightarrow$	$(\ V\ \ ,\ Y)$	$:$	A
				$\vdots$				
O	f_n	F_n		u_n				a_n
P						$f_n(u_n)$		
O							y_n	
P		u_n		$F_n(u_n, y_n)$				
				$\vdots$				

□

We are now ready to study double-linear negation. In all generality, the double-linear negation of a uniform automaton $\mathcal{A}$ is isomorphic to the following

$$(\mathcal{A} \multimap \bot) \multimap \bot \ \simeq\ (Q_{\mathcal{A}}, q^\iota, U^{X^U}, X^U, \delta_{(\mathcal{A}\multimap\bot)\multimap\bot}, \Omega_{\mathcal{A}}) : A$$

$$\text{with}\quad \delta_{(\mathcal{A}\multimap\bot)\multimap\bot}(a, F, f) = \delta_{\mathcal{A}}(a, F(f), f(F(f)))$$

We shall see much later that there is actually always a simulation $(\mathcal{A} \multimap \bot) \multimap \bot \Vdash \mathcal{A}$. However, there is apparently no straightforward way of computing such simulation, which goes against the philosophy dictating that extraction of realizers from proofs should be computationally easy, so we have not adopted the double linear negation elimination for LSFOM. However, it is straightforward

to check that if $\mathcal{A}$ is non-deterministic ($U \simeq 1$) or universal ($X \simeq 1$), then $(\mathcal{A} \multimap \bot) \multimap \bot$ is in fact isomorphic to $\mathcal{A}$; this justifies our adopting double linear negation elimination restricted to polarized formulas.

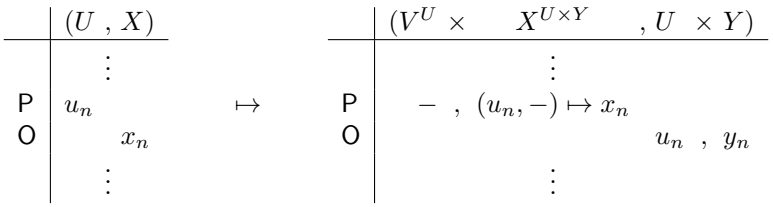
Before moving on, let us observe that $- \multimap -$ also implements correctly implication at the level of languages. Our argument relies crucially on the determinacy of simulation games.

Lemma 4.2.11. *For any uniform alternating automata $\mathcal{A}, \mathcal{B} : A$, we have*

$$\mathcal{L}(\mathcal{A} \multimap \mathcal{B}) = \{w \in A^\omega \mid w \in \mathcal{L}(\mathcal{A}) \Rightarrow w \in \mathcal{L}(\mathcal{B})\}$$

Proof sketch. The left-to-right inclusion is rather straightforward using previous Lemmas. By Lemma 4.2.10, there is a simulation $(\mathcal{A} \multimap \mathcal{B}) \otimes \mathcal{A} \Vdash \mathcal{B}$. Thus, by Lemma 4.2.3, we have $\mathcal{L}((\mathcal{A} \multimap \mathcal{B}) \otimes \mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$, and thus $\mathcal{L}(\mathcal{A} \multimap \mathcal{B}) \cap \mathcal{L}(\mathcal{A}) \subseteq \mathcal{L}(\mathcal{B})$ by Lemma 4.2.7. This is equivalent to the inclusion we were looking for.

The converse inclusion is more involved: suppose it is false for some $w \in A^\omega$. Then necessarily, $w \notin \mathcal{L}(\mathcal{B})$, otherwise we could lift the winning strategy in the acceptance game to $\mathcal{L}(\mathcal{A} \multimap \mathcal{B})$. So, by definition of the right-hand side, we have $w \notin \mathcal{L}(\mathcal{A})$ too. By determinacy of the acceptance games (Lemma 4.2.2), there is a winning O-strategy for the acceptance game in $\mathcal{A}$ over w, which can be seen as a family of maps $f_n : U^{n+1} \to X$. From this winning O-strategy, a winning P-strategy for the acceptance game in $\mathcal{A} \multimap \mathcal{B}$ over w may be built as in the picture below where $-$ denotes an arbitrary legal move.



More formally, the P-strategy in $\mathcal{A} \multimap \mathcal{B}$ consists of two sequences $h_n : U^n \times Y^n \to V^U$ and $H_n : U^n \times Y^n \to X^{U\times Y}$ such that $H_n((u_i)_{i<n}, (y_i)_{i<n})(u_n, y_n) = f_n((u_i)_{i\leq n}$ for every sequences $(u_i)_{i\leq n}$ and $(y_i)_{i\leq n}$ and h_n is arbitrary. □

Corollary 4.2.12. *For any uniform alternating automaton $\mathcal{A}$, $\mathcal{L}(\mathcal{A} \multimap \bot) = \mathcal{L}(\mathcal{A})^c$.*

Polarized exponentials As with the automata-theoretic interpretation of SFOM, we use McNaughton's theorem (Theorem 1.1.6) as a black box to define the interpretation of the exponentials.

Lemma 4.2.13. *For any uniform non-deterministic automaton $\mathcal{A} : A$, there is a deterministic automaton $?\mathcal{A} : A$ such that $\mathcal{L}(\mathcal{A}) = \mathcal{L}(?\mathcal{A})$. Dually, for a universal automaton $\mathcal{B} : A$, there is a deterministic automaton $!\mathcal{B} = ?(\mathcal{B} \multimap \bot) \multimap \bot : A$ such that $\mathcal{L}(\mathcal{B}) = \mathcal{L}(!\mathcal{B})$.*

For a non-deterministic automaton $\mathcal{A}$, we take $!\mathcal{A} = \mathcal{A}$, and similarly, for a universal automaton $\mathcal{B}$, we take $?\mathcal{B} = \mathcal{B}$. This still maintains the following crucial invariants:

- $\mathcal{L}(!\mathcal{A}) = \mathcal{L}(\mathcal{A})$ and $\mathcal{L}(?\mathcal{B}) = \mathcal{L}(\mathcal{B})$ whenever those automata are well-defined.
- Whenever defined, $!\mathcal{A}$ is non-deterministic and $?\mathcal{B}$ is universal.

Then, Lemma 4.2.4 shows that we readily have $\mathcal{A} \Vdash ?\mathcal{A}$ and that, dually $!\mathcal{B} \Vdash \mathcal{B}$. This justifies the dereliction rules. As for promotion, it suffices to apply Lemma 4.2.3 to the premiss and Lemma 4.2.4 to the conclusion to conclude.

Since we have already discussed contraction and weakening for non-deterministic and universal automata, we readily get the corresponding rules for the exponential modalities. The last thing to check is that the exponentials are functorial and monoidal, that is

- that $\mathcal{A} \Vdash \mathcal{B}$ implies $!\mathcal{A} \Vdash !\mathcal{B}$ and $?\mathcal{A} \Vdash ?\mathcal{B}$; this is done by using Lemma 4.2.4 and 4.2.3.
- that we have $!(\mathcal{A} \otimes \mathcal{B}) \Vdash !\mathcal{A} \otimes !\mathcal{B}$ and $?\mathcal{A} \parr ?\mathcal{B} \Vdash ?(\mathcal{A} \parr \mathcal{B})$, which is also done by exploiting Lemma 4.2.4 and the basic properties of $!, ?, \otimes$ and $\parr$ on recognized languages.

Remark. *In [61], an interpretation of ! as an dealternation operator turning general alternating (tree) automata into non-deterministic automata is investigated, and a corresponding promotion rule is given. This could very well be adapted to our setting to get more general ! and ?, but we*

refrain from doing so for a couple of reasons, which mostly boil down to keeping things simple. First, computing the realizer associated with the promotion rule becomes highly non-trivial as this relies on McNaughton's theorem and determinacy of parity games for the underlying automata. This is in contrast with the interpretation of proofs given elsewhere in this thesis, which are invariant with respect to the precise interpretation of formulas as automata. Second, we shall prove much later a completeness result for the underlying model of LSFOM *that does not readily extend to the setting with full exponentials. Lastly, this* ! *is not functorial, meaning that the interpretation of proofs is not invariant under cut-elimination. In particular, it means that the fragment consisting of* $\forall$, $\exists$, $\otimes$, $\multimap$ *and* ! *does not constitute a model of first-order intuitionistic exponential multiplicative linear logic as commonly understood. However it should be stressed that this last problem is more secondary, as we are not be interested in the dynamics of cut-elimination.*

Substitution and quantifications As previously, the logical characterization of quantification first calls for a formal definition of substitution at the level of uniform automata.

Definition 4.2.14. *Given a uniform Muller automaton* $\mathcal{A} = (Q_{\mathcal{A}}, q^{\iota}_{\mathcal{A}}, U, X, \delta_{\mathcal{A}}, [\mathcal{F}]_{\infty}) : B$ *and a Mealy machine* $\mathcal{M} = (Q_{\mathcal{M}}, q^{\iota}_{\mathcal{M}}, \delta_{\mathcal{M}}) : A^{\omega} \to B^{\omega}$*, define the substituted automaton* $\mathcal{M}^*\mathcal{A} = (Q_{\mathcal{A}} \times Q_{\mathcal{M}}, (q^{\iota}_{\mathcal{A}}, q^{\iota}_{\mathcal{M}}), U, X, \delta_{\mathcal{M}^*\mathcal{A}}, [\mathcal{F}_{\mathcal{M}^*\mathcal{A}}]_{\infty})$ *with*

$$\begin{array}{lcl} \pi_2(\delta_{\mathcal{M}^*\mathcal{A}}(a,(q,r)),u,x) & = & \pi_2(\delta_{\mathcal{M}}(a,r)) \\ \pi_1(\delta_{\mathcal{M}^*\mathcal{A}}(a,(q,r)),u,x) & = & \delta_{\mathcal{A}}(\pi_1(\delta_{\mathcal{M}}(a,r)),q,u,x) \\ X \in \mathcal{F}_{\mathcal{M}^*\mathcal{A}} & \Leftrightarrow & \pi_1(X) = \{q \mid (q,r) \in X\} \in \mathcal{F} \end{array}$$

As in Section 3.2, we allow ourselves to write $f^*\mathcal{A}$ for a f.s. causal function f rather than a given Mealy machine in the sequel. The language recognized by the substituted automaton still corresponds formally to the following.

Lemma 4.2.15. *For every uniform Muller automaton* $\mathcal{A} : B$ *and f.s. causal function* $f : A^{\omega} \to B^{\omega}$*, we have*

$$\mathcal{L}(f^*\mathcal{A}) = \{x \in A^{\omega} \mid f(x) \in \mathcal{L}(\mathcal{A})\}$$

Now we are ready to discuss the (co-)projection automata. They will correspond to the expected usual constructions on non-deterministic and universal automata and have the usual behaviour for recognized languages. However, we shall give for both a single general construction for alternating uniform automata, which is going to be unsound for language inclusion in the most general case, *but still sound for the deduction rules of* LSFOM.

Definition 4.2.16. *Given a uniform automaton* $\mathcal{A} = (Q_{\mathcal{A}}, q^{\iota}_{\mathcal{A}}, U, X, \delta_{\mathcal{A}}, \Omega_{\mathcal{A}}) : A \times B$*, define the automaton* $\exists_{\pi_2}\mathcal{A} := (Q_{\mathcal{A}}, q^{\iota}_{c}A, U \times A, X, \delta_{\exists_{\pi_2}\mathcal{A}}, \Omega_{\mathcal{A}}) : B$ *with*

$$\delta_{\exists_{\pi_2}\mathcal{A}}(b,q,(u,a),x) = \delta_{\mathcal{A}}((a,b),q,u,x)$$

Dually, define the automaton $\forall_{\pi_2}\mathcal{A} := (Q_{\mathcal{A}}, q^{\iota}_{c}A, U^A, X \times A, \delta_{\forall_{\pi_2}\mathcal{A}}, \Omega_{\mathcal{A}}) : A$ *with*

$$\delta_{\forall_{\pi_2}\mathcal{A}}(b,q,f,(x,a)) = \delta_{\mathcal{A}}((a,b),q,f(a),x)$$

The basic rationale behind the definition is that control of the piece of the parameter alphabet that we wish to quantify over is given to one of the two players. The definition for $\forall$ is slightly more involved because we would ideally wish that the parameter, even if control over it is given to P or O, to be played first in a round. As it is not possible, we allow the move of P to depend on it by making P play a function $f \in U^A$ instead of its usual move $u \in U$.

Before giving some intuition as to how the deduction rules for $\exists$ are interpreted in the general case, let us make note when the (co)-projection are sound with respect to language recognition.

Lemma 4.2.17. *If* $\mathcal{A} : A \times B$ *is a non-deterministic automaton, then we have*

$$\mathcal{L}(\exists_{\pi_2}\mathcal{A}) = \{w \in B^{\omega} \mid \exists u \in A^{\omega}.\langle u, w\rangle \in \mathcal{L}(\mathcal{A})\}$$

Similarly, if $\mathcal{A} : A \times B$ *is a universal automaton, then we have*

$$\mathcal{L}(\forall_{\pi_2}\mathcal{A}) = \{w \in B^{\omega} \mid \forall u \in A^{\omega}.\langle u, w\rangle \in \mathcal{L}(\mathcal{A})\}$$

Now, the soundness of the logical rules of $\exists$ is implied by the following Lemma.

Lemma 4.2.18. *Let* $\mathcal{A} : A \times B$ *and* $\mathcal{B} : B$ *be uniform automata. We have*

- *for any f.s. causal function $f : B^\omega \to A^\omega$, a canonical realizer $\langle f, \mathrm{id}\rangle^* \mathcal{A} \Vdash \exists_{\pi_2} \mathcal{A}$*

- *a way of turning a realize $\exists_{\pi_2} \mathcal{A} \Vdash \mathcal{B}$ into a realizer $\mathcal{A} \Vdash \pi_2^* \mathcal{B}$.*

Let us recall that the intuition is that the first clause simulates the introduction of existential quantification, with f serving as witness which may depend on the parameter of sort B^ω; if $\mathcal{A}$ is the interpretation of the formula $\varphi(a, b)$, the first realizer corresponds to a proof $\varphi(f(b), b) \vdash \exists a^{A^\omega}.\varphi(a, b)$. As for the second clause, it simulates the deduction rule corresponding to the elimination of an existential: $\exists a^{A^\omega} \varphi(a, b) \vdash \psi(b)$ if and only if $\varphi(a, b) \vdash \psi(b)$ (for a not occurring in ψ).

Proof sketch. The canonical winning P-strategy corresponding to the first item may be pictured as follows

	$(U\ ,\ X) \longrightarrow (U \times A\ \ ,\ X)\ :\ B$				
			$\vdots$		
O	u_n				b_n
P			$(u_n, f(b)_n)$		
O				x_n	
P		x_n			
			$\vdots$		

Note that $f(b)_n$ is computable from $(b_i)_{i \leq n}$ which has already been seen when P makes their first move at round n.

The second item is very straightforward when putting side by side the boards of both simulation games; both games are seen to be the same, up to a relabelling of moves.

	$(U \times A\ \ ,\ X) \longrightarrow (V,\ Y)\ :\ B$				
			$\vdots$		
O	(u_n, a_n)				b_n
P			v_n		
O				y_n	
P		x_n			
			$\vdots$		

	$(U\ ,\ X) \longrightarrow (V,\ Y)\ :\ A \times B$				
			$\vdots$		
O	u_n				(a_n, b_n)
P			v_n		
O				y_n	
P		x_n			
			$\vdots$		

□

4.3 Soundness and completeness

At this juncture, we have an interpretation function $[\![-]\!]$ from LSFOM formulas with free variables $x_1^{A_1^\omega}, \ldots, x_k^{A_k^\omega}$ to uniform alternating automata over $A_1 \times \cdots \times A_k$ defined inductively in the obvious way. The previous section also establishes the following invariant on the interpretation.

Lemma 4.3.1. *If the formula φ is*

- *positive, then the automaton $[\![\varphi]\!]$ is non-deterministic.*

- *negative, then the automaton $[\![\varphi]\!]$ is universal.*

- *deterministic, then the automaton $[\![\varphi]\!]$ is deterministic.*

This, together with Lemma 4.2.4, allow to derive a preliminary soundness lemma for negative formulas which is useful to show that all the axioms of LSFOM are valid in the model.

Definition 4.3.2. *Define a map $\lfloor - \rfloor$ taking* LSFOM *formulas to* FOM *formulas by recursion as follows*

$$\begin{array}{rcl@{\qquad}rcl}
\lfloor \bot \rfloor & := & \bot & \lfloor \mathbf{I} \rfloor & := & \top \\
\lfloor \mathtt{t} = \mathtt{u} \rfloor & := & \mathtt{t} = \mathtt{u} & \lfloor \varphi \otimes \psi \rfloor & := & \lfloor \varphi \rfloor \wedge \lfloor \psi \rfloor \\
\lfloor \varphi \parr \psi \rfloor & := & \lfloor \varphi \rfloor \vee \lfloor \psi \rfloor & \lfloor \varphi \multimap \psi \rfloor & := & \lfloor \varphi \rfloor \Rightarrow \lfloor \psi \rfloor \\
\lfloor \exists a^A \varphi \rfloor & := & \exists a^A \lfloor \varphi \rfloor & \lfloor \forall a^A \varphi \rfloor & := & \forall a^A \lfloor \varphi \rfloor \\
\lfloor !\varphi \rfloor & := & \lfloor \varphi \rfloor & \lfloor ?\varphi \rfloor & := & \lfloor \varphi \rfloor
\end{array}$$

Note in particular that we have $\lfloor \varphi^L \rfloor = \varphi$.

Lemma 4.3.3. *If φ is a negative formula, then $\mathbf{I} \Vdash [\![\varphi]\!]$ if and only if $\mathsf{FOM} \vdash \lfloor\varphi\rfloor$.*

This preliminary lemma is especially useful to show that all of the FOM axioms of Figure 4.3 are trivially realized in the model. Combining this observation with the various finite-state strategy combinators that we have only sketched in the last section allows to derive the following soundness theorem.

Theorem 4.3.4. *If the sequent $\overline{\varphi} \vdash \overline{\varphi'}$ is derivable in LSFOM, then we have $\bigotimes \overline{[\![\varphi]\!]} \Vdash \parr\!\!\!\bigcirc \overline{[\![\varphi']\!]}$.*

From this general soundness theorem, we derive, as with SFOM, soundness with respect to Church's synthesis.

Corollary 4.3.5. *If $\varphi(x^{A^\omega}, y^{B^\omega})$ is a FOM formula and LSFOM derives $\forall x^{A^\omega}.\exists y^{B^\omega}.\varphi^L(x,y)$, then one can extract from the formal proof a f.s. causal function $f : A^\omega \to B^\omega$ such that $\mathsf{FOM} \vdash \forall x^{A^\omega}.\varphi(x, f(x))$.*

Proof. Apply Theorem 4.3.4 to the derivation $\vdash \forall x^{A^\omega}.\exists y^{B^\omega}.\varphi^L(x,y)$ to get a winning strategy in the simulation game from $\mathbf{I}$ to $[\![\forall x^{A^\omega}.\exists y^{B^\omega}.\varphi^L(x,y)]\!]$. Keeping in mind that φ^L is deterministic, up to isomorphism of alphabets, the winning strategy is exactly a causal map $f : A^\omega \to B^\omega$ such that $\varphi^L(x, f(x))$ is trivially realized. By the previous remarks, it means that $\mathsf{FOM} \vdash \lfloor\varphi^L(x, f(x))\rfloor = \varphi(x, f(x))$. □

The converse statement is derivable without referring to the automata-theoretic interpretation of LSFOM.

Lemma 4.3.6. *If there is f.s. causal function such that $\mathsf{FOM} \vdash \forall x^{A^\omega}.\varphi(x, f(x))$, then $\mathsf{LSFOM} \vdash \forall x^{A^\omega}\exists y^{B^\omega}\varphi^L(x,y)$.*

Proof. Clearly, FOM proves the open sequent $\vdash \varphi(x, f(x))$, so by Lemma 4.1.6, LSFOM proves $\vdash \varphi^L(x, f(x))$. The result then follow by applying a right $\exists$ rule and a right $\forall$ rule. □

Towards a complete axiomatization While the realizability model of LSFOM does not admit classical reasoning, it is still effectively two-valued because of the determinacy of simulation games.

Lemma 4.3.7. *For every closed formula φ of LSFOM, we have either $\Vdash [\![\varphi]\!]$ or $\Vdash [\![\varphi]\!] \multimap \bot$. Furthermore, there is an algorithm taking φ as input deciding which one is true.*

Proof. Apply determinacy for the trivial simulation game from $\mathbf{I}$ to φ (Lemma 4.2.2). If P wins, then the first alternative holds. Otherwise, there is necessarily a winning O-strategy in the simulation game from $\mathbf{I}$ to $\varphi \multimap \bot$. Were it not the case, there would be another winning P-strategy; combine it with the first and the simulation

$$(\mathcal{A} \multimap \bot) \otimes \mathcal{A} \Vdash \bot$$

and we would be able to extract a winning P-strategy in the $\bot$ automaton, which is impossible. □

Therefore, it is natural to ask if there is a nice axiomatization extending LSFOM covering the whole model. Since the two-valuedness is effective thanks to the Büchi-Landweber theorem, there is necessarily a recursive axiomatization, but this on its own does not tell us much. We shall give such an axiomatization in Chapter 7 inspired by Dialectica.

Chapter 5

Dialectica fibrations

This chapter is devoted to presenting the Dialectica transformation. Historically, this is a logical translation devised by Gödel to eliminate quantification in higher-typed arithmetic. The basic idea is that, in this interpretation, a formula $\varphi(z^\kappa)$ is mapped to formula $\varphi_D(u^\tau, x^\sigma; z^\kappa)$ representing the winning condition of a two-moves two-player game. In such a game, ∃loïse would be asked to provide a witness u^τ of the validity of the formula and ∀bélard answers with a counter-witness x^κ.

As hinted in previous chapters, our approach to Church's synthesis interprets formulas as infinite two-player games and proofs as strategies. Connectives correspond to operation on games, which have a very uniform structure. This structure is highly reminiscent of the Dialectica interpretation we shall explore in this chapter. In order to keep a reasonable level of generality, we formalize our interpretation in terms of categorical logic. One advantage of categorical logic is that the accompanying notion of "model" is relaxed to the point that theories and models have essentially the same status. Another is that it axiomatizes cleanly the structure necessary to have a soundness theorem for proof systems for the fragment of linear logic presented in the previous chapter, *full intuitionistic linear logic* augmented with first-order quantifiers. Usually, this axiomatization also ensures that the interpretation of proofs preserves *cut-elimination*. However, this will be true here only as far as first-order intuitionistic multiplicative linear logic is concerned. Indeed, the computational interpretation of full intuitionistic linear logic is a more difficult and less standard topic, therefore, we shall only ask enough additional structure to interpret proof trees without concerning ourselves with cut-elimination for full intuitionistic linear logic.

The exposition of this chapter is highly inspired from Hofstra's [31], which itself follows from a series of work (see e.g. [6]) on the categorical aspects of the Dialectica transformation as initiated in de Paiva's thesis [21]. However, we are not aware of any single source covering both the interpretation of quantifiers, (linear) propositional connectives, our unusual exponentials in a self-contained fashion and the characterization theorem.

5.1 Categorical models of propositional linear logic

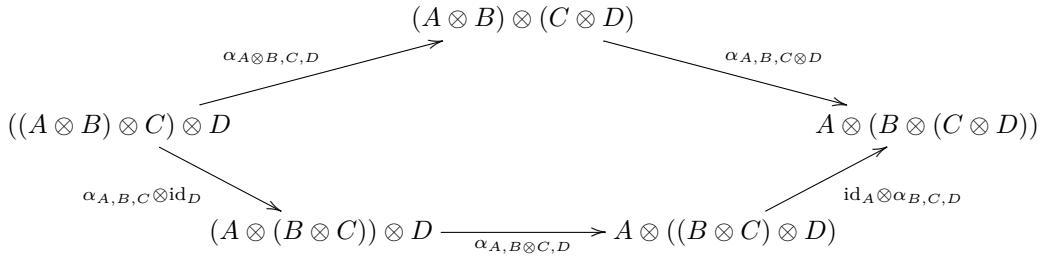
The basic idea is that a model is a category whose objects represent formulas and morphisms proofs. Since the Dialectica interpretation is very much tied to the notion of quantification, we shall later on generalize these notions to a fibered setting. Fibrations at first glance require an overhead, which might make such a generalization seem somewhat perilous. However, this can be dealt with in a fairly straightforward manner if one remembers that both $\mathfrak{Cat}$ and $\mathfrak{Fib}$ are 2-categories. While we think it more intuitive to first expose the situation in $\mathfrak{Cat}$, we shall remark on the 2-categorical nature of the structures involved.

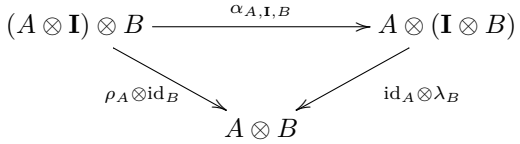
The material here is based on [49] which review categorical models of linear logic. However, we target full intuitionistic linear logic with exponentials, a mild extension of [34], so our notion of model does not appear per se in [49]. We accomodate the definition by allowing an additional monoidal structure for $⅋$, together with a suitable natural transformation $A⊗(B⅋C) \to (A⊗B)⅋C$ satisfying obvious coherence conditions (see e.g. [18]) and exponentials.

Definition 5.1.1. *A* monoidal category *is a category* $\mathbb{C}$ *together with a*

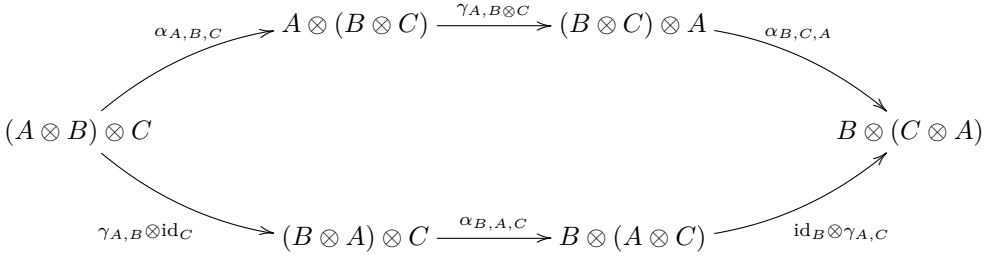
- *a bifunctor* $- ⊗ - : \mathbb{C}^2 \to \mathbb{C}$
- *a distinguished object* $\mathbf{I}$

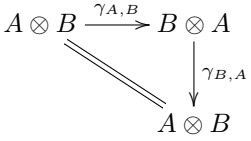
- *natural isomorphisms* $\rho_A : A \times \mathbf{I} \to A$, $\lambda_A : \mathbf{I} \times A \to A$ *and* $\alpha_{A,B,C} : (A \otimes B) \otimes C \to A \otimes (B \otimes C)$ *subject to the following coherence conditions:*





A symmetric *monoidal category* $(\mathbb{C}, \otimes, \mathbf{I})$ *moreover comes equipped with natural isomorphisms* $\gamma_{A,B} : A \otimes B \to B \otimes A$ *subject to the following coherences:*





Example 5.1.2. *If* $\mathbb{C}$ *has chosen cartesian products* $\times$ *and a terminal object* 1*, then* $(\mathbb{C}, \times, 1)$ *is a symmetric monoidal category.*

Definition 5.1.3. *A monoidal category* $\mathbb{C}$ *is called* closed *if every functor* $- \otimes A : \mathbb{C} \to \mathbb{C}$ *has a right adjoint* $A \multimap - : \mathbb{C} \to \mathbb{C}$*. In such a case, we have a natural isomorphism*

$$[A \otimes B, C]_{\mathbb{C}} \qquad \cong \qquad [A, B \multimap C]_{\mathbb{C}}$$

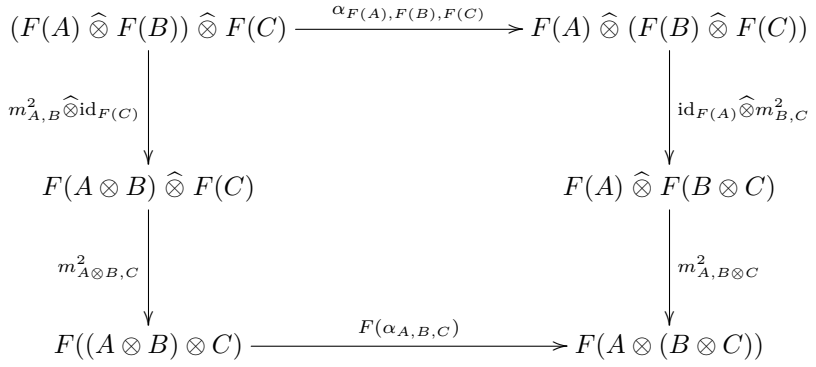
Monoidal closed categories are models of intuitionistic multiplicative linear logic IMLL. In order to translate intuitionistic logic, we require in addition an exponential modality !. At the categorical level, ! is interpreted as a comonad satisfying additional properties.

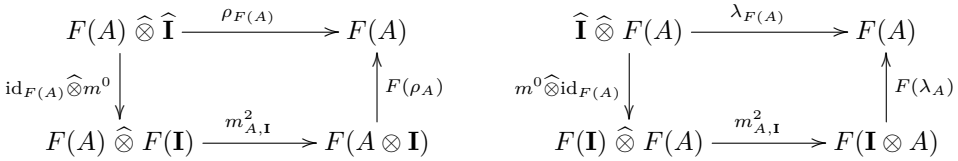
Keeping in mind that any monad over a category $\mathbb{C}$ may be decomposed as an adjunction between a coKleisli coKlei($\mathbb{C}$) and $\mathbb{C}$, it was noticed in (e.g. [5]) that the exponential modality could be conveniently axiomatized as a lax monoidal adjunction between a monoidal closed category and a cartesian category. Let us make this notion precise.

Definition 5.1.4. *Let* $(\mathbb{C}, \otimes, \mathbf{I})$ *and* $(\mathbb{D}, \widehat{\otimes}, \widehat{\mathbf{I}})$ *be two monoidal categories. A* lax monoidal functor *is given by a functor* $F : \mathbb{C} \to \mathbb{D}$*, together with natural transformations*

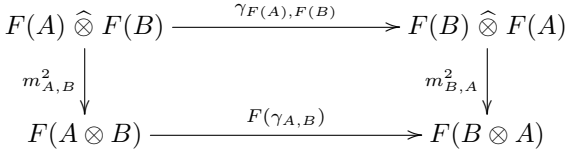
$$m^0 : \widehat{\mathbf{I}} \to F(\mathbf{I}) \qquad\qquad m^2_{A,B} : F(A) \mathbin{\widehat{\otimes}} F(B) \to F(A \otimes B)$$

making the following diagrams commute.





Assuming $(\mathcal{C}, \otimes, \mathbf{I})$ *and* $(\mathcal{D}, \widehat{\otimes}, \widehat{\mathbf{I}})$ *are actually symmetric monoidal categories, a* symmetric lax monoidal functor *between them satisfy a further coherence diagram.*



An oplax monoidal functor *is a functor* $F : \mathbb{C} \to \mathbb{D}$ *equiped with natural transformations*

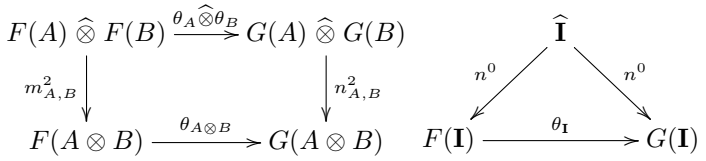
$$n^0 : F(\mathbf{I}) \to \widehat{\mathbf{I}} \qquad\qquad n^2_{A,B} : F(A \otimes B) \to F(A) \mathbin{\widehat{\otimes}} F(B)$$

satisfying similar coherence conditions as above.

A monoidal natural transformation *between lax monoidal functors* $(F, m^0, m^2), (G, n^0, n^2) : \mathbb{C} \to \mathbb{D}$ *is a natural transformation*

$$\theta_A : F(A) \longrightarrow G(A)$$

additionally making the two diagrams



Definition 5.1.5. *An adjunction* $L \dashv R$ *between two symmetric monoidal catgories is called monoidal if both* L *and* R *are symmetric lax monoidal and the unit and counit are monoidal natural transformations. Similarly,* $L \dashv R$ *is called symmetric oplax monoidal if both* L *and* R *are symmetric oplax monoidal and the unit and counit are monoidal natural transformations.*

Definition 5.1.6. *A* Linear-Non-Linear adjunction *(henceforth abbreviated as LNL-adjunction) is given by a monoidal adjunction* $L \dashv R$ *where* $L : \mathbb{C} \to \mathbb{L}$ *whose the monoidal structure on* $\mathbb{C}$ *is given by a choice of cartesian products and a terminal object.*

The intuition behind LNL-adjunction is that the cartesian category $(\mathbb{C}, \times, 1)$ corresponds to the category of duplicable hypotheses. The associated exponential operator ! is obtained as the composition $L \circ R$, which readily yields a comonad structure for ! by the usual properties of adjunctions. Dereliction $\mathbf{der}_A : !A \to A$ is given by the counit $L(R(A)) \to A$ while the comultiplication $\mathbf{dig}_A : !A \to !!A$ is built by precomposing and postcomposing the unit $X \to R(L(X))$ with R and L respectively. The monoidal structure allows to interpret weakening $!A \to \mathbf{I}$ and contraction $!A \to !A \otimes !A$ using the fact that L is actually *strong monoidal.* Asking for an adjunction with left adjoint strong monoidal is in fact enough to recover all of the data of a monoidal adjunction.

Lemma 5.1.7 ([49] Proposition 13)**.** *Let $L \dashv R$ be an adjunction between two monoidal categories, with L lax monoidal. The adjunction lifts to a monoidal adjunction if and only if L is actually strong monoidal.*

We shall often use this characterization in the sequel to exhibit monoidal adjunctions, as well as the obvious dualization: an adjunction $L \dashv R$ with R strong monoidal gives rise to an oplax monoidal adjunction.

Definition 5.1.8. *A categorical model of* IMELL *consists of a symmetric monoidal closed category $(\mathbb{L}, \otimes, \mathbf{I})$ and a LNL-adjunction $I^+ \dashv R^+$ between some cartesian category $(\mathbb{C}, \times, 1)$ and $(\mathbb{L}, \otimes, \mathbf{I})$. We write $!$ for the induced comonad over $\mathbb{L}$.*

This notion of model for intuitionistic multiplicative linear logic is rather well-understood and ensures that proofs equal up to cut-elimination and commuting conversions are necessarily equated.

We are interested in extending those models in order to interpret an extension of full intuitionistic linear logic from [34]. This logic arises naturally from the study of Dialectica categories, but require a more sophisticated analysis if one wants to interpret cut-elimination. Since we are moreover interested in strict extensions, we shall not concern ourselves too much with equating the interpretation of proofs up to cut-elimination and commuting conversions in the sequel.

In order to model full intuitionistic linear logic, we mainly require an additional family of morphism. Unlike [34], we do not require coherence on top of naturality.

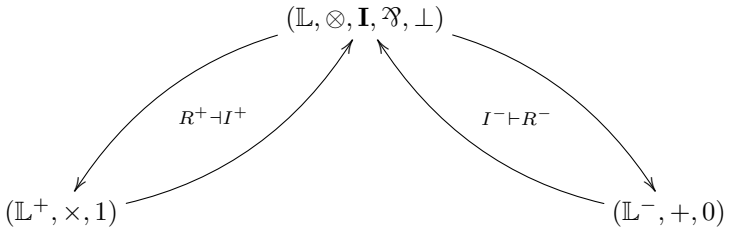
Definition 5.1.9. *A model of full intuitionistic linear logic (*FIMLL*) is given by a monoidal-closed category $(\mathbb{C}, \otimes, \mathbf{I})$, an additional monoidal structure $(⅋, \bot)$ over $\mathbb{C}$ and a natural transformation $\mathbf{dist}_{X,Y,Z} : X \otimes (Y ⅋ Z) \to (X \otimes Y) ⅋ Z$.*

Remark. *Note that any model of* IMLL *yields a trivial model of* FIMLL *by taking $\otimes = ⅋$. The distribution is then obtained using the associator of the underlying monoidal structure.*

We moreover extend full intuitionistic linear logic with exponential modalities ! and ? to get the system FIMELL. As such, we extend the notion of model of IMELL to accomodate those connectives and full intuitionistic logic. Let us stress that, since we are *not* concerned with modeling cut-elimination properly, it would be inappropriate to call those FIMELL-models.

Definition 5.1.10. *A* FIMELL*-category consists of the following data.*

- *A model of* IMELL*, that is, a symmetric monoidal closed category $(\mathbb{L}, \otimes, \mathbf{I})$.*
- *An additional symmetric monoidal structure $(⅋, \bot)$ over $\mathbb{L}$.*
- *A distributivity law $\mathbf{dist}_{A,B,C} : A \otimes (B ⅋ C) \to (A \otimes B) ⅋ C$, so that $\mathbb{L}$ is a model of full intutionistic linear logic.*
- *A cartesian category $\mathbb{L}^+$ of positive objects and a category of negative objects $\mathbb{L}^-$..*
- *A LNL-adjunction $I^+ \dashv R^+$ between $(\mathbb{L}^+, \times, 1)$ and $(\mathbb{L}, \otimes, \mathbf{I})$.*
- *An oplax monoidal adjunction $R^- \dashv I^-$ between $(\mathbb{L}, ⅋, \bot)$ and $(\mathbb{L}^-, +, 0)$.*



- *Writing $! := I^+ \circ R^+$ and $? := R^- \circ I^-$, we additionally require natural transformations.*

$$!A \otimes ?B \quad \longrightarrow \quad ?(!A \otimes B) \qquad\qquad !(A ⅋ ?B) \quad \longrightarrow \quad !A ⅋ ?B$$

Remark. *In the models we are going to be considering later on, $\mathbb{L}$ is going to be a proof-relevant category while $\mathbb{L}^+$ and $\mathbb{L}^-$ will constitue full subcategories of $\mathbb{L}$. Hence, the functors I^+ and I^- should be thought of as "inclusions" and R^+ and R^- as "retractions" in these particular cases. Of course, this is not necessarily true for other* FIMELL*-categories, where other naming conventions may be more appropriate.*

5.2 Fibrations for linear logic

Our purpose here is merely to introduce the necessary background to define and study particular Dialectica fibrations. We refer the interested readers to [36] for an introduction to fibred approach to categorical logic.

Fibrations may be regarded as one of the most generic notion of model for logic. The basic idea is that, a fibration is a particular kind of functor $p : \mathbb{E} \to \mathbb{B}$. The category $\mathbb{B}$, customarily called the *base*, consists of the objects the logic is concerned with, while objects of $\mathbb{E}$, the *total space* consists of predicates. The object component of p maps predicates $\varphi \in \mathbb{E}_0$ to the object $X \in \mathbb{B}$ over which the free variables of φ range over. The morphisms f of the base $\mathbb{B}$ correspond to terms. The condition for p to be a fibration is that every such morphism f admits *cartesian liftings* f^* corresponding to substitution.

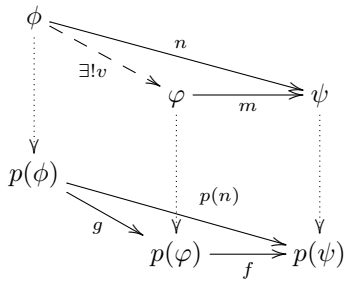
5.2.1 Basic theory and examples

Definition 5.2.1. *Let $p : \mathbb{E} \to \mathbb{B}$ be a functor.*

- *A morphism v in $\mathbb{E}$ is vertical if $p(v) = \mathrm{id}$.*
- *For an object A in $\mathbb{B}$, the* fiber of p over A *is the subcategory of $\mathbb{E}$ consisting of objects φ satisfying $p(\varphi) = A$ and vertical morphisms between them. We write p_A for this category.*

If $p(\varphi) = A$, we say that φ is an object over A. Similarly, if $p(v) = f$, v is said to lie over f.

Definition 5.2.2. *A morphism $m : \varphi \to \psi$ of the category $\mathbb{E}$ over $f : p(\varphi) \to p(\psi)$ is called* p-cartesian *if and only if for every $n : \phi \to \psi$ and factorisation $p(n) = f \circ g$, there exists a unique morphism v over g for which $m \circ v = n$.*



In this case, m is a cartesian lifting of f.

The functor $p : \mathbb{E} \to \mathbb{B}$ is called a fibration over $\mathbb{B}$ *if for every morphism $f : X \to p(\varphi)$ of the category $\mathbb{B}$ has a p-cartesian lifing with codomain φ.*

As hinted previously, from a logical perspective, cartesian maps ought to be thought as term substitution in formulas. On the other hand, vertical morphisms correspond to entailments. Let us enumerate list a couple of properties which are routinely used to manipulate cartesian morphisms.

Lemma 5.2.3. *Let $p : \mathbb{E} \to \mathbb{B}$ be a fibration.*

- *The composite of two cartesian maps remains cartesian.*
- *If two maps m, m' are cartesian over f with the same codomain, then there exists a unique vertical isomorphism v such that $m \circ v = m'$.*
- *Every morphism in $\mathbb{E}$ factors as a vertical map followed by a cartesian map. This factorization is unique up to unique vertical isomorphism.*
- *When two vertical maps v, v' in $\mathbb{E}$ satisfy $m \circ v = m \circ v'$ with m cartesian, then $v = v'$.*
- *A map which is both vertical and cartesian is an isomorphism.*

While the notion of fibration is lightweight as a fibration $p : \mathbb{E} \to \mathbb{B}$ is nothing but a functor satisfying some property, it is sometimes inconvenient to think that substitution by a "term" is defined only up to vertical isomorphism. An arguably more natural point of view would be to consider the notion of indexed category.

Definition 5.2.4. *A* $\mathbb{B}$-indexed category *is a pseudo-functor* $P : \mathbb{B}^{\mathrm{op}} \to \mathfrak{Cat}$. *This means that for all objects* A *of the base, we have a category* $P(A)$*, and for each morphism* $f : A \to B$ *a substitution functor* $P(f) : P(B) \to P(A)$ *together with a family of coherence isomorphisms* $P(f) \circ P(g) \cong P(g \circ f)$ *and* $P(\mathrm{id}) \cong \mathrm{id}$*, themselves subject to further coherence axioms (see Definition 1.1.4 [36]).*

P is called a strict $\mathbb{B}$-indexed category if it is actually a functor $P : \mathbb{B}^{\mathrm{op}} \to \mathfrak{Cat}$.

$\mathbb{B}$-indexed categories give rise to fibrations over $\mathbb{B}$ via the Grothendieck construction.

Construction 5.2.5 (Grothendieck construction)**.** *Let $\int_{\mathbb{B}} P$ be the category of elements of P defined as follows:*

- *An object is a pair (A, φ) where A is an object of $\mathbb{B}$ and φ an object of $P(A)$.*
- *A morphism $(A, \varphi) \to (B, \psi)$ is a pair (f, m) where $f : A \to B$ and $m : \varphi \to P(f)(\psi)$.*

The first projection functor $\int_{\mathbb{B}} P \to \mathbb{B}$ is seen to be a fibration: for any $f : A \to B$ and φ object of $P(B)$, $f^* := (f, \mathrm{id}) : (A, P(f)(\varphi)) \to (B, \varphi)$ is a cartesian lifting of f.

Note that a $\mathbb{B}$-indexed category give rise to a choice of cartesian liftings for the associated fibration $\int_{\mathbb{B}} P \to \mathbb{B}$.

For any fibration $p : \mathbb{E} \to \mathbb{B}$, we call such a choice a *cleavage* of p. Cleavages always exist using the axiom of choice for classes. A fibration equipped with a cleavage is called *cloven*. There is a counterpart to the Grothendieck construction mapping cloven fibrations to pseudo-functors by mapping objects A of $\mathbb{B}$ to $p_{\mathbb{B}}$, making the two notions equivalent. We do not detail this here and refer the interested reader to e.g. [36][Proposition 1.4.5].

Indexed categories give an easy mean to construct a variety of fibrations from suitable contravariant (pseudo-)functors, but can become nevertheless cumbersome when dealing more involved constructions. On the other hand, much of the structural theory of fibrations is rather elegant, but definitions of total categories may get fairly verbose even in simple cases. In the sequel, we shall officially work with cloven fibrations, although it might be useful to keep in mind the basic pseudo-functorial structure to maintain certain intuitions. In particular, a lot of simple semantic cases arise from strict indexed categories; when a fibration $p : \mathbb{E} \to \mathbb{B}$ arise from a strict indexed category (i.e., there exists a cleavage extending to a functor $\mathbb{B}^{\mathrm{op}} \to \mathbb{E}$), then we call it *split*.

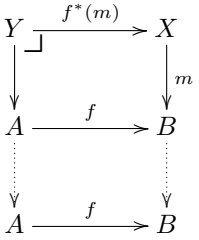
Let us now turn to several basic examples of fibrations.

Example 5.2.6. *Let $\mathcal{T}$ be a multisorted first-order theory with pairing, i.e., a signature for terms and a set of theorems closed by deduction. Build the base $\mathbb{B}[\mathcal{T}]$ by taking types as objects and terms as morphisms. There is a contravariant functor $\mathbb{B}[\mathcal{T}]^{\mathrm{op}} \to$ **Preord** which takes objects τ to the suitable Lindenbaum algebra consisting of formulas $\varphi(x^\tau)$, preoredered by deduction (i.e., there exists a morphism $\varphi(x^\tau) \to \psi(x^\tau)$ if and only if $\mathcal{T} \vdash \varphi(x^\tau) \Rightarrow \psi(x^\tau)$). This is the* syntactic fibration *associated to $\mathcal{T}$.*

Example 5.2.7. *Let $\mathbf{Set}_{\subseteq}$ be the (large) order of sets and inclusion, seen as a category. The powerset $\mathcal{P}$ constitutes a contravariant functor $\mathcal{P} : \mathbf{Set}^{\mathrm{op}} \to \mathbf{Set}_{\subseteq}$. The associated split fibration $\int_{\mathbf{Set}} \mathcal{P}$ corresponds to the "standard" logic of sets (with bounded quantifications).*

Example 5.2.8. *Let* $\mathrm{Sub}(\mathbb{B})$ *be the full subcategory of $\mathbb{B}^{\to}$ where objects are restricted to be monomorphisms. The restriction of the* cod *functor* $\mathrm{Sub}_{\mathbb{B}} : \mathrm{Sub}(\mathbb{B}) \to \mathbb{B}$ *is a fibration whenever $\mathbb{B}$ have all pullbacks along monomorphisms. There is a fibered equivalence between $\int_{\mathbf{Set}} \mathcal{P}$ and* $\mathrm{Sub}_{\mathbf{Set}}$.

Example 5.2.9. *If $\mathbb{B}$ has all pullbacks,* $\mathrm{cod} : \mathbb{B}^{\to} \to \mathbb{B}$ *is a fibration. If $f : A \to B$ is morphism of the base and $m : X \to B$ an object abover B, then a cartesian lift of f with codomain m is obtained by pulling back f along m.*



Example 5.2.10. *Suppose that $\mathbb{B}$ has cartesian products. Build the total space of the* simple fibration $\mathfrak{Simpl}(\mathbb{B})$ *as follows.*

- **Objects:** *pairs of objects (A, X) of $\mathbb{B}$*
- **Morphisms:** *a morphism $(A, X) \to (B, Y)$ is a pair of $\mathbb{B}$-morphism (f, f_0) where $f : A \to B$ and $f_0 : A \times X \to Y$.*
- **Identities:** *the identity on (A, X) is the map (id, π_2).*
- **Composition:** *given $(f, f_0) : (A, X) \to (B, Y)$ and $(g, g_0) : (B, Y) \to (C, Z)$, the composite is defined to be the pair $(g \circ f, g_0 \circ \langle f \circ \pi_1, f_0 \rangle)$.*

This category is fibered over $\mathbb{B}$ via the first projection. A cartesian lifting of $f : A \to B$ with codomain (B, X) is (f, π_2).

In the sequel, while we are going to mostly describe general constructions over fibrations, it will be helpful to keep these basic instances in mind. Let us end this section with a couple of additional way of building fibrations.

Lemma 5.2.11. *If p is a fibration and the diagram below is a pullback square in $\mathfrak{Cat}$, then p' is a fibration.*

$$\begin{array}{ccc} \mathbb{E}' & \longrightarrow & \mathbb{E} \\ {\scriptstyle p'}\downarrow & & \downarrow{\scriptstyle p} \\ \mathbb{B}' & \xrightarrow{F} & \mathbb{B} \end{array}$$

This construction is sometimes referred to as the change of base *of p along the functor F.*

Additionally, if $p : \mathbb{E} \to \mathbb{B}$ and $q : \mathbb{B} \to \mathbb{B}'$ are fibrations, so is $q \circ p$.

Example 5.2.12. *When $\mathbb{B}'$ is a subcategory of $\mathbb{B}$, change of base can be seen as the canonical way of restricting the predicates of $p : \mathbb{E} \to \mathbb{B}$ to those object already in $\mathbb{B}$. Typically, there is an obvious inclusion* Mealy $\to$ **Set** *along which the fibration* $\mathrm{Sub}_{\mathbf{Set}}$ *may be pulled back to obtain the standard model of* FOM*.*

Example 5.2.13. *Consider the dualization functor $(-)^{\mathrm{op}} : \mathfrak{Cat} \to \mathfrak{Cat}$. If $P : \mathbb{B}^{\mathrm{op}} \to \mathfrak{Cat}$ is an indexed category, then so is $(-)^{\mathrm{op}} \circ P : \mathbb{B}^{\mathrm{op}} \to \mathfrak{Cat}$ corresponding to the opposite indexed category. If $p = \int_{\mathbb{B}} P$, we write p^{op} for a fibration equivalent to $\int_{\mathbb{B}} (-)^{\mathrm{op}} \circ P$ and call it the opposite fibration*[1]

Remark. *Dualization will play a major part role in the sequel. Formally speaking, the notion is helpful to make precise the notion of contravariant functors between fibrations, which appears when dealing with monoidal closure and to give an expeditive definition of a certain construction $\mathfrak{Prod}$ in terms of its dual $\mathfrak{Sum}$.*

5.2.2 The category of (cloven) fibrations

In this subsection, we cover basic material regarding the 2-category of fibrations $\mathfrak{Fib}$. While our main goal is rather to construct fibrations out of old ones rather than to carry out a study of $\mathfrak{Fib}$ itself, a modicum of understanding the global structure of $\mathfrak{Fib}$ is useful to model linear logic. In particular, adapting LNL definitions require a clean notion of adjunction between fibrations, which can also be put to work to summarize the data needed for e.g. monoidal closed fibrations.

Definition 5.2.14. *Let $p : \mathbb{E} \to \mathbb{B}$ and $q : \mathbb{F} \to \mathbb{B}$ be two fibrations. A* fibred functor *$F : p \to q$ is a functor $\mathbb{E} \to \mathbb{F}$ such that $q \circ F = p$ and F sends p-cartesian arrows to q-cartesian arrows. Furthermore, if p and q are equipped with cleavages $f \mapsto \hat{f}$, F preserves cleavages if and only if $F(\hat{f}) = \hat{f}$. A natural transformation $\eta : F \to G$ between two functors is* vertical *if all of its components are.*

Cloven fibrations over $\mathbb{B}$, cleavage-preserving fibred functors and vertical natural transformations form a (2-)category $\mathfrak{Fib}(\mathbb{B})$.

[1] This notion is determined only up to equivalence if we do not fix a canonical way of going from indexed categories to fibrations.

Arranging $\mathfrak{Fib}(\mathbb{B})$ into a (large) 2-category allows to easily generalize the propositional approach presented in Section 5.1. Indeed, the notions which require carrying over to the fibered setting could have just as well been formulated for an arbitrary 2-category. Since we mostly manipulate two kinds of 2-categories, $\mathfrak{Cat}$ and $\mathfrak{Fib}(\mathbb{B})$ which are fairly close to one another, we repeat the necessary definitions here.

Lemma 5.2.15. *The product of two fibrations $p : \mathbb{E} \to \mathbb{B}$ and $q : \mathbb{F} \to \mathbb{B}$ is obtained by computing the following pullback in $\mathfrak{Cat}$.*

$$\begin{array}{ccc} \mathbb{E} \times_{\mathbb{B}} \mathbb{F} & \longrightarrow & \mathbb{F} \\ \downarrow & & \downarrow{\scriptstyle q} \\ \mathbb{E} & \xrightarrow[p]{} & \mathbb{B} \end{array}$$

The terminal fibration over $\mathbb{B}$ is the identity functor $\mathrm{id} : \mathbb{B} \to \mathbb{B}$.

Definition 5.2.16. *Let $p : \mathbb{E} \to \mathbb{B}$ and $q : \mathbb{F} \to \mathbb{B}$ be fibrations and $F : p \to q$ and $G : q \to p$ be fibered functors. We say that F is a fibered left ajoint to G if there are* vertical *natural transformations $\eta_X : X \to G(F(X))$ (the* unit*) and $\epsilon_A : F(G(A)) \to A$ (the* counit*) satisfying the usual triangular identities $G(\epsilon_A) \circ \eta_{G(A)} = \mathrm{id}_{G(A)}$ and $\epsilon_{F(X)} \circ F(\eta_X) = \mathrm{id}_{F(X)}$.*

$$\begin{array}{ccccc} & & G(F(G(A)) & & \\ & {\scriptstyle \eta_{G(A)}} \nearrow & & \searrow {\scriptstyle G(\epsilon_A)} & \\ G(A) & & = & & G(A) \end{array} \qquad \begin{array}{ccccc} & & G(F(G(A)) & & \\ & {\scriptstyle G(\epsilon_A)} \nearrow & & \searrow {\scriptstyle \eta_{G(A)}} & \\ F(X) & & = & & G(A) \end{array}$$

A fibered adjunction *between p and q consists of the data (F, G, η, ϵ). We write $F \dashv G$ for fibered adjunctions[2], oftentimes leaving the unit and counit implicit.*

In the sequel, we heavily use adjunctions to build models for the exponential modalities and quantifiers. So let us stress a couple of elementary properties of adjunctions.

Lemma 5.2.17. *Fibered adjunctions in $\mathfrak{Fib}(\mathbb{B})$ may be arranged in a category[3] $\mathfrak{Adj}(\mathfrak{Fib}(\mathbb{B}))$.*

- **Objects:** *fibrations (i.e., same objects as $\mathfrak{Fib}(\mathbb{B})$).*
- **Morphisms:** *a morphism from p to q is a fibered adjunction $L \dashv R$, with $L : p \to q$.*
- **Composition:** *given (L, R, η, ϵ) and $(L', R', \eta', \epsilon')$ with $L : p \to p'$ and $L' : p' \to p''$, we have a composite adjunction $(L' \circ L, R \circ R', (R(\eta'_{L(X)}) \circ \eta_X)_X, (\epsilon'_A \circ L'(\epsilon_{R'(A)}))_A)$.*

Furthermore, a functor $\mathfrak{F} : \mathfrak{Fib}(\mathbb{B}) \to \mathfrak{Fib}(\mathbb{B})$ restricts to a functor $\mathfrak{Adj}(\mathfrak{Fib}(\mathbb{B})) \to \mathfrak{Adj}(\mathfrak{Fib}(\mathbb{B}))$ (since any 2-functor preserves adjunctions).

In $\mathfrak{Cat}$, adjunctions are often more concisely described in terms of hom-sets. For functors L, R, we have $L \dashv R$ whenever there exists a natural isomorphism $[L(A), X] \cong [A, R(X)]$, from suitable unit and counit may be deduced. This is often the preferred way to describe adjunctions in practice, however, it relies on the specifics of $\mathfrak{Cat}$. The following Lemma allows to fall back on this description in a fiberwise manner, provided that we prove additional coherence conditions known as the *Beck-Chevalley* conditions.

Lemma 5.2.18 ([36], Lemma 1.8.9)**.** *Let $p : \mathbb{E} \to \mathbb{B}$ and $q : \mathbb{F} \to \mathbb{B}$ be fibrations and $F : p \to q$ be a fibered functor. F has a left (resp. right) adjoint if and only if.*

- *For each object A of $\mathbb{B}$, the restriction $F_A : p_A \to q_A$ has a left (resp. right) adjoint $K(A)$*
- *The* Beck-Chevalley *condition holds, i.e., for all maps $u : A \to B$ and functors induced by a choice of cartesian lifts $u^* : p_B \to p_A$ and $u^\# : q_B \to q_A$ in p and q respectively, the natural transformation $K(A) \circ u^\#(\varphi) \to u^* \circ K(B)(\varphi)$ (resp. $u^* \circ K(B) \to K(A) \circ u^\#$) is an isomorphism obtained by taking the identity through the following transformations:*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{K(B)(\varphi) \to K(B)(\varphi)}{\varphi \to F_B \circ K(B)(\varphi)}}{u^\#(\varphi) \to u^\# \circ F_A \circ K(B)(\varphi)}}{u^\#(\varphi) \to F_A \circ u^* \circ K(B)(\varphi)}}{K(A) \circ u^\#(\varphi) \to u^* \circ K(B)(\varphi)}$$

[2] In what follows, we shall never encounter an adjunction between fibered functors which is not fibered itself.
[3] Let us ignore higher-dimensional generalizations.

Oftentimes, we will exhibit fibered adjunctions using Lemma 5.2.18 by showing there exists fiberwise adjoints, usually by giving only of the two adjoint and

Finally, we sometimes use the suitable notion of *equivalence of fibrations*.

Definition 5.2.19. An equivalence of fibrations *from* $p : \mathbb{E} \to \mathbb{B}$ *to* $q : \mathbb{F} \to \mathbb{B}$ *consists of a pair of fibered functors* $F : p \to q$ *and* $G : q \to p$ *with vertical natural isomorphisms* $G(F(X)) \xrightarrow{\sim} X$ *and* $F(G(A)) \xrightarrow{\sim} A$

5.2.3 Logical aspect of fibrations

We now give the structure necessary to interpret FOFIMELL in a fibration. For the propositional part, this consists essentially in lifting the notions in the last section in order for categorical models of linear logic to the 2-category $\mathfrak{Fib}(\mathbb{B})$. As all the notions used in defining the notion of models of linear logic make sense in all 2-categories[4], this straightforward. Let us give some details for the definition of monoidal-closed fibrations.

Definition 5.2.20 (See also [64, Def. 2.1] and [50, Sec 3.1])**.** *Let* $p : \mathbb{E} \to \mathbb{B}$ *be a fibration. A monoidal structure over* p *is given by fibred functors* $\mathbf{I} : 1 \to p$ *and* $- \otimes - : p \times p \to p$*, as well as vertical natural transformations* $\rho : A \otimes \mathbf{I} \to A$*,* $\lambda_A : \mathbf{I} \otimes A \to A$ *and* $\alpha : (A \otimes B) \otimes C \to A \otimes (B \otimes C)$ *satisfying the making the usual diagrams (see Definition 5.1.1) commute.*

This endows each fiber p_A *with a monoidal structure preserved by substitution. The fibration* p *is called* monoidal closed *if each fiber is monoidal closed and the monoidal closed structure is preserved by substitution.*

If $\otimes$ *coincides with the cartesian product* $\times$ *in every fiber, then we say that* p *has (chosen) fibered cartesian products. If each fiber is cartesian closed, we shall say that* p *is cartesian closed.*

In concrete terms, for a fibration $p : \mathbb{E} \to \mathbb{B}$, it means that each fibre p_A comes equipped with a symmetric monoidal structure $(\otimes, 1)$ and that this structure is preserved by substitution. We do not explicitate the lifting of similar notions (such as "lax monoidal fibred functor") for the exponentials of linear logic as they are straightforward.

New notions that justify the fibered settings are the interpretation of first-order quantification and equalities.

Definition 5.2.21. *Assume* $\mathbb{B}$ *to be cartesian. The fibration* $p : \mathbb{E} \to \mathbb{B}$ *is said to have simple sums (resp. products) if, for every projection* $\pi : A \times B \to A$*, the functor* $\pi^* : p_A \to p_{A \times B}$ *has a left (resp. right) adjoint written* $\exists_\pi$ *(resp.* $\forall_\pi$*) fulfilling the following Beck-Chevalley condition: for any pullback square whose horizontal arrows are projections*

$$\begin{array}{ccc} A \times B & \xrightarrow{\pi_2} & B \\ {\scriptstyle \mathrm{id}_A \times f}\downarrow & & \downarrow{\scriptstyle f} \\ A \times C & \xrightarrow[\pi_2]{} & C \end{array}$$

the canonical natural transformation

$$\begin{array}{ccc} p_{A \times B} & \xrightarrow{\exists_{\pi_2}} & p_B \\ {\scriptstyle (\mathrm{id}_A \times f)^*}\uparrow & \Rightarrow & \uparrow{\scriptstyle f^*} \\ p_{A \times C} & \xrightarrow[\exists_{\pi_2}]{} & p_C \end{array}$$

is an isomorphism.

The Beck-Chevalley condition of Definition 5.2.21 is an instance of the condition in Lemma 5.2.18. This becomes clearer how by reformulating the property of having finite sums as the existence of a suitable adjoint to the fibered functor $\mathfrak{Sum}$ defined in the next section (Lemma 5.3.8).

[4]Depending on the presentation, some care may be needed when axiomatizing the exponentials. An often used alternative to LNL-adjunctions is to axiomatize the comonad !; then, the LNL-adjunction is recovered by considering the Kleisli category associated to !. This migh be troublesome because Kleisli objects do not need to exist for arbitrary 2-categories. Thankfully, they do for $\mathfrak{Fib}(\mathbb{B})$.

Definition 5.2.22. *The fibration p is said to have equalities if, for every morphism $\delta := \langle \mathrm{id}_A, \mathrm{id}_A \rangle : A \to A \times A$, the functor $(\delta \times \mathrm{id})^* : p_{A \times B} \to p_{(A \times A) \times B}$ has a left adjoint $\exists_{\delta \times \mathrm{id}}$ satisfying the Beck-Chevalley condition: for any pullback square*

$$\begin{array}{ccc} A \times B & \xrightarrow{\delta \times \mathrm{id}_A} & (A \times A) \times B \\ {\scriptstyle \mathrm{id}_A \times f}\downarrow & & \downarrow{\scriptstyle f} \\ A \times C & \xrightarrow[\delta \times \mathrm{id}_A]{} & (A \times A) \times C \end{array}$$

the canonical natural transformation

$$\begin{array}{ccc} p_{A \times B} & \xrightarrow{\exists_{\pi_2}} & p_{(A \times A) \times B} \\ {\scriptstyle (\mathrm{id}_A \times f)^*}\uparrow & \Rightarrow & \uparrow{\scriptstyle f^*} \\ p_{A \times C} & \xrightarrow[\exists_{\pi_2}]{} & p_{(A \times A) \times C} \end{array}$$

is an isomorphism.

Definition 5.2.23. *A* FOFIMELL *fibration is a triple of fibrations (p^-, p, p^+) such that:*

- *p has monoidal structures $(\otimes, \mathbf{I})$ and $(\parr, \bot)$.*
- *There is a vertical natural transformation $\mathbf{dist}_{\varphi,\psi,\phi} : \varphi \otimes (\psi \parr \phi) \to (\varphi \otimes \psi) \parr \phi$.*
- *$(p, \otimes, \mathbf{I})$ is fiberwise monoidal closed.*
- *p has simple sums and products.*
- *p^+ has fibered cartesian product.*
- *There is fibered LNL adjunction between $(p, \otimes, \mathbf{I})$ and $(p^+, \times, \mathbf{I})$ inducing a fibered comonad $!$ over p.*
- *p^- has fibered coproduct.*
- *There an oplax monoidal fibered adjunction between $(p, \parr, \bot)$ and $(p^-, +, 0)$ inducing a fibered monad $?$ over p.*
- *We have vertical natural transformations*

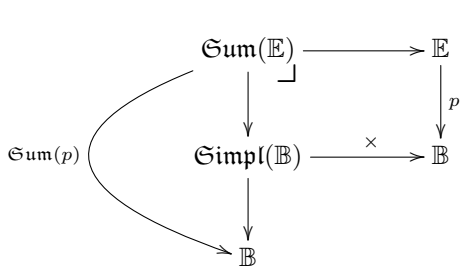
$$!\varphi \otimes ?\psi \quad \longrightarrow \quad ?(!\varphi \otimes \psi) \qquad\qquad !(\varphi \parr ?\psi) \quad \longrightarrow \quad !\varphi \parr ?\psi$$

5.3 The Dialectica construction

In this section we define the structure of the functor $\mathfrak{Dial} : \mathfrak{Fib}(\mathbb{B}) \to \mathfrak{Fib}(\mathbb{B})$ corresponding to the Dialectica interpretation. This construction was already considered by Hofstra [31] in order to clarify the universal property of the construction. In particular, it is shown that the interpretation has the structure of a pseudo-monad, which can be recovered as the composition of two other pseudo-monads $\mathfrak{Sum} \circ \mathfrak{Prod}$ and a distributive law. $\mathfrak{Sum}$ (resp. $\mathfrak{Prod}$) may be characterized in terms of universal property, namely, freely adding coproducts (resp. products). However, here we are interested in how the connective of full intuitionistic linear logic are modeled. It will turn out that the propositional part of p may be lifted to $\mathfrak{Dial}(p)$ as soon as $\mathbb{B}$ is supposed to be cartesian closed and quantifications will be modelled. Our main point of divergence with previous work is that we give a non-standard interpretation for exponentials of linear logic rooted in a polarity system. In a nutshell, $\mathfrak{Sum}$ (resp. $\mathfrak{Prod}$) shall correspond to the world of *positive* (resp. *negative*) predicates, and the embedding $\mathfrak{Sum}(p) \to \mathfrak{Dial}(p)$ (resp. $\mathfrak{Prod}(p) \to \mathfrak{Dial}(p)$) admits a right (resp. left) monoidal adjoint when p has sums (resp. products), a strong assumption. This give rise to exponentials, which, rather than adding computational content enabling duplication, allow one player not to have to play. To do so, the winning condition gets more complex and requires sums.

5.3.1 The $\mathfrak{Sum}$ construction

Before discussing $\mathfrak{Dial}$, we first discuss the simpler functor $\mathfrak{Sum} : \mathfrak{Fib}(\mathbb{B}) \to \mathfrak{Fib}(\mathbb{B})$, which plays a key rôle in defining !. $\mathfrak{Sum}$ is a broad generalization of the simple fibration over $\mathbb{B}$, which can be recovered as $\mathfrak{Sum}(\mathrm{Id}_{\mathbb{B}})$. Given an arbitrary fibration $p : \mathbb{E} \to \mathbb{B}$, $\mathfrak{Sum}(p)$ is built as prescribed by the following diagram in $\mathfrak{Cat}$. $\mathfrak{Sum}(p)$ is readily is seen to be a fibration using Lemma 5.2.11.



with

$$\begin{array}{rccc} \times : & \mathfrak{Simpl}(\mathbb{B}) & \to & \mathbb{B} \\ & (X, Y) & \mapsto & X \times Y \\ & (f, f_0) & \mapsto & \langle f \circ \pi_1, f_0 \rangle \end{array}$$

We give a direct description in the following definition.

Definition 5.3.1. *Let $p : \mathbb{E} \to \mathbb{B}$ be a fibration with cartesian products in $\mathbb{B}$. The total space $\mathfrak{Sum}(\mathbb{E})$ of the associated fibration $\mathfrak{Sum}(p)$ is defined as follows:*

- **Objects:** *objects are triples (A, U, φ) such that A and U are objects of $\mathbb{B}$ and φ belongs to $p_{A \times U}$. We write sometimes write such triples $(a : A, u : U, \varphi(a, u))$.*
- **Morphisms:** *morphisms from $(a : A, u : U, \varphi(a, u))$ to $(b : B, v : V, \psi(b, v))$ are triples (f, f_0, α) where*
  - *$f : A \to B$ is a $\mathbb{B}$-morphism.*
  - *$f_0 : A \times U \to V$ is a $\mathbb{B}$-morphism.*
  - *$\alpha : \varphi(a, u) \to \psi(f(a), f_0(a, u))$ is a $p_{A \times U}$-morphism.*
- **Composition:** *given $(f, f_0, \alpha) : (a : A, u : U, \varphi(a, u)) \to (b : B, v : V, \psi(b, v))$ and $(g, g_0, \beta) : (b : B, v : V, \psi(b, v)) \to (c : C, w : W, \phi(c, w))$, the composite is defined as $(g \circ f, g_0 \circ \langle f \circ \pi_1, f_0 \rangle, \langle f \circ \pi_1, f_0 \rangle^*(\beta) \circ \alpha)$*

The fibration itself $\mathfrak{Sum}(p) : \mathfrak{Sum}(\mathbb{E}) \to \mathbb{B}$ is defined as the projection on the first component. Therefore, a morphism (f, f_0, α) is vertical when $f = \mathrm{id}$ and a cartesian lift of $f : A \to B$ with target $(b : B, u : U, \varphi(b, u))$ is given by $(f, \mathrm{id}, (f \times \mathrm{id})^*) : (a : A, u : U, \varphi(f(a), u)) \to (b : B, u : U, \varphi(b, u))$.

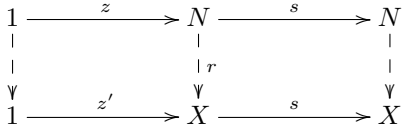
The intuitive idea is that a walking predicate $\varphi(a)$ of $\mathfrak{Sum}(p)$ corresponds to a predicate "$\exists u\ \varphi_S(u, a)$", and deduction in $\mathfrak{Sum}(p)$ should be carried out accordingly. However, let us remark that this intuition may be somewhat misleading, as the quotes indicates; the notion of sum therein do *not* correspond to the notion of sum in p, but rather a stronger one which should be witnessed by morphism in the base $\mathbb{B}$.

Example 5.3.2. *One may apply the $\mathfrak{Sum}$ construction to the syntactic fibration $p : \mathbb{E} \to \mathsf{Mealy}$ corresponding to* FOM*. Then, a walking predicate of $\mathfrak{Sum}(p)$ is a triple $(a : A^\omega, u : U^\omega, \varphi(a, u))$ where A and U are alphabets and φ is a* FOM *formula. An entailment*

$$(a : A^\omega, u : U^\omega, \varphi(a, u)) \quad \to \quad (a : A^\omega, v : V^\omega, \psi(a, v))$$

is essentially a Mealy*-morphism, that is, a f.s. causal function $f : A^\omega \times U^\omega \to V^\omega$ such that $\varphi(a, u) \vdash \psi(a, f(a, u))$ is derivable in* FOM*; therefore, $\mathfrak{Sum}(p)$ is not a preposetal fibration like* FOM*. In fact, it is now easy to check that $\mathfrak{Sum}(p)$ is equivalent to the fibration generated by the automata-based model of* SFOM *given in Chapter 3.*

Example 5.3.3. *Consider a cartesian-closed category $\mathbb{T}$ with a* natural number object *N, that is, an object N together with morphisms $z : 1 \to N$ and $s : N \to N$ such that, for every object X of $\mathbb{T}$ and morphisms $z' : 1 \to X$ and $s' : X \to X$, there is a unique map r making the following diagram commute.*



The above requirements essentially state that $\mathbb{T}$ is a model of Gödel's system T with sums, an extension of simply-typed λ-calculus with a recursor for natural numbers. In particular, one may be build such a category syntactically by taking system T types as objects and system T terms as morphisms.

Now, letting p be the fibration corresponding to its standard classical model as given in Example 5.2.8, the fibration $\mathfrak{Sum}(p)$ gives an interpretation first-order arithmetic essentially corresponding to typed realizability*. Predicates are interpreted as triples $(n : N, u : U, \varphi(n,u))$ and entailments $(n : N, u : U, \varphi(n,u)) \to (n : N, v : V, \psi(n,v))$ are $\mathbb{T}$-morphisms $f : N \times U \to V$ such that $\varphi(n,u) \to \psi(n, f(n,u))$ holds in p.*

Lemma 5.3.4. *If p has a symmetric monoidal structure $(\otimes, \mathbf{I})$, the following is the object part of a symmetric monoidal structure over $\mathfrak{Sum}(p)$.*

$$\begin{array}{lrcl} \textbf{Unit:} & A & \mapsto & (a : A, b : \mathbf{I}, \mathbf{I}_A) \\ \textbf{Product:} & (a : A, u : U, \varphi(a,u)), (a : A, v : V, \psi(a,v)) & \mapsto & (a : A, (u,v) : U \times V, \varphi(a,u) \otimes \psi(a,v)) \end{array}$$

Furthermore, if $\otimes$ is actually a cartesian product and $\mathbf{I}$ a terminal object, then this lifting coincide with a cartesian structure over $\mathfrak{Sum}(p)$.

Proposition 5.3.5. *If p has a symmetric monoidal closed structure $(\otimes, \mathbf{I})$, simple products and $\mathbb{B}$ is cartesian closed, then the symmetric monoidal structure over $\mathfrak{Sum}(p)$ determined in Lemma 5.3.4 is closed, the linear arrow given by*

$$(a : A, u : U, \varphi(a,u)), (a : A, v : V, \psi(a,v)) \quad \mapsto \quad (a : A, f : V^U, \forall u\ \varphi(a,u) \multimap \psi(a, \mathrm{ev}(f,u)))$$

Lemma 5.3.6. *Suppose that p has two monoidal structures $(\otimes, \mathbf{I})$ and $(\parr, \bot)$, as well as a distributivity law $\mathbf{dist}_{\varphi,\psi,\phi} : \varphi \otimes (\psi \parr \phi) \to (\varphi \otimes \psi) \parr \phi$. Then $\mathfrak{Sum}(p)$ also has a distributivity law between the induced monoidal structures defined as follows for the objects $(a : A, u : U, \varphi(a,u)), (a : A, v : V, \psi(a,v))$ and $(a : A, w : W, \phi(a,w))$.*

$$A \times (U \times (V \times W)) \xrightarrow{\pi_2} U \times (V \times W) \xrightarrow{\sim} (U \times V) \times W$$

$$\varphi(a,u) \otimes (\psi(a,v) \parr \phi(a,w)) \xrightarrow{\mathbf{dist}} (\varphi(a,u) \otimes \psi(a,v)) \parr \phi(a,w)$$

Lemma 5.3.7. *$\mathfrak{Sum}(p)$ has all simple sums; considering objects of the base A, B and the projection $\pi : A \times B \to A$, the object part of the right adjoint $\exists_\pi : \mathfrak{Sum}(p)_{A \times B} \to \mathfrak{Sum}(p)_A$ is*

$$\exists_\pi : \quad ((a,b) : A \times B, u : U, \varphi(a,b,u)) \quad \mapsto \quad (a : A, (u,b) : U \times B, \varphi(a,u,b))$$

Furthermore, if $\mathbb{B}$ is cartesian-closed and p has simple products, then $\mathfrak{Sum}(p)$ also has simple products $\forall_\pi$, whose object part is

$$\forall_\pi : \quad ((a,b) : A \times B, u : U, \varphi(a,b,u)) \quad \mapsto \quad (a : A, f : U^B, \forall b^B\ \varphi(a,b,\mathrm{ev}(f,b))))$$

As pointed out in [31], $\mathfrak{Sum}$ extends to a pseudo-monad over $\mathfrak{Fib}(\mathbb{B})$, whose category of algebra correspond to a restriction of $\mathfrak{Fib}(\mathbb{B})$, where morphisms are required to preserve simple sums. While we are not going to investigate the general properties of $\mathfrak{Sum}$, we are going to employ the instantiation of the unit

$$\begin{array}{rccl} \eta^{\mathfrak{Sum}(p)} : & p & \to & \mathfrak{Sum}(p) \\ & \varphi \in p_A & \mapsto & (a : A, * : 1, \varphi(a)) \end{array}$$

in the sequel. In fact, object (isomorphic) to some $\eta^{\mathfrak{Sum}(p)}$ will be called *deterministic*.

Lemma 5.3.8. *$\eta^{\mathfrak{Sum}(p)}$ has a fibered left adjoint $\exists^p$ whose object part is*

$$\begin{array}{rccc} \exists^p : & \mathfrak{Sum}(p) & \to & p \\ & (a : A, u : U, \varphi(a,u)) & \mapsto & (a : A, \exists u\ \varphi(a,u)) \end{array}$$

if and only if p has fibered sums.

Let us conclude this subsection by recalling that there is a dual construction $\mathfrak{Prod}(p)$, that is also of interest to us. As we did for $\mathfrak{Sum}(p)$, let us spell out the definition.

Definition 5.3.9. *Let $p : \mathbb{E} \to \mathbb{B}$ be a fibration with cartesian products in $\mathbb{B}$. The total space $\mathfrak{Prod}(\mathbb{E})$ of the associated fibration $\mathfrak{Prod}(p)$ is defined as follows:*

- **Objects:** *objects are triples (A, X, φ) such that A and X are objects of $\mathbb{B}$ and φ belongs to $p_{A\times X}$. We write sometimes write such triples $(a : A, x : X, \varphi(a, x))$.*

- **Morphisms:** *morphisms from $(a : A, x : X, \varphi(a, x))$ to $(b : B, x : X, \psi(b, x))$ are triples (f, f_0, α) where*

  - *$f : A \to B$ is a $\mathbb{B}$-morphism.*
  - *$f_0 : A \times Y \to X$ is a $\mathbb{B}$-morphism.*
  - *$\alpha : \varphi(a, f_0(a, y)) \to \psi(f(a), y)$ is a $p_{A\times Y}$-morphism.*

- **Composition:** *given $(f, f_0, \alpha) : (a : A, x : X, \varphi(a, x)) \to (b : B, y : y, \psi(b, y))$ and $(g, g_0, \beta) : (b : B, y : Y, \psi(b, y)) \to (c : C, z : Z, \phi(c, z))$, the composite is defined as $(g \circ f, f_0 \circ \langle g \circ \pi_1, g_0\rangle, \langle g \circ \pi_1, g_0\rangle^*(\beta) \circ \alpha)$*

The fibration itself $\mathfrak{Prod}(p) : \mathfrak{Prod}(\mathbb{E}) \to \mathbb{B}$ is defined as the projection on the first component.

As remarked in [31], $\mathfrak{Prod}(p) \cong \mathfrak{Sum}(p^{\mathrm{op}})^{\mathrm{op}}$.

5.3.2 The $\mathfrak{Dial}$ construction

We are now ready to describe the fibration $\mathfrak{Dial}(p)$. As for $\mathfrak{Sum}(p)$, their is a basic intuition that a walking predicate $\varphi(a)$ of $\mathfrak{Dial}(p)$ should correspond to a predicate "$\exists u \forall x\ \varphi_D(u, x, a)$" of p; the same caveat on the interpretation of quantifiers apply, namefly that they should be understood more as quantifiers determined by $\mathbb{B}$ rather than by the logic associated to p as a whole. This may lead us to want $\mathfrak{Dial}(p) = \mathfrak{Sum}(\mathfrak{Prod}(p))$. As before, let us give an expanded definition definition below, which ensures that $\mathfrak{Dial}(p) \cong \mathfrak{Sum}(\mathfrak{Prod}(p))$.

Definition 5.3.10. *Let $p : \mathbb{E} \to \mathbb{B}$ be a fibration with cartesian products in $\mathbb{B}$. The total space $\mathfrak{Dial}(\mathbb{E})$ of the associated fibration $\mathfrak{Dial}(p)$ is defined as follows:*

- **Objects:** *objects are triples (A, U, X, φ) such that A, U and X are objects of $\mathbb{B}$ and φ belongs to $p_{A\times U\times X}$. We write sometimes write such triples $(a : A, u : U, x : X, \varphi(a, u, x))$.*

- **Morphisms:** *morphisms from $(a : A, u : U, x : X, \varphi(a, u, x))$ to $(b : B, v : V, y : Y, \psi(b, v, y))$ are tuples (s, f, F, α) where*

  - *$s : A \to B$ is a $\mathbb{B}$-morphism.*
  - *$f : A \times U \to V$ is a $\mathbb{B}$-morphism.*
  - *$F : A \times U \times Y \to X$ is a $\mathbb{B}$-morphism.*
  - *$\alpha : \varphi(a, u, F(a, u, y)) \to \psi(s(a), f(a, u), y)$ is a $p_{A\times U\times Y}$-morphism.*

- **Composition:** *given*

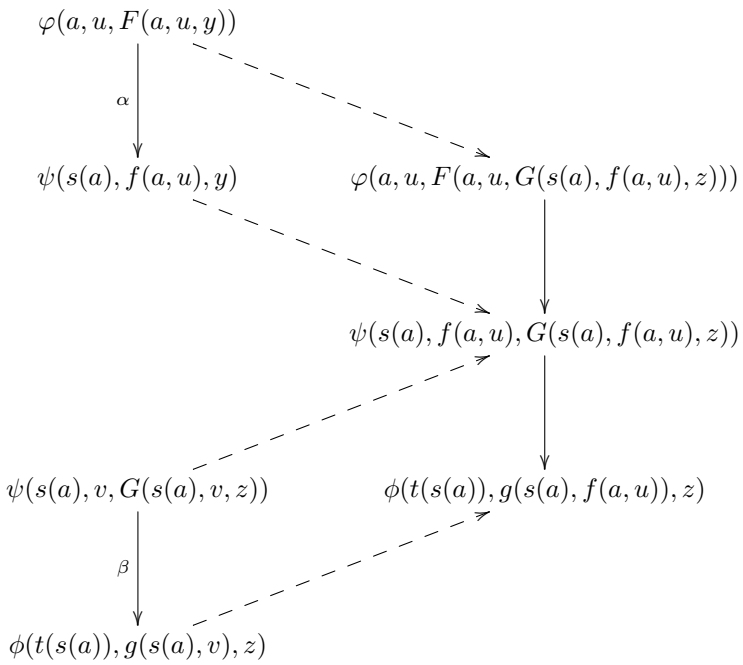
$$(s, f, F, \alpha) : (a : A, u : U, x : X, \varphi(a, u, x)) \to (b : B, v : V, y : Y, \psi(b, v, y)) \quad \text{and}$$
$$(t, g, G, \beta) : (b : B, v : V, y : Y, \psi(b, v, y)) \to (c : C, w : W, z : Z, \phi(c, w, z))$$

the composite is defined as

$$(t \circ s, g \circ \langle s \circ \pi_1, f\rangle, F \circ \langle \pi_1, \pi_2, G \circ \langle s \circ \pi_1, f \circ \langle \pi_1, \pi_2\rangle, \pi_3\rangle\rangle, \gamma)$$

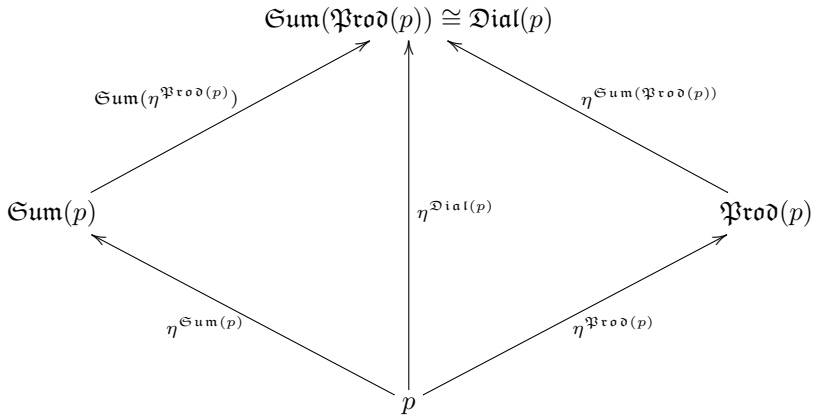
where γ is defined as the composite of the arrows on the right-handside of the following

diagram, the dashed arrows denoting cartesian lifts.



The fibration itself $\mathfrak{Dial}(p) : \mathfrak{Dial}(\mathbb{E}) \to \mathbb{B}$ *is defined as the projection on the first component.*

As shown in [31], $\mathfrak{Dial} \cong \mathfrak{Sum} \circ \mathfrak{Prod}$ is functorial. There is an embedding $\eta^{\mathfrak{Dial}(p)} : p \to \mathfrak{Dial}(p)$, which may be computed as any of the following two composite sitting in the following commutative diagram.



$$\begin{array}{rccc} \eta^{\mathfrak{Dial}(p)} : & p & \to & \mathfrak{Dial}(p) \\ & \varphi \in p_A & \mapsto & (a : A, * : 1, * : 1, \varphi(a)) \end{array}$$

Now, we survey the structure that $\mathfrak{Dial}(p)$ may inherit from p alone, which turns out to largely come from our preliminary observation on $\mathfrak{Sum}(p)$ and the fact that $\mathfrak{Dial}(p) \cong \mathfrak{Prod}(\mathfrak{Sum}(p))$. At the propositional level, the only new aspect is the monoidal closure of $\mathfrak{Dial}(p)$, which is inherited from the monoidal closure of p when $\mathbb{B}$ happens to be cartesian-closed.

First, symmetric monoidal structures may be inherited from p by composing Lemma 5.3.4 with its dual for $\mathfrak{Prod}$.

Lemma 5.3.11. *Suppose that* $p : \mathbb{E} \to \mathbb{B}$ *has a monoidal structure* $(\otimes, unit)$. $\mathfrak{Dial}(p)$ *inherits a monoidal structure, whose product, also denoted* $\otimes$*, has the following object component.*

$$\left(\begin{array}{c} a : A, u : U, x : X \\ \varphi(a,u,x) \end{array} \right), \left(\begin{array}{c} a : A, v : V, y : Y \\ \psi(a,v,y) \end{array} \right) \mapsto \left(\begin{array}{c} a : A, (u,v) : U \times V, (x,y) : X \times Y \\ \varphi(a,u,x) \otimes \psi(a,v,y) \end{array} \right)$$

Similarly, distributive laws between monoidal products may be inherited from p by applying Lemma 5.3.6 twice.

Lemma 5.3.12. *Suppose that* p *has two monoidal structures* $(\otimes, \mathbf{I})$ *and* $(\parr, \bot)$*, as well as a distributivity law* $\mathbf{dist}_{\varphi,\psi,\phi} : \varphi \otimes (\psi \parr \phi) \to (\varphi \otimes \psi) \parr \phi$*. Then* $\mathfrak{Dial}(p)$ *also has a distributivity law between the induced monoidal structures defined as follows*

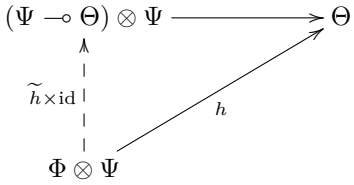
Lemma 5.3.13. *Suppose that $p : \mathbb{E} \to \mathbb{B}$ has a monoidal closed structure $(\otimes, \mathbf{I})$ and that $\mathbb{B}$ is cartesian-closed. Then, $\mathfrak{Dial}(p)$ inherits a monoidal closed structure. The monoidal product is given as per 5.3.11, and the object part of the functor $(a : A, v : V, y : Y, \psi(a,v,y)) \multimap - : \mathfrak{Dial}(p)_A \to \mathfrak{Dial}(p)_A$ is*

$$\begin{pmatrix} a : A, u : U, x : X \\ \varphi(a,u,x) \end{pmatrix} \mapsto \begin{pmatrix} a : A, (f,F) : V^U \times X^{U\times Y}, (u,y) : U \times Y \\ \varphi(a,u,F(a,u,y)) \multimap \psi(a, f(a,u), y) \end{pmatrix}$$

Proof. Let

$$\begin{aligned} \Phi &= \begin{pmatrix} a : A, u : U, x : X \\ \varphi(a,u,x) \end{pmatrix} \\ \Psi &= \begin{pmatrix} a : A, v : V, y : Y \\ \psi(a,v,y) \end{pmatrix} \\ \Theta &= \begin{pmatrix} a : A, w : W, z : Z \\ \theta(a,w,z) \end{pmatrix} \end{aligned}$$

be objects of $\mathfrak{Dial}(p)_A$. We need to exhbit a map $\mathrm{ev} : (\Psi \multimap \Theta) \otimes \Psi \to \Theta$ such that, for every map $h : \Phi \otimes \Psi \to \Theta$, there exists a unique map $\widetilde{h} : \Phi \to \Psi \multimap \Theta$ making the following diagram commute.



The map $\mathrm{ev} = (\mathrm{id}, \mathrm{ev}_1, \mathrm{ev}_2, \mathrm{ev}_3)$ is defined as follows:

- $\mathrm{ev}_1 : A \times ((W^V \times Y^{V\times Z}) \times V) \to W$ is the composite

$$A \times ((W^V \times Y^{V\times Z}) \times V) \xrightarrow{\langle \pi_1 \circ \pi_1, \pi_2 \rangle \circ \pi_2} W^V \times V \xrightarrow{\quad \mathrm{ev} \quad} W$$

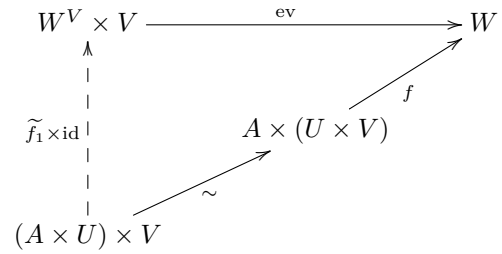
- $\mathrm{ev}_2 : A \times ((W^V \times Y^{V\times Z}) \times V) \times Z \to V \times Z$ is the pairing of

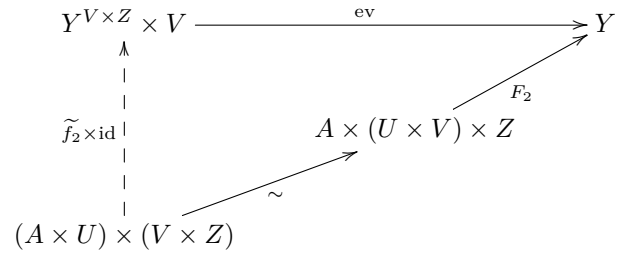
$$A \times ((W^V \times Y^{V\times Z}) \times V) \times Z \xrightarrow{\quad \pi_2 \circ \pi_2 \quad} V$$

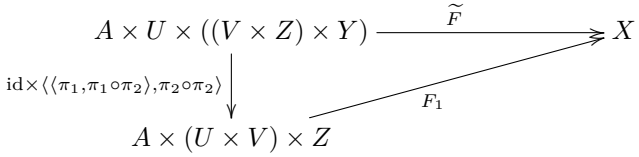
$$A \times ((W^V \times Y^{V\times Z}) \times V) \times Z \xrightarrow{\quad \pi_3 \quad} Z$$

- $\mathrm{ev}_3 : (\psi(a,v,\mathrm{ev}(F,\langle v,z\rangle)) \multimap \theta(a,\mathrm{ev}(f,v),z)) \otimes \psi(a,v,\mathrm{ev}(F,\langle v,z\rangle)) \to \theta(a,\mathrm{ev}(f,v),z))$ is the evaluation map in p.

Writing $h = (\mathrm{id}, f, \langle F_1, F_2\rangle, \alpha)$ and $\widetilde{h} = (\mathrm{id}, \langle \widetilde{f}_1, \widetilde{f}_2\rangle, \widetilde{F}, \widetilde{\alpha})$, On the first three components, this amounts to having the following diagrams commuting







It is clear that they uniquely determine $\widetilde{f_1}$ and $\widetilde{f_2}$ to be curryfication and $\widetilde{F}$ to be F_1 precomposed with a suitable projection. Similarly, $\widetilde{\alpha}$ is then forced to be the curryfication of α.

Then one would need to check the Beck-Chevalley condition to conclude by Lemma 5.2.18; this is rather straightforward to reduce this to easy equational reasoning and the the Beck-Chevalley condition for the monoidal closure in p.

□

Lemma 5.3.14. *The fibration $\mathfrak{Dial}(p)$ has simple sums, and, if $\mathbb{B}$ is cartesian-closed, $\mathfrak{Dial}(p)$ has also simple products. Given a projection $\pi : A \times B \to A$ and an object $(U, X, \varphi) : A \times B$, the object component of the functors $\exists_\pi, \forall_\pi$ are*

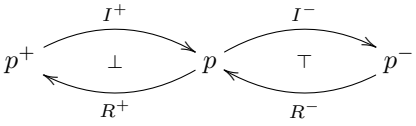
$$\exists_\pi : \begin{pmatrix} (a,b) : A \times B, u : U, x : X \\ \varphi(a,b,u,x) \end{pmatrix} \mapsto \begin{pmatrix} a : A, (u,b) : U \times B, x : X \\ \varphi(a,b,u,x) \end{pmatrix}$$
$$\forall_\pi : \begin{pmatrix} (a,b) : A \times B, u : U, x : X \\ \varphi(a,b,u,x) \end{pmatrix} \mapsto \begin{pmatrix} a : A, f : U^B, (x,b) : X \times B \\ \varphi(a,v,\mathrm{ev}(f,b),x) \end{pmatrix}$$

Proof. We do not give the explicit construction here, but appeal repeatedly to Lemma 5.3.7, using the fact that $\mathfrak{Dial}(p) \cong \mathfrak{Sum}(\mathfrak{Prod}(p))$.

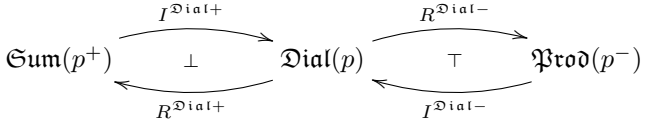
- $\mathfrak{Dial}(p)$ clearly has simple sums since it is a $\mathfrak{Sum}$ fibration.
- Dually, $\mathfrak{Prod}(p)$ has simple products.
- Therefore, since $\mathbb{B}$ is additionally cartesian-closed, $\mathfrak{Sum}(\mathfrak{Prod}(p))$ has simple products.

Unwinding the definitions and checking that the definition on objects coincide with the above is straightforward. □

Theorem 5.3.15. *Let (p^+, p, p^-) be a* FOFIMELL *fibration with the following string of monoidal adjunctions for exponential modalities.*



Then, this FOFIMELL *fibration may be lifted to another* FOFIMELL*-fibration $(\mathfrak{Sum}(p^+), \mathfrak{Dial}(p), \mathfrak{Prod}(p^-))$ by ensuring $I^{\mathfrak{Dial}+} \cong \mathfrak{Sum}(\eta^{\mathfrak{Prod}(p)} \circ I^+)$, $R^{\mathfrak{Dial}+} \cong \mathfrak{Sum}(\forall^{p^+} \circ R^+)$, $R^{\mathfrak{Dial}-} \cong \eta^{\mathfrak{Sum}(\mathfrak{Prod}(p))} \circ \mathfrak{Prod}(I^-)$ and $I^{\mathfrak{Dial}-} \cong \forall^{\mathfrak{Prod}(p)} \circ \mathfrak{Dial}(R^-)$.*



Proof. Assuming the previous Lemma, the crucial point is to check that we have suitable adjunctions $I^{\mathfrak{Dial}+} \dashv R^{\mathfrak{Dial}+}$ and $R^{\mathfrak{Dial}-} \dashv I^{\mathfrak{Dial}-}$ and the vertical natural transformations.

$$!\varphi \otimes ?\psi \quad \longrightarrow \quad ?(!\varphi \otimes \psi) \qquad\qquad !(\varphi \parr ?\psi) \quad \longrightarrow \quad !\varphi \parr ?\psi$$

Let us define the adjunctions on objects, and derive the action of the induced comonad and monad:

$$\begin{array}{lcl} I^{\mathfrak{Dial}+}(a : A, u : U, \varphi(a,u)) & := & (a : A, u : U, * : 1, I^+(\varphi(a,u))) \\ R^{\mathfrak{Dial}+}(a : A, u : U, x : X, \varphi(a,u,x)) & := & (a : A, u : U, R^+(\forall x^X\ \varphi(a,u,x))) \\ !(a : A, u : U, x : X, \varphi(a,u,x)) & = & (a : A, u : U, * : 1, !(\forall x^X\ \varphi(a,u,x))) \end{array}$$

$$\begin{array}{lcl} I^{\mathfrak{Dial}-}(a : A, x : X, \varphi(a,x)) & := & (a : A, * : 1, x : X, I^-(\varphi(a,x))) \\ R^{\mathfrak{Dial}-}(a : A, u : U, x : X, \varphi(a,u,x)) & := & (a : A, f : X^U, R^-(\exists u^U\ \varphi(a,u,\mathrm{ev}(f,u)))) \\ ?(a : A, u : U, x : X, \varphi(a,u,x)) & = & (a : A, * : 1, f : X^U, ?(\exists u^U\ \varphi(a,u,\mathrm{ev}(f,u)))) \end{array}$$

One may check by hand that $I^{\mathfrak{Dial}+} \dashv R^{\mathfrak{Dial}+}$ (respectively $R^{\mathfrak{Dial}-} \dashv I^{\mathfrak{Dial}-}$) and that $I^{\mathfrak{Dial}+}$ and $R^{\mathfrak{Dial}+}$ may be equipped with a lax (respectively oplax for $R^{\mathfrak{Dial}-}$ and $I^{\mathfrak{Dial}-}$) monoidal structure by hand. A more abstract approach would be to notice the equivalence of fibred functors announed in the statement and use the fact that, in an arbitrary 2-category such as $\mathfrak{Fib}(\mathbb{B})$, (op)lax monoidal adjunctions compose and are preserved by functors.

By Lemma 5.3.7, since $\mathbb{B}$ is assumed to be cartesian-closed and p^+ has all simple products, so does $\mathfrak{Sum}(p^+)$. By a completely dual argument, $\mathfrak{Prod}(p^-)$ has all simple sums.

In order to conclude, it thus suffices to show that we have the following vertical natural transformations arbitrary predicate φ and ψ of $\mathfrak{Dial}(p)$.

$$!\varphi \otimes ?\psi \quad \longrightarrow \quad ?(!\varphi \otimes \psi) \qquad\qquad !(\varphi \parr ?\psi) \quad \longrightarrow \quad !\varphi \parr ?\psi$$

Working in the fiber over A and expanding the definitions, it means we should have the following vertical natural transformations.

$$\left(\begin{array}{c} a:A, \quad u:U, \quad f:Y^V \\ \big(!\forall x^X\ \varphi(a,u,x)\big) \otimes \big(?\exists v^V\ \psi(a,v,\mathrm{ev}(f,v))\big) \end{array}\right) \quad \longrightarrow \quad \left(\begin{array}{c} a:A, \quad *:1, \quad g:Y^{U\times V} \\ ?\exists(u,v)^{U\times V}\ \big(!\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle))\big) \end{array}\right)$$

$$\left(\begin{array}{c} a:A, \quad u:U, \quad *:1 \\ !\forall(x,f)^{X\times Y^V}\ \big(\varphi(a,u,x) \parr ?\exists v^V\ \psi(a,v,\mathrm{ev}(f,v))\big) \end{array}\right) \quad \longrightarrow \quad \left(\begin{array}{c} a:A, \quad u:U, \quad f:Y^V \\ \big(!\forall x^X\ \varphi(a,u,x)\big) \parr \big(?\exists v^V\ \psi(a,v,\mathrm{ev}(f,v))\big) \end{array}\right)$$

Let us focus on the first one. The $\mathbb{B}$-level part of the morphism is induced by the unique map $A \times U \to 1$ and the obvious partial evaluation map $A \times U \times Y^{U\times V} \to U \times Y^{U\times V} \to Y^V$. At the level of propositions, it thus suffices to give a proof in p of the following implication.

$$\big(!\forall x^X\ \varphi(a,u,x)\big) \otimes \big(?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle))\big) \quad \multimap \quad ?\exists(u,v)^{U\times V}\ \big(!\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle))\big)$$

Deriving it in the FIMELL sequent calculus is straightforward. Note that its interpretation into p makes crucial use of the corresponding natural transformation $!\varphi \otimes ?\psi \quad \longrightarrow \quad ?(!\varphi \otimes \psi)$ in p_A.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle))}}{\psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash \exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle))}}{\psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle))} \qquad \dfrac{}{!\forall x^X\ \varphi(a,u,x) \vdash !\forall x^X\ \varphi(a,u,x)}}{!\forall x^X\ \varphi(a,u,x), \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash !\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle))}}{!\forall x^X\ \varphi(a,u,x), \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash \exists(u,v)^{U\times V}\ (!\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)))}}{!\forall x^X\ \varphi(a,u,x), \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash ?\exists(u,v)^{U\times V}\ (!\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)))}}{!\forall x^X\ \varphi(a,u,x), \exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash ?\exists(u,v)^{U\times V}\ (!\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,y))}}{!\forall x^X\ \varphi(a,u,x), ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash ?\exists(u,v)^{U\times V}\ (!\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)))}}{!\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)) \vdash ?\exists(u,v)^{U\times V}\ (!\forall x^X\ \varphi(a,u,x) \otimes ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,\langle u,v\rangle)))}$$

□

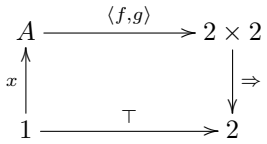
5.3.3 Relationship to Gödel's Dialectica

For the sake of illustration, let us consider a particular case corresponding roughly to the original functional interpretation given by Gödel in [25], whose goal was to give a consistency proof for first-order arithmetic from the proof of normalization of System T, a simply typed λ-calculus with primitive integers and a (higher-order) recursor[5]. We only here give an outline of the construction as an illustration; the interested reader may consult [4] or [40] for more details on System T, Gödel's functional interpretation and applications to proof-theory.

Consider the *initial* cartesian-closed category $\mathbb{T}$ with a natural number object and the coproduct $2 = 1 + 1$ (this latest addition is more for convenience than necessity) to use as a base; this may be built using the syntax of System T augmented with booleans and an if/then/else construct to define morphisms, with term equated up to $\beta\eta$-equivalence. Call $\bot, \top : 1 \to 2$ the two canonical global elements of the booleans. In particular, for every object A of $\mathbb{T}$, we may preorder morphisms $f : A \to 2$ by setting $f \leq g$ if and only if for every global element $x : 1 \to A$, the following diagram

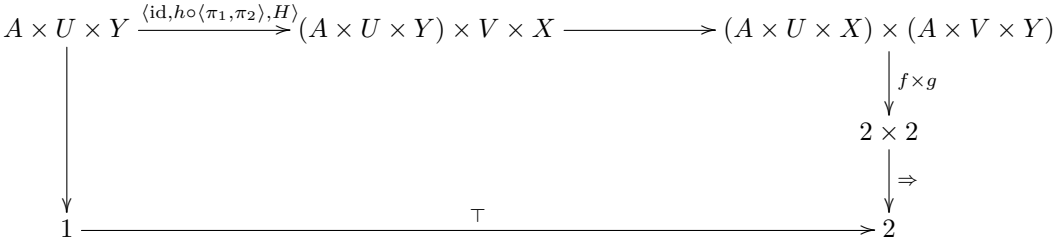
[5] System T may be alternatively be seen as a higher-order extension to primitive recursive functions. The crucial point differentiating the two is that System T's recursor may output higher-order functions rather than only natural numbers.

commutes (or, if seen as closed system T terms, we ask that for every closed term u of type A we have $f\ u =_\beta \top \ \Rightarrow\ g\ u =_\beta \top$)[6]



This map $A \mapsto ([A,2]_{\mathbb{T}}, \leq)$ extends to a contravariant functor $T : \mathbb{T}^{\mathrm{op}} \to \mathfrak{Cat}$ making $t := \int T \to \mathfrak{Cat}$ a preposetal fibration. Furthermore, owing to the internal boolean algebra structure of 2, t is also boolean. However, t does *not* have simple quantifications for straightforward recursive-theoretic reasons.

A predicate in $\mathfrak{Dial}(t)$ is a tuple (A, U, X, f) where A, U, X are objects of $\mathbb{T}$ and f a $\mathbb{T}$-morphism $A \times U \times X \to 2$, and a vertical map $(A, U, X, f) \to (A, V, Y, g)$ is a pair of maps (h, H) with $h : A \times U \to V$ and $H : A \times U \times Y \to X$ such that



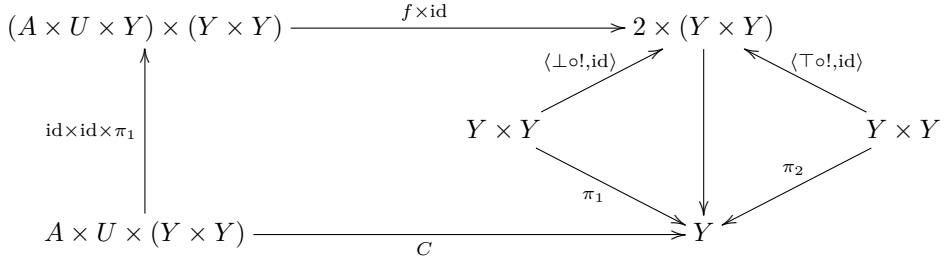
The subsequent material shows that $\mathfrak{Dial}(t)$ can interpret intuitionistic linear logic *with simple quantifiers*, as well as basic arithmetical predicates. In order to show that $\mathfrak{Dial}(t)$ may interpret Heyting arithmetic, one may[7] give non-canonical contraction and weakening maps for arbitrary $\mathfrak{Dial}(t)$ predicates $\Phi = (a : A, U, X, f : A \times U \times X \to 2)$.

$$w_\Phi : \Phi \multimap \mathbf{I} \qquad\qquad c_\Phi : \Phi \ \multimap\ \Phi \otimes \Phi$$

Such maps are available respectively because of the non-emptiness of the interpretation of types of $\mathbb{T}$ and the effective nature of the notion of truth value in t. More specifically, w_Φ can be taken to be some arbitrarily fixed map $\maltese_X : A \times U \times 1 \to 1 \to X$. Writing $c_\Phi = (c, C)$, $c : A \times U \to U \times U$ is the unique morphism factorizing through the diagonal map $U \xrightarrow{\langle \mathrm{id}, \mathrm{id} \rangle} U \times U$. On the other hand, $C : A \times U \times (Y \times Y) \to Y$, instead of duplicating an input of type U must pick wisely one of the two component of $Y \times Y$. One way to do this is consider the output of the map $f \circ (\mathrm{id} \times \mathrm{id} \times \pi_1)$: if it is $\top$, then we may pick the first component, otherwise we pick the second. Informally speaking, C corresponds to the System T term

$$\lambda(a, u, (y_1, y_2)).\mathtt{if}\ f(a, u, y_1)\ \mathtt{then}\ y_2\ \mathtt{else}\ y_1$$

Alternatively, C may be characterized as the only morphism making the following diagram commute.



[6]The appearance of global elements here is a distateful technicality. Although it will not be apparent since we do not provide proofs, this serves to ensure the correctness of the ad-hoc contraction map c_Φ in the sequel.

[7]An alternative approach would be to consider the cartesian product $\Phi \times \Phi'$ and give maps $\Phi \times \Phi' \to \Phi \otimes \Phi'$ and $\Phi \otimes \Phi' \to \Phi \times \Phi'$ and to use the canonical contraction and weakening maps associated with the cartesian product. While we have not treated them, cartesian product can be shown to exist in $\mathfrak{Dial}(t)$ provided that we have coproducts in the base (this is not the case here, but it would be straightforward to extend $\mathbb{T}$ to satisfy this desiderata). Those maps would involve essentialy the same kind of non-canonical "tricks" as those provided below. While we mention the cartesian product, let us remark that the main reason to consider $\otimes / \multimap$ is that $\mathfrak{Dial}(p)$ is not (fiberwise) cartesian closed. The generalization of the Dialectica construction considered in [51] recovers cartesian closure by using a generalized $\mathfrak{Dial}$ construction where families $X \to U$ are considered instead of pairs (U, X).

Then it can be checked (c, C) is a morphism in $\mathfrak{Dial}(t)$. Note that from a technical standpoint, this is proven using the strong normalization of System T.

Putting all of this together, this yields an interpretation of Heyting arithmetic in $\mathfrak{Dial}(t)$ via elementary means. Furthermore, it can be checked that $\mathfrak{Dial}(t)$ is non-degenerate if and only if $\mathbb{T}$ is non-degenerate. This reduction from the consistency of (the Dialectica interpretation of) HA to the non-degeneracy of system T is one of the main ingredient of Gödel's consistency proof of arithmetic. This reduction (as well as the reduction of consistency of PA to HA via a double-negation translation) is relatively elementary from the point of view of foundations[8] and readily formalizes in weak susbsystems of arithmetic; the foundationally hard part of the consistency proof of PA lies with the normalization of system T, which requires induction up to ϵ_0.

It should be stressed that since t does not have simple quantification, the canonical functor $\mathfrak{Sum}(t) \to \mathfrak{Dial}(t)$ is not part of a LNL-adjunction

5.3.4 Elimination of double linear negation

In general, $\mathfrak{Dial}(p)$ does not give rise to a model of classical linear logic. In the context of a symmetric monoidal closed fibration, this would be given by a choice of so-called *dualizing object* $\bot_A$ in each fiber p_A preserved by substitution. Recall that a dualizing object in a symmetric monoidal category is an object $\bot$ such that the canonical natural transformation

$$\Lambda(\mathrm{ev} \circ \gamma) \ : \ \varphi \ \to \ (\varphi \multimap \bot) \multimap \bot$$

is an isomorphism. For instance, take $\mathcal{C} = \mathbf{Set}$, p an arbitrary symmetric monoidal closed fibration and consider the fiber over 1 of $\mathfrak{Dial}(p)$. Suppose we are given a candidate dualizing object $\bot = (a : A, b : B, \psi)$ (possibly different from the unit of the tensorial $\parr$ of a FOFIMELL fibration). Then, for any object $\Phi = (u : U, x : X, \mathbf{I})$, we have

$$(\Phi \multimap \bot) \multimap \bot \cong (* : 1, F : A^{A^U \times X^{U \times B}} \times (U \times B)^{A^U \times X^{U \times B} \times B}, f : A^U \times X^{U \times B} \times B, \psi \multimap \psi)$$

An isomorphism $\Phi \cong (\Phi \multimap \bot) \multimap \bot$ would in particular induce an isomorphism $U \cong A^{A^U \times X^{U \times B}} \times (U \times B)^{A^U \times X^{U \times B} \times B}$, which is only possible when either U or X is a subsingleton. Therefore, $({}^D p)$ is never a model of classical linear logic when $\mathcal{C} = \mathbf{Set}$, or even $\mathbf{FinSet}$. However, this does not rule out the existence of morphisms $\varphi \to (\varphi \multimap \bot) \multimap \bot$ for every φ; we show that such a family exists for $\mathfrak{Dial}(p)$ when $\mathcal{C} = \mathbf{Set}, \mathbf{FinSet}$. This allow to show that, as far as entailment is concerned, classical linear logic is sound for those fibrations. However, the family of morphism $(\varphi \multimap \bot) \multimap \bot (\varphi \multimap \bot) \multimap \bot$ does not give rise to any kind of coherence condition; we do not even know if such a family may be arranged into a natural transformation. The proof crucially relies on the full axiom of choice in $\mathbf{Set}$.

Theorem 5.3.16. *Say that a* FOFIMELL*-fibration $p : \mathbb{E} \to \mathbb{C}$ eliminates double linear negation when, for every predicate φ, there is a vertical morphism $(\varphi \multimap \bot) \multimap \bot \to \varphi$ in $\mathbb{E}$.*

If p is a FOFIMELL*-fibration eliminating double linear negations, so is $\mathfrak{Dial}(p)$ if $\mathcal{C} = \mathbf{Set}$, assumed to satisfy the axiom of choice, or $\mathbf{FinSet}$.*

Proof. Assume that p is a FOFIMELL fibration over $\mathbf{Set}$ where double-linear negation may be eliminated. Write $\bot$ for the unit of the product $\parr$ of p and $\mathfrak{Dial}(p)$ (which one is meant can be inferred from context). Taking $\Phi = (a : A, u : U, x : X, \varphi(a, u, x))$ to be a predicate of $\mathfrak{Dial}(p)$, $(\Phi \multimap \bot) \multimap \bot$ is vertically isomorphic to

$$\big(a : A, F : U^{X^U}, f : X^U, (\varphi(a, \mathrm{ev}(F, f), \mathrm{ev}(f, \mathrm{ev}(F, f))) \multimap \bot) \multimap \bot\big)$$

Since p is assumed to admit double linear negation elimination, it is sufficient to exhibit a vertical map $\Phi \to \Psi$ with $\Psi = \big(a : A, F : U^{X^U}, f : X^U, \varphi(a, \mathrm{ev}(F, f), \mathrm{ev}(f, \mathrm{ev}(F, f)))\big)$. Such a map is given by:

- functions $g : A \times U^{X^U} \to U$ and $G : A \times U^{X^U} \times X \to X^U$
- a p-proof $\varphi(a, F, \mathrm{ev}(G, (a, F, x))) \to \varphi(a, \mathrm{ev}(g, (a, \mathrm{ev}(G, (a, F, x)))), x)$

[8] But not obvious from the above observations; it would still remain to be checked that the axioms of arithmetic, and in particular, the induction scheme is admissible in $\mathfrak{Dial}(t)$. We refer the reader to [4] for details.

We aim to have an essentially trivial p-proof; furthermore, g and G will not depend on their first component. To this end, it suffices to find set-theoretic functions $h : U^{X^U} \to U$ and $H : U^{X^U} \times X \to X^U$ such that, for every $F \in U^{X^U}$ and $x \in X$ we have

$$F(H(F,x)) = h(F) \qquad \text{and} \qquad H(F,x)(F(H(F,x))) = x$$

At this point, it is convenient to start reasoning in the language of type theory, which may be interpreted in **Set**: given a family of sets $(A_i)_{i\in I}$, $\sum_{i\in I} A_i$ designate the disjoint union and $\prod_{i\in I} A_i$ the cartesian product of the family. Recall that for every family $(A_{i,j})_{(i,j)\in I\times J}$, there is a canonical isomorphism

$$\prod_{i\in I}\sum_{j\in J} A_{i,j} \quad \cong \quad \sum_{f:I\to J}\prod_{i\in I} A_{i,f(i)}$$

which is sometimes known as the type-theoretic axiom of choice[9]. We may reformulate the above desiderata as the non-emptiness of a sum of products. Then, using the above isomorphism twice, this family can be shown to be isomorphic to

$$\prod_{F\in U^{X^U}}\sum_{u\in U}\prod_{x\in X}\sum_{f\in X^U}\{* \mid F(f) = u \quad \text{and} \quad f(u) = x\}$$

Write as shorthand $\neg A$ for the function space $A \to \emptyset$. By the genuine axiom of choice in **Set**, we know that for any family $(A_i)_{i\in I}$, the product

$$\prod_{i\in I} A_i^{\neg\neg A_i}$$

is non-empty. This allow to dualize the type-theoretic axiom of choice and show that, for any family $(A_{i,j})_{(i,j)\in I\times J}$, there exists a map

$$\prod_{f:I\to J}\sum_{i\in I} A_{i,f(i)} \quad \to \quad \sum_{i\in I}\prod_{j\in J} A_{i,j}$$

Therefore, we may fix $F \in U^{X^U}$ and apply this dual version of the type-theoretic axiom of choice to

$$\left(\sum_{f\in X^U}\{* \mid F(f) = u \quad \text{and} \quad f(u) = x\}\right)_{(u,x)\in U\times X}$$

Using once again the axiom of choice in **Set**, the non-emptiness of the original family can be deduced from the non-emptiness of the product

$$\prod_{F\in U^{X^U}}\prod_{\widetilde{x}\in X^U}\sum_{u\in U}\sum_{f\in X^U}\{* \mid F(f) = u \quad \text{and} \quad f(u) = \widetilde{x}(u)\}$$

which is easy: an inhabitant is given by the graph of the map

$$\begin{array}{lll} U^{X^U} \times X^U & \to & U \times X^U \times 1 \\ (F, \widetilde{x}) & \mapsto & (F(\widetilde{x}), \widetilde{x}, *) \end{array}$$

When $\mathcal{C} = \mathbf{FinSet}$, all families above are finite and choice may be safely eliminated. □

5.4 The characterization theorem

Up to now, we established that the construction $\mathfrak{Dial}$ preserves FOFIMELL fibrations. The proof-theoretic Dialectica interpretation defines a translation of formulas $\varphi \mapsto \varphi_D$ by induction over the syntax, which basically amounts to interpreting every connective as in $\mathfrak{Dial}(p)$ while remaining in p; the precise translation is given in Figure 5.1. The soundness theorem states that basic FOFIMELL deduction is preserved by induction on the proof.

$$\mathsf{FOFIMELL} \vdash \varphi \qquad \Longrightarrow \qquad \exists u\ \mathsf{FOFIMELL} \vdash \forall x\ \varphi_D(u,x)$$

From a technical perspective, this theorem amounts to checking that $\mathfrak{Dial}(p)$ has all the structure presented in the previous section.

[9]Note however that it does *not* require that **Set** validates the axiom of choice to be valid.

The other crucial theorem of the proof-theoretic approach to Dialectica is the *characterization theorem*, which is essentially an internalized version of the soundness theorem to $\mathfrak{Dial}(p)$-like systems. It requires extending of FOFIMELL with a choice scheme (LAC), several (linear) semi-intuitionistic principles (LSIP) and two specific exponential axioms (DEXP), so as to show the equivalence between FOMELL predicates $\varphi(a)$ and their Dialectica translation $\varphi^D(a) := \exists u\, \forall x\, \varphi_D(u,x,a)$.

$$\mathsf{FOFIMELL} + \mathsf{LSIP} + \mathsf{LAC} + \mathsf{DEXP} \vdash \varphi(a) \multimap \exists u\, \forall x\, \varphi_D(u,x,a)$$

From a structural point of view, it turns out that the group of axioms LSIP + LAC + DEXP can be interpreted in a proof-relevant way by asking that certain FOFIMELL proofs be actually isomorphisms, which is the case in $\mathfrak{Dial}(p)$ if p is a FOFIMELL fibrations. We therefore formulate LSIP + LAC + DEXP in a proof-relevant way in Definition 5.4.1.

Definition 5.4.1. *A* FOFIMELL *fibration p is said to satisfy:*

- LSIP *when the following canonical natural transformations are actually isomorphims.*

$$\begin{array}{ccccc}
(\forall a\ ?\varphi(a)) \otimes ?\psi & \longrightarrow & \forall a\ (?\varphi(a) \otimes ?\psi) & (1)\\
(\forall a\ ?\varphi(a)) \parr ?\psi & \longrightarrow & \forall a\ (?\varphi(a) \parr ?\psi) & (2)\\
\exists a\ (\varphi(a) \parr \psi) & \longrightarrow & (\exists a\ \varphi(a)) \parr \psi & (3)\\
\exists a\ (?\psi \multimap ?\varphi(a)) & \longrightarrow & ?\psi \multimap \exists a\ ?\varphi(a)) & (4)\\
\exists a\ (?!\varphi(a) \multimap ?!\psi) & \longrightarrow & (\forall a\ ?!\varphi(a)) \multimap ?!\psi & (5)
\end{array}$$

- LAC *when the following natural transformation is a isomorphism.*

$$\exists f^{B^A}\ \forall a^A\ \varphi(a, \mathrm{ev}(f,a)) \qquad \longrightarrow \qquad \forall a^A\ \exists b^B\ \varphi(a,b) \qquad (6)$$

- PEXP *when there is a natural transformation*[10]

$$?!\varphi \quad \longrightarrow \quad !?\varphi \qquad (7)$$

and when the following natural transformations are isomorphisms.

$$\begin{array}{ccccc}
?!\varphi \otimes ?!\psi & \longrightarrow & ?(!\varphi \otimes !\psi) & (8)\\
!(?\varphi \parr ?\psi) & \longrightarrow & !?\varphi \parr !?\psi & (9)\\
!\varphi \multimap ?\psi & \longrightarrow & ?(!\varphi \multimap ?\psi) & (10)\\
!(?\varphi \multimap !\psi) & \longrightarrow & !\varphi \multimap ?\psi & (11)\\
!(a=b) & \longrightarrow & a=b & (12)\\
a=b & \longrightarrow & ?(a=b) & (13)
\end{array}$$

- DEXP *when the following natural transformations are isomorphisms.*

$$\begin{array}{ccccc}
\exists a\ !\varphi(a) & \longrightarrow & !\exists a\ \varphi(a) & (14)\\
?\exists a^A\ \forall b^B\ ?\varphi(a,b) & \longrightarrow & \forall f^{B^A}\ ?\exists a^A\ ?\varphi(a, \mathrm{ev}(f,a)) & (15)
\end{array}$$

Remark. *If one considers the interpretation of these statements in a non-linear fibration, the reader mind find them all rather straightforward, save for axioms 4, 5, 6 and 15, which correspond respectively to* Independance of Premiss *(4),* Markov's Principle *(5) and the axiom of choice (6).*

Theorem 5.4.2 (Soundness)**.** *If p is an arbitrary* FOFIMELL *fibration, then $\mathfrak{Dial}(p)$ is a* FOFIMELL+ LSIP + LAC + DEXP *fibration. Furthermore, if p satisfies* PEXP*, so does $\mathfrak{Dial}(p)$.*

Proof. Since we already know that $\mathfrak{Dial}(p)$ is a FOFIMELL fibration whenever p is by Theorem 5.3.15, one only needs to check that the additional axioms LSIP + LAC + DEXP are satisfied to prove the first half of the statement. All of the additional axioms, when interpreted in $\mathfrak{Dial}(p)$, the $\mathbb{B}$-components are easily seen to be isomorphic using the cartesian-closed structure of $\mathbb{B}$. Let us detail a couple of cases.

[10] In practice, one could also ask for a distributive law of the monad ? over the comonad ! which would also be preserved by the $\mathfrak{Dial}$ construction. Since we are later on motivated by provability rather than isomorphism, we content ourselves with a natural transformation.

- The linear independence of premiss (axiom 4 of LSIP)

$$\exists a^A\ (?\Psi \multimap ?\Phi(a)) \quad \simeq \quad ?\Psi \multimap \exists a^A\ ?\Phi(a))$$

for $\mathfrak{Dial}(p)$ predicates

$$?\Psi = \begin{pmatrix} b : B, * : 1, x : X \\ \psi(b, x)) \end{pmatrix} \qquad \text{and} \qquad \Phi = \begin{pmatrix} (a, b) : A \times B, * : 1, y : Y \\ \varphi(a, b, y) \end{pmatrix}$$

can be read off as

$$\begin{pmatrix} b : B, (a, g) : A \times X^Y, y : Y \\ \psi(b, \mathrm{ev}(g, y)) \multimap \varphi(a, b, y) \end{pmatrix} \qquad \simeq \qquad \begin{pmatrix} b : B, (a, g) : A^1 \times X^{Y \times 1}, y : Y \\ \psi(b, \mathrm{ev}(g, \langle y, * \rangle)) \multimap \varphi(\mathrm{ev}(a, *), b, y) \end{pmatrix}$$

which is obviously true in $\mathfrak{Dial}(p)$.

- For the linear axiom of choice (axiom 6, LAC), we are led to consider

$$\forall a^A \exists b^B\ \Phi(a, b) \qquad \to \qquad \exists f^{B^A} \forall a^A\ \Phi(a, \mathrm{ev}(f, a))$$

for the $\mathfrak{Dial}(p)$ predicate

$$\Phi = \begin{pmatrix} (a, b, c) : A \times B \times C, u : U, x : X \\ \varphi(a, b, c, u, x) \end{pmatrix}$$

can be read off as

$$\begin{pmatrix} c : C, f : (U \times B)^A, (a, x) : A \times X \\ \varphi(a, \pi_2(\mathrm{ev}(f, a)), c, \pi_1(\mathrm{ev}(f, a)), x) \end{pmatrix} \qquad \simeq \qquad \begin{pmatrix} c : C, (g, h) : U^A \times B^A, (a, x) : A \times X \\ \varphi(a, \mathrm{ev}(h, a), c, \mathrm{ev}(g, a), x) \end{pmatrix}$$

which is obviously true in $\mathfrak{Dial}(p)$.

Now, let us assume that p satisfies PEXP and show that $\mathfrak{Dial}(p)$ also does.

- For the axiom

$$?!\Psi \longrightarrow !?\Psi$$

we need to provide a natural proof scheme of

$$?\exists u^U !\forall f^{X^U} \psi(u, \mathrm{ev}(f, u)) \quad \longrightarrow \quad !\forall x^X ?\exists u^U \psi(u, x)$$

To this end, it suffices to note that there are canonical FOIMELL proofs

$$\begin{array}{lll} \rho_{\varphi}^{\exists,!} & : & \exists u^U !\varphi(u) \ \vdash\ !\exists u^U \varphi(u) \\ \rho_{\phi}^{\forall,?} & : & ?\forall x^X \phi(x) \ \vdash\ \forall x^X ?\varphi(x) \\ \rho^{\exists\forall,\forall\exists} & : & \exists u^U \forall f^{X^U} \psi(u, \mathrm{ev}(f, u)) \ \vdash\ \forall x^X \exists u^U \psi(u, x) \end{array}$$

and that the axiom scheme $\lambda_{\phi}^{?,!} : ?!\phi \to !?\phi$ in p can be instantiated at $\exists u^U \forall f^{X^U} \psi(u, \mathrm{ev}(f, u))$. The desired natural transformation can be obtained as the composite

$$?\exists u^U !\forall f^{X^U} \psi(u, \mathrm{ev}(f, u)) \xrightarrow{!\rho^{\forall,?} \circ !?\rho^{\exists\forall,\forall\exists} \circ \lambda^{?,!} \circ ?\rho^{\exists,!}} !\forall x^X ?\exists u^U \psi(u, x)$$

- For the axiom 8

$$?!\Phi \otimes ?!\Psi \simeq ?(!\Phi \otimes !\Psi)$$

it is sufficient consider the natural p-isomorphisms

$$(?\exists u^U\ !\varphi(u)) \otimes (?\exists\ v^V !\psi(v)) \quad \simeq \quad ?(\exists u^U\ !\varphi(u) \otimes \exists v^V\ !\psi(v)) \quad \simeq \quad ?\exists (u, v)^{U \times V}\ (!\varphi(u) \otimes !\psi(v))$$

The second half is straightforward to obtain from the Frobenius law. As for the first half, it is a consequence of the isomorphisms

$$\exists u^U\ !\varphi(u) \simeq !\exists u^U\ !\varphi(u) \qquad \exists v^V\ !\psi(v) \simeq !\exists v^V\ !\psi(v)$$

and the following instantiation of axiom 8 in p

$$(?!\exists u^U\ !\varphi(u)) \otimes (?!\exists\ v^V !\psi(v)) \quad \simeq \quad ?(!\exists u^U\ !\varphi(u) \otimes !\exists v^V\ !\psi(v))$$

$$
\begin{array}{rcll}
(\mathtt{t}=\mathtt{t}')^D & := & (\mathtt{t}=\mathtt{t}')_D & := \quad \mathtt{t}=\mathtt{t}' \\
(\varphi\otimes\psi)^D(a) & := & \exists\langle u,v\rangle\forall\langle x,y\rangle.\ (\varphi\otimes\psi)_D(\langle u,v\rangle,\langle x,y\rangle,a) & := \\
 & & & \exists\langle u,v\rangle\forall\langle x,y\rangle.\ \varphi_D(u,x,a)\otimes\psi_D(v,y,a) \\
(\varphi\parr\psi)^D(a) & := & \exists\langle u,v\rangle\forall\langle x,y\rangle.\ (\varphi\parr\psi)_D(\langle u,v\rangle,\langle x,y\rangle,a) & := \\
 & & & \exists\langle u,v\rangle\forall\langle x,y\rangle.\ \varphi_D(u,x,a)\parr\psi_D(v,y,a) \\
(\varphi\multimap\psi)^D(a) & := & \exists\langle f,F\rangle\forall\langle u,y\rangle.\ (\varphi\multimap\psi)_D(\langle f,F\rangle,\langle u,y\rangle,a) & := \\
 & & & \exists\langle f,F\rangle\forall\langle u,y\rangle.\ \varphi_D(u,\mathrm{ev}(F,\langle uy\rangle),a)\multimap\psi_D(\mathrm{ev}(f,u),y,a) \\
(\exists w.\varphi)^D(a) & := & \exists\langle u,w\rangle\forall x.\ (\exists w.\varphi)_D(\langle u,w\rangle,x,a) & := \quad \exists\langle u,w\rangle\forall x.\ \varphi_D(u,x,\langle a,w\rangle) \\
(\forall w.\varphi)^D(a) & := & \exists f\,\forall\langle x,w\rangle.\ (\forall w.\varphi)_D(f,\langle x,w\rangle,a) & := \quad \exists f\,\forall\langle x,w\rangle.\ \varphi_D(\mathrm{ev}(f,w),x,\langle a,w\rangle) \\
(!\varphi)^D(a) & := & \exists u.\ (!\varphi)_D(u,-,a) & := \quad \exists u.\ !\forall x.\ \varphi_D(u,x,a) \\
(?\varphi)^D(a) & := & \forall X.\ (?\varphi)_D(-,X,a) & := \quad \forall X.\ ?\exists u.\ \varphi_D(u,\mathrm{ev}(X,u),a)
\end{array}
$$

Figure 5.1: The Dialectica translation for FOFIMELL (types are left implicit).

- The dual axiom 9 $!(?\Phi \parr ?\Psi) \simeq !?\Phi \parr !?\Psi$ is treated similarly, except that axiom 2 of LSIP muste be used instead of the Frobenius law.

- The validity of all the remaining PEXP axioms in $\mathfrak{Dial}(p)$ is straightforward as they translate almost exactly to their counterparts in p.

□

Definition 5.4.3. *The* MFOLL *predicates of a* FOFIMELL *fibration consist of the following inductively generated family.*

$$\varphi,\psi ::= \mathbf{I} \mid \varphi\otimes\psi \mid \bot \mid \varphi\parr\psi \mid \varphi\multimap\psi \mid \exists a\ \varphi \mid \forall a\ \varphi \mid !\varphi \mid ?\varphi \mid f^*(a\doteq b)$$

Theorem 5.4.4. *A* FOFIMELL *fibration p satisfying* LSIP, LAC *and* DEXP *has, for every* MFOLL *predicate φ, an equivalence.*

$$\varphi(a) \qquad \leftrightarrow \qquad \exists u\ \forall x\ \varphi_D(u,x,a)$$

The proof is going to be a straightforward induction over the syntax, employing the additional axioms we discussed. However, before embarking in the proof of Theorem 5.4.4, we need to prove that the formulas φ_D are well-behaved in the following sense.

Definition 5.4.5. *A predicate φ is called* positive *if there exists a map*

$$!\varphi \quad\longrightarrow\quad \varphi$$

Dually, φ is negative *if there exists a map*

$$?\varphi \quad\longrightarrow\quad \varphi$$

φ is deterministic *if it is both positive and negative.*

Remark. *Definition 5.4.5 is related to the polarity system presented in Definition 4.1.3. Indeed, this system gives a syntactic criterion to classify $\mathfrak{Dial}(p)$ predicate according to Definition 5.4.5:*

$$\Phi = \begin{pmatrix} a:A, u:U, x:X \\ \varphi(a,u,x) \end{pmatrix}$$

- *Φ is positive when $U\simeq 1$ and $\varphi(a,u,x)$ is positive in p.*

- *Φ is negative when $X\simeq 1$ and $\varphi(a,u,x)$ is negative in p.*

- *Φ is deterministic when $U\simeq X\simeq 1$ and $\varphi(a,u,x)$ is deterministic in p.*

Do note that the above item do not necessarily extend to equivalences.

Definition 5.4.6. *Define by recursion the following translations between predicates of first-order logic and first-oder multiplicative exponential linear logic.*

$$\begin{array}{rcl|rcl}
(-)^L : \mathsf{FO} \to \mathsf{FOMELL} & & & \lfloor - \rfloor : \mathsf{FOMELL} \to \mathsf{FO} & & \\
 & & & \lfloor \bot \rfloor & := & \bot \\
\bot^L & := & \bot & \lfloor \mathbf{I} \rfloor & := & \top \\
\top^L & := & \mathbf{I} & \lfloor t = u \rfloor & := & t = u \\
(t = u)^L & := & t = u & \lfloor \varphi \otimes \psi \rfloor & := & \lfloor \varphi \rfloor \wedge \lfloor \psi \rfloor \\
(\varphi \vee \psi)^L & := & \varphi^L \parr \psi^L & \lfloor \varphi \parr \psi \rfloor & := & \lfloor \varphi \rfloor \vee \lfloor \psi \rfloor \\
(\varphi \Rightarrow \psi)^L & := & \varphi^L \multimap \psi^L & \lfloor \varphi \multimap \psi \rfloor & := & \lfloor \varphi \rfloor \Rightarrow \lfloor \psi \rfloor \\
(\varphi \wedge \psi)^L & := & \varphi^L \otimes \psi^L & \lfloor \exists a^A \varphi \rfloor & := & \exists a^A \lfloor \varphi \rfloor \\
(\exists a^A \varphi)^L & := & ?\exists a^A \varphi^L & \lfloor \forall a^A \varphi \rfloor & := & \forall a^A \lfloor \varphi \rfloor \\
(\forall a^A \varphi)^L & := & !\forall a^A \varphi^L & \lfloor !\varphi \rfloor & := & \lfloor \varphi \rfloor \\
 & & & \lfloor ?\varphi \rfloor & := & \lfloor \varphi \rfloor
\end{array}$$

THe following is then asily proven by induction over the syntax of φ.

Lemma 5.4.7. *In a* $\mathsf{FOFIMELL} + \mathsf{PEXP}$ *fibration, for any inductively generated* FO *predicate* φ*,* φ^L *is deterministic.*

Corollary 5.4.8. *For every* MFOLL *predicate* φ *interpreted in a* $\mathsf{FOFIMELL} + \mathsf{PEXP}$ *fibration,* φ_D *is deterministic.*

Proof. We use the fact that $\varphi_D = \lfloor \varphi_D \rfloor^L$, which is easily seen by induction over φ, and the above lemma. □

Proof of Theorem 5.4.4. The proof is by induction over the syntax.

- **Case** $a = b$ In this case, both clauses are syntactically equal.
- **Case** $\varphi(a) \otimes \psi(a)$**:** by the induction hypothesis, it suffices to exhibit an equivalence

  $$\big(\exists u^U \, \forall x^X \, \varphi_D(u,x,a)\big) \otimes \big(\exists v^V \, \forall y^Y \, \psi_D(v,y,a)\big) \qquad \leftrightarrow \qquad \exists (u,v)^{U \times V} \, \forall (x,y)^{X \times Y} \, \varphi_D(u,x,a) \otimes \psi_(v,y,a)$$

  This is true because $\otimes$ commute with $\forall$ by axiom 1 from LSIP. $\otimes$ furthermore commute with $\exists$ using the usual Frobenius law. $\exists x \, (\varphi \otimes \psi) \simeq (\exists x \, \varphi) \otimes \psi$.
- **Case** $\varphi(a) \parr \psi(a)$**:** by the induction hypothesis, it suffices to exhibit an equivalence

  $$\big(\exists u^U \, \forall x^X \, \varphi_D(u,x,a)\big) \parr \big(\exists v^V \, \forall y^Y \, \psi_D(v,y,a)\big) \qquad \leftrightarrow \qquad \exists (u,v)^{U \times V} \, \forall (x,y)^{X \times Y} \, \varphi_D(u,x,a) \otimes \psi_(v,y,a)$$

  This is the dual of $\otimes$, where $\parr$ commutes with $\forall$ and $\exists$ because of the axioms 3 and 2 from LSIP.
- **Case** $\varphi(a) \multimap \psi(a)$**:** by the induction hypothesis, it suffices to construct an equivalence induced by the following string of isomorphisms

  $$\begin{array}{rl}
  \big(\exists u^U \, \forall x^X \, \varphi_D(u,x,a)\big) \multimap \exists v^V \, \forall y^Y \, \psi_D(v,y,a) & \\
  \simeq & \\
  \forall u^U \big((\forall x^X \, \varphi_D(u,x,a)) \multimap \exists v^V \, \forall y^Y \, \psi_D(v,y,a)\big) & \\
  \simeq & \text{By } \mathsf{LSIP}, \text{ 4.} \\
  \forall u^U \exists v^V \big((\forall x^X \, \varphi_D(u,x,a)) \multimap \forall y^Y \, \psi_D(v,y,a))\big) & \\
  \simeq & \text{By } \mathsf{LAC}. \\
  \exists f^{V^U} \forall u^U \big((\forall x^X \, \varphi_D(u,x,a)) \multimap \forall y^Y \, \psi_D(\mathrm{ev}(f,u),y,a))\big) & \\
  \simeq & \\
  \exists f^{V^U} \forall (u,y)^{U \times Y} \big((\forall x^X \, \varphi_D(u,x,a)) \multimap \psi_D(\mathrm{ev}(f,u),y,a))\big) & \\
  \simeq & \text{By } \mathsf{LSIP}, \text{ 5.} \\
  \exists f^{V^U} \forall (u,y)^{U \times Y} \exists x^X \, \varphi_D(u,x,a)) \multimap \psi_D(\mathrm{ev}(f,u),y,a)) & \\
  \simeq & \text{By } \mathsf{LAC}. \\
  \exists (f,F)^{V^U \times X^{U \times Y}} \forall (u,y)^{U \times Y} \exists x^X \, \varphi_D(u,\mathrm{ev}(F,\langle u,y\rangle,a)) \multimap \psi_D(\mathrm{ev}(f,u),y,a)) &
  \end{array}$$
- **Case** $\exists b^B \, \varphi(a,b)$**:** The required equivalence is immediate.
- **Case** $\forall b^B \, \varphi(a,b)$**:** by the induction hypothesis, it suffices to exhibit an equivalence

  $$\forall b^B \exists u^U \, \forall x^X \, \varphi_D(u,x,a,b) \qquad \leftrightarrow \qquad \exists u^{U^B} \, \forall (x,f)^{X \times B} \varphi_D(u,x,a,\mathrm{ev}(f,x))$$

  which is immediate by LAC.

- **Case** $!\varphi(a)$**:** by the induction hypothesis, it suffices to exhibit an equivalence

$$!(\exists u^U\ \forall x^X\ \varphi_D(u,x,a)) \qquad \leftrightarrow \qquad \exists u^U\ !\forall x^X \varphi_D(u,x,a)$$

which is given by axiom 14 from DEXP and Corollary 5.4.8.

- **Case** $?\varphi(a)$**:** by the induction hypothesis, it suffices to exhibit an equivalence

$$?(\exists u^U\ \forall x^X\ \varphi_D(u,x,a)) \qquad \leftrightarrow \qquad \forall f^{X^U}?\exists u^U \varphi_D(u,\mathrm{ev}(f,u),a)$$

which is given by axiom 15 from DEXP and Corollary 5.4.8.

□

Chapter 6

An infinitary Dialectica-based synchronous game model

In this chapter, we consider a variation $\mathfrak{Dial}^{\blacktriangleright}$ of the construction $\mathfrak{Dial}$ over a particular base $\mathbb{S}$ of synchronous functions. Our main goal is to build a model of FIMELL where formulas are interpreted by infinite games whose strategies are representable in $\mathbb{S}$.

In terms of complexity, $\mathbb{S}$ is a full subcategory of the so-called topos of trees sharing its cartesian-closed structure and its guarded fixpoint combinator. This allows to carry out the construction of $\mathfrak{Dial}$ over a base containing Mealy, the category of alphabets and causal functions induced by finite-state transducers, as a subcategory.

6.1 Higher-order synchronous functions

We describe here convenient cartesian-closed extensions of Mealy, which are going to serve as higher-order syntax for richer setting. Our main goal here is to have a cartesian-closed category in which Mealy embeds with a fixpoint operator extending $\mathbf{fix}_b$. The most natural candidate for this extension is the so-called *topos of trees* $\mathbb{T}$, the natural setting to represent arbitrary synchronous functions: objects are infinite trees and morphisms are depth-preserving homomorphisms.

Definition 6.1.1. *Let $\mathbb{N}_{\leq}$ be the preorder category whose objects are natural numbers, and where there is a unique morphism $n \to m$ if and only if $n \leq m$. The topos of finite-branching trees $\mathbb{T}$ is the category of finite presheaves over the category $\mathbb{N}_{\leq}$, that is whose objects are functors $\mathbb{N}_{\leq} \to$ **FinSet** and morphisms natural transformations between them. Unwinding the definition, it may be equivalently described as follows:*

- **Objects:** *sequences $(A_n)_{n\in\mathbb{N}}$ of finite sets and restriction maps $(r_n : A_{n+1} \to A_n)_{n\in\mathbb{N}}$.*
- **Morphisms:** *a morphism from $(A_n)_{n\in\mathbb{N}} \to (B_n)_{n\in\mathbb{N}}$ is a sequence of functions $(f_n : A_n \to B_n)_{n\in\mathbb{N}}$ making all of the following squares commute.*

$$\begin{array}{ccc} A_{n+1} & \xrightarrow{f_{n+1}} & B_{n+1} \\ {\scriptstyle r_n}\downarrow & & \downarrow{\scriptstyle r_n} \\ A_n & \xrightarrow[f_n]{} & B_n \end{array}$$

By convention, for any object A of $\mathbb{T}$ or any relevant subcategory, we take $A_{-n} = 1$ for any $n > 0$; the extended restriction maps r_{-n} are thus uniquely determined.

While $\mathbb{T}$ captures all the desiderata we have put forward so far, one of its drawbacks is that the non-uniform structure of branching means that the possible type of an output of a morphism $f : A \to B$ at step n may depend on the outputs of f at all previous steps. However, we want to model simpler situations with uniform branching. This essentially means restricting to objects A of $\mathbb{T}$, such that, for every n

$$\forall a, a' \in A_n \; r_n^{-1}(\{a\}) \simeq r_n^{-1}(\{a'\})$$

A convenient way to make this restriction is to consider the simpler category of sequences of sets and maps.

Definition 6.1.2. *Call $\widehat{\mathbb{N}}$ the category of presheaves over the discrete category $\mathbb{N}$:*

- **Objects:** *sequences $(A_n)_{n\in\mathbb{N}}$ of finite sets.*
- **Morphisms:** *a morphism $(A_n)_{n\in\mathbb{N}} \to (B_n)_{n\in\mathbb{N}}$ is a sequence of functions $(f_n : A_n \to B_n)_{n\in\mathbb{N}}$.*

There is an obvious forgetful functor $U : \widehat{\mathbb{N}} \to \mathbb{T}$ erasing the restriction maps. When $\widehat{\mathbb{N}}$ and $\mathbb{T}$ are seen as presheaves categories, this correspond to precomposing with the inclusion functor $\mathbb{N} \to \mathbb{N}_{\leq}$.

$$\begin{array}{rlcl} U: & \mathbb{T} & \to & \widehat{\mathbb{N}} \\ & (A_n)_{n\in\mathbb{N}}, (r_n^A)_{n\in\mathbb{N}} & \mapsto & (A_n)_{n\in\mathbb{N}} \\ & (f_n)_{n\in\mathbb{N}} & \mapsto & (f_n)_{n\in\mathbb{N}} \end{array}$$

This functor has a right adjoint R. Abstractly, for an object A of $\widehat{\mathbb{N}}$, $R(A)$ is the right Kan extension along the aforementioned inclusion $\mathbb{N} \to \mathbb{N}_{\leq}$. More concretely, R is computed as follows.

$$\begin{array}{rlcl} R: & \widehat{\mathbb{N}} & \to & \mathbb{T} \\ & (A_n)_{n\in\mathbb{N}} & \mapsto & (\prod_{i\leq n} A_i)_{n\in\mathbb{N}}, (\pi_1 : \prod_{i\leq n+1} A_i \to \prod_{i\leq n} A_i)_{n\in\mathbb{N}} \\ & (f_n)_{n\in\mathbb{N}} & \mapsto & (\langle f_0, \ldots, f_n\rangle)_{n\in\mathbb{N}} \end{array}$$

We define $\mathbb{S}$ to be (isomorphic to) the full subcategory of $\mathbb{T}$ whose objects are of the form $R(A)$.

Definition 6.1.3. *The category of uniform trees and synchronous functions $\mathbb{S}$ is defined as follows.*

- **Objects:** *sequences of finite sets $(A_n)_{n\in\mathbb{N}}$*
- **Morphisms:** *a morphism from $A = (A_n)_{n\in\mathbb{N}}$ to $A = (B_n)_{n\in\mathbb{N}}$ is a family*

$$f \quad = \quad \left(f_n : \prod_{i\leq n} A_i \longrightarrow B_n \right)_{n\in\mathbb{N}}$$

- **Composition:** *given morphisms $f : A \to B$ and $g : B \to C$, $g \circ f$ is defined as*

$$(g \circ f)_n(a_0, \ldots, a_n) = g_n(f_0(a_0), f_1(a_0, a_1), \ldots, f_n(a_0, \ldots, a_n))$$

By abuse of notation, we shall regard $\mathbb{S}$ as a full subcategory of $\mathbb{T}$.

The embedding functor $M : \mathsf{Mealy} \to \mathbb{S}$ can be straightforwardly defined: at the level of objects, which are those of **FinSet**, M obtained by composing R with the constant functor $\Delta : \mathbf{FinSet} \to \mathbf{FinSet}^{\mathbb{N}^{\mathrm{op}}} = \widehat{N}$. Concretely, it means that an alphabet Σ is mapped to the sequence $(\Sigma^n)_{n\in\mathbb{N}}$, with projections $r_n : \Sigma^{n+1} \cong \Sigma^n \times \Sigma \to \Sigma^n$ as restriction maps. Then the homsets $[R(\Delta(\Sigma)), R(\Delta(\Gamma))]_{\mathbb{T}}$ are isomorphic to the sets of (not necessarily finite-state!) causal functions $\Sigma^\omega \to \Gamma^\omega$. The point of allowing more causal functions and objects is mostly to overcome the lack of cartesian-closure in Mealy (Proposition 2.1.5).

Lemma 6.1.4. *$\mathbb{S}$ is a cartesian closed category. The cartesian structure is defined pointwise as $(A \times B)_n = A_n \times B_n$ with the obvious projections. The exponentials are inherited from $\mathbb{T}$:*

$$(A \to B)_n = (\prod_{i\leq n} A_i) \to B_n \qquad \mathrm{ev}_n(\langle f_0, a_0\rangle \ldots \langle f_n, a_n\rangle) = f_n(a_0 \ldots a_n)$$

Proof. Since R is a right adjoint, $\mathbb{S}$ is an exponential ideal in $\mathbb{T}$ and inherits all finite limits; for our purpose, it is sufficient to notice that $\widehat{\mathbb{N}}, \mathbb{S}$ and $\mathbb{T}$ all share the same cartesian structure, which happens to be preserved by U, R and Δ and to discuss the cartesian closed-structure of $\mathbb{S}$. □

$\mathbb{S}$ also has a *guarded fixpoint theorem*. This is a well-known feature of $\mathbb{T}$, widely used to model step-indexing. As $\mathbb{S}$ is a full subcategory of $\mathbb{T}$ (and has enough objects), this theorem readily holds there. To state the theorem, we first need to consider the endofunctor $\blacktriangleright : \mathbb{T} \to \mathbb{T}$ acting on objects by "delaying" the sequence family under consideration by one time step. Concretely, it is defined as follows on objects

$$\begin{array}{rlcl} \blacktriangleright: & \mathbb{S} & \longrightarrow & \mathbb{S} \\ & A & \mapsto & \begin{array}{lcl} 0 & \mapsto & 1 \\ n+1 & \mapsto & A_n \end{array} \end{array}$$

The second ingredient needed to state the fixpoint theorem is the natural transformation $\mathrm{next}_A : A \to \blacktriangleright A$ which accordingly sends an input sequence to the same sequence delayed by one time step.

$$\begin{array}{rccc} (\mathrm{next}_A)_0 : & A_0 & \longrightarrow & 1 \\ & a_0 & \mapsto & * \end{array}$$

$$\begin{array}{rccc} (\mathrm{next}_A)_{n+1} : & \prod_{k\leq(n+1)} A_k & \longrightarrow & A_n \\ & (a_0,\dots,a_n,a_{n+1}) & \mapsto & a_n \end{array}$$

At this point, it is possible to define a *fixpoint combinator* $\mathbf{fix}_A : A^{\blacktriangleright A} \to A$ as follows

$$\begin{array}{rccc} (\mathbf{fix}_A)_0 : & (1 \to A_0) & \longrightarrow & A_0 \\ & f_0 & \mapsto & f_0(*) \end{array}$$

$$\begin{array}{rccc} (\mathbf{fix}_A)_{n+1} : & \prod_{k\leq(n+1)}(\prod_{i\leq k}(\blacktriangleright A)_i \to A_k) & \longrightarrow & A_{n+1} \\ & f_0 \dots f_n f_{n+1} & \mapsto & f_{n+1}((\mathbf{fix}_A)_n(f_0 \dots f_n)) \end{array}$$

The definition is rather technical and relies on the explicit description of the $\mathbf{fix}_A$ morphism. It is also possible to give the following implicit characterization.

Lemma 6.1.5. *$\mathbf{fix}_A$ is the unique morphism $h : A^{\blacktriangleright A} \to A$ such that, for every $f : U \to A^{\blacktriangleright A}$, we have* $\mathrm{ev} \circ \langle f, h \circ f\rangle = h \circ f$

Using the cartesian-closed structure of $\mathbb{S}$, it is possible to derive a parametric version of the theorem which is more useful in practice.

Corollary 6.1.6. *For every $f : A\times \blacktriangleright B \to B$, there exists a unique morphism*

$$\mathbf{fix}(f) : A \to B$$

such that

$$\mathbf{fix}(f) = f \circ \langle \mathrm{id}, \mathrm{next} \circ \mathbf{fix}(f)\rangle$$

Remark. *Note that the statement itself does not refer to the exponential structure of $\mathbb{S}$. In fact, an analogous version of this theorem hold for the category* Mealy *under the guise of Lemma 2.1.6; this connection will be used to adapt techniques used in this chapter to* FOM*.*

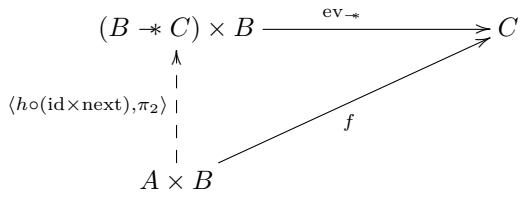
Definition 6.1.7. *Let A and B be objects of $\mathbb{S}$. Call a $\mathbb{S}$ morphism $f : A \to B$* pointwise *if it is some $R(g)$ for some g in $\widehat{\mathbb{N}}$. Write $A \multimap B$ for the exponential in $\widehat{\mathbb{N}}$ (which is defined pointwise, e.g. $(A \multimap B)_n = B_n^{A_n}$), while reserving B^A for genuine exponentials in $\mathbb{S}$. We call $A \multimap B$ the* pointwise *exponential in $\mathbb{S}$.*

Remark. *$- \multimap -$ is defined on all objects of $\mathbb{S}$, but this does not extend to morphisms: $- \multimap -$ is* not *a functor $\mathbb{S}^{\mathrm{op}} \times \mathbb{S} \to \mathbb{S}$. It can however be seen as the restriction of a suitable functor $\widehat{\mathbb{N}}^{\mathrm{op}} \times \mathbb{T} \to \mathbb{T}$.*

This pointwise exponential is going to be an essential ingredient when considering monoidal closure and simple products in fibrations $\mathfrak{Dial}^{\blacktriangleright}(p)$ and constitutes the only reason why we consider $\mathbb{S}$ instead of $\mathbb{T}$. This forces us to give up on plenty of objects of $\mathbb{T}$, such as the subojbect classifier. While this is not problematic in the scope of this thesis, let us point out that it is likely that this may be remedied by considering games with possibly non-uniform branching (i.e. which depend on past moves) and a suitable generalization of our development. This would roughly correspond to moving from Dialectica fibrations as discussed here to the more expressive Dialectica fibrations as investigated in [51], albeit with more technicality since we are dealing with infinite games rather than "two-move games".

Pointwise exponentials come equipped with a similar structure, although not natural in $\mathcal{S}$. We write $\mathrm{ev}_{\multimap} : (A \multimap B) \times A \to B$ for the pointwise evaluation map $R(\mathrm{ev})$ induced by the exponential structure in $\widehat{\mathbb{N}}$.

Lemma 6.1.8. *Let A, B and C be objects of $\mathbb{S}$ and f an arbitrary $\mathbb{S}$-morphism $A \times B \to C$. There exists a unique morphism $h : A\times \blacktriangleright B \to B \multimap C$ making the following diagram commute.*



We write $\Lambda_{-*}(f)$ for h in the sequel.

Proof. Let h^1, h^2 be morphisms such that the above commute. For positive n, the commuting diagram means that we should have, for every sequences $(a_k, b_k)_{k\leq n}$,

$$h^i_n((a_k, b_{k-1})_{k\leq n})(b_n) = f_n((a_k, b_k)_{k\leq n})$$

Since the sequence $(a_k, b_{k-1})_{k\leq n}$ and b_n are arbitrary, this means $h^1_n = h^2_n$; furthermore, this constitutes a valid definition of h. □

Lemma 6.1.9. *There exists a $\mathbb{S}$-isomorphism*

$$B^A \simeq (A \multimap B)^{\blacktriangleright A}$$

Proof. Unfolding the definitions, the components of the (pointwise) bijection is obtained from the following **FinSet**-isomorphisms.

$$(B^A)_n = B_n^{\prod_{k\leq n} A_k} \simeq B_n^{A_n \times \prod_{k<n} A_k} \simeq (B_n^{A_n})^{\prod_{k<n} A_k} = \left((A \multimap B)^{\blacktriangleright A}\right)_n$$

□

All the structure we gave so far on $\mathbb{S}$ amount to the typed syntax presented in Figure 7.1. Contrary to the analogue for finite-state synchronous functions, this syntax does not capture *every* object and morphism in $\mathbb{S}$. However, it does capture all the construction that we will use in the sequel to interpret our infinitary game model.

6.2 The $\mathfrak{Dial}^{\blacktriangleright}$ construction

We now discuss the variant of the $\mathfrak{Dial}$ construction modelling infinite two-player games for fibrations over the base $\mathbb{S}$. Intuitively, for a classical posetal fibration p, $\mathfrak{Dial}(p)$ embodies a notion of proof corresponding to two-moves games: in the object $(a : A, u : U, x : X, \varphi(a, u, x))$, first the existential player provides a witness u and then an opponent attempts to provide a counter-witness x. The predicate $\varphi(a, u, x)$, an object of p, is then a winning condition for this two-moves games. As $\mathbb{S}$ is cartesian-closed, this construction can be carried out for fibration over $\mathbb{S}$. However the resulting proofs do *not* correspond to strategies for games of infinite durations. In this section, we present a construction $\mathfrak{Dial}^{\blacktriangleright} : \mathfrak{Fib}(\mathbb{S}) \to \mathfrak{Fib}(\mathbb{S})$ which takes a fibration p, which should be regarded as a logical language over $\mathbb{S}$, to another fibration in which formulas are interpreted as infinite games. We then show that, a FOFIMELL-fibration (p^+, p, p^-) can be lifted to a FOFIMELL-fibration $(\mathfrak{Sum}(p^+), \mathfrak{Dial}^{\blacktriangleright}(p), \mathfrak{Prod}(p^-))$. The definitions are very similar to those involved in Theorem 6.2.15, which give a similar lifting for $\mathfrak{Dial}(p)$, aside from the following two points:

- The pointwise exponential $A \multimap B$ is used instead of the genuine exponential of $\mathbb{S}$ when defining the propositional structure of $\mathfrak{Dial}^{\blacktriangleright}$.
- Both exponentials are defined using the genuine exponential of $\mathbb{S}$; the definition of ? changes significantly.

Although the informal connexions between $\mathfrak{Dial}$ and $\mathfrak{Dial}^{\blacktriangleright}$ are a useful guideline to study the proof theory of the latter, the formal link we have is thus rather weak where simple quantification and monoidal closure are concerned.

Before giving a full description of $\mathfrak{Dial}^{\blacktriangleright}$ construction, we first describe the dynamics of our game model in the simple case where we have no indexing and no winning conditions. This will yield a category of *zigzag games* modelling FIMELL. Then we shall describe how to extend this category to a fibration over $\mathbb{S}$ by considering indexed zigzag games. $\mathfrak{Dial}^{\blacktriangleright}(p)$ as coming from a pseudofunctor $\mathbb{S}^{\mathrm{op}} \to \mathfrak{Cat}$. This construction is an adaptation heavily inspired from the construction of the fibration of tree automata from [61].

6.2.1 Zigzag games

A *zigzag game* is going to be a pair of objects (U, X) of $\mathbb{S}$. This pair of object is intended to model an infinite duration game between two players, proponent (P) and opponent (O). At round n, the interaction goes as follows:

- P plays an element $u_n \in U_n$.

- Then, O plays an element $x_n \in X_n$.

When dealing with such games, we are in fact only interested in total, deterministic P-strategies. Here, such a strategy is readily given by a $\mathbb{S}$-morphism $\blacktriangleright X \to U$.

Zigzag games are arranged in a category DZ, whose morphisms are designed to reflect this behaviour. Letting (U, X) and (V, Y) be two zigzag games, consider the *simulation game* $(U, X) \to (V, Y)$ defined as follows at round n:

- O plays an element $u_n \in U_n$ in the left-hand-side.
- P plays an element $v_n \in V_n$ in the right-hand side.
- O answers with an element $y_n \in Y_n$ in the right-hand side.
- P concludes the round with an element $x_n \in X_n$ in the left-hand side.

	$(U\ ,\ X)$	$\longrightarrow$	$(V,\ Y)$
	$\vdots$		
O	u_n		
P			v_n
O			y_n
P	x_n		
	$\vdots$		

Formally speaking, such a strategy may be seen as pair (f, F) of $\mathbb{S}$-morphisms, with

$$f : U \times \blacktriangleright X \to V \qquad \text{and} \qquad F : U \times X \to Y$$

A morphism from (U, X) to (V, Y) in the category DZ is a P-strategy in the simulation game. The identity are going to be given by a copycat strategy, where P systematically imitates O's last move.

	$(U\ ,\ X)$	$\longrightarrow$	$(U,\ X)$	:	A
	$\vdots$				
O	u_n				a_n
P			u_n		
O				x_n	
P	x_n				
	$\vdots$				

The composition of two strategies $(f, F) : (U, X) \to (V, Y)$ and $(g, G) : (V, Y) \to (W, Z)$ is informally given by P simulating a play over the three games (U, X), (V, Y) and (W, Z), keeping the current state of the play in the middle game (V, Y) as additional internal memory.

	$(U\ ,\ X)$	$\longrightarrow$	$(V,\ Y)$	$\longrightarrow$	$(W,\ Z)$
	$\vdots$				
O	u_n				
			v_n		
P					w_n
O					z_n
			y_n		
O	x_n				
	$\vdots$				

While this description is nice as it captures *exactly* what is a P strategy in a concise way, it is helpful to see P-strategies as a set of possible plays of P, that is, a subset $S \subseteq [1, (U \times X) \times (V \times Y)]_{\mathbb{S}}$. This correspondence will turn out to yield a faithful functor $\mathsf{HS} : \mathsf{DZ} \to \mathbf{Rel}$, which is in turn going to determine how composition is carried out in DZ. In fact, this is how we are going to deduce associativity of composition in DZ from the associativity of composition in **Rel**. This follows the approach taken for simple games by Hyland and Schalk in [35] (hence the denomination HS) for *simple games*[1]

[1]Note that, formally speaking, zigzag games are particular kind of simple games. The crucial difference is that zigzag strategies are much more rigid (P cannot freely pick in which component they play in zigzag strategies). At the end of day, it means that the associativity of composition in DZ is a simpler particular case of associativity of composition of P-strategies in simple games.

Definition 6.2.1. *The category* DZ *is defined as follows:*

- **Objects:** *pairs* (U, X) *of* $\mathbb{S}$*-objects.*
- **Morphisms:** *a morphism* $(U, X) \to (V, Y)$ *is a* P*-strategy* (f, F) *with*

$$f : U \times \blacktriangleright Y \to V \qquad \text{and} \qquad F : U \times Y \to X$$

Furthermore, there exists a faithful functor $\mathsf{HS} : \mathsf{DZ} \to \mathbf{Rel}$ *which completely determines composition in* DZ*. On objects* $\mathsf{HS}(U, X) = (U \times X)^* + ((U \times X)^* \times U)$ *and, for morphisms* $(f, F) : (U, X) \to (V, Y)$*,* $\mathsf{HS}(f, F)$ *is the least set closed under the following clauses (writing pairs vertically and with* $k \geq -1$*):*

- *for every* $(u_i)_{i=0}^k \in \prod_{i=0}^k U_i$*,* $(v_i)_{i=0}^k \in \prod_{i=0}^k V_i$*,* $(x_i)_{i=0}^k \in \prod_{i=0}^k X_i$ *and* $(y_i)_{i=0}^k \in \prod_{i=0}^k Y_i$*, if*

$$\begin{pmatrix} \mathsf{inl}((u_0, x_0) \dots (u_k, x_k)) \\ \mathsf{inl}((v_0, y_0) \dots (v_k, y_k)) \end{pmatrix} \in \mathsf{HS}(f, F)$$

  then, for every $u_{k+1} \in U_{k+1}$*, we have*

$$\begin{pmatrix} \mathsf{inr}((u_0, x_0) \dots (u_k, x_k), u_{k+1}) \\ \mathsf{inr}((v_0, y_0) \dots (v_k, y_k)), f_k((u_0, *), (u_1, y_0) \dots (u_{k+1}, y_k)) \end{pmatrix} \in \mathsf{HS}(f, F)$$

- *for every* $(u_i)_{i=0}^k \in \prod_{i=0}^k U_i$*,* $(v_i)_{i=0}^k \in \prod_{i=0}^k V_i$*,* $(x_i)_{i=0}^k \in \prod_{i=0}^k X_i$ *and* $(y_i)_{i=0}^k \in \prod_{i=0}^k Y_i$*, if*

$$\begin{pmatrix} \mathsf{inr}((u_0, x_0) \dots (u_k, x_k), u_{k+1}) \\ \mathsf{inr}((v_1, y_1) \dots (v_k, y_k), v_{k+1})) \end{pmatrix} \in \mathsf{HS}(f, F)$$

  then, for every $y_{k+1} \in Y_{k+1}$*, we have*

$$\begin{pmatrix} \mathsf{inl}((u_0, x_0) \dots (u_k, x_k), (u_{k+1}, F_{k+1}((u_0, y_0), \dots, (u_{k+1}, y_{k+1})))) \\ \mathsf{inl}((v_0, y_0) \dots (v_k, y_k)(v_{k+1}, y_{k+1})) \end{pmatrix} \in \mathsf{HS}(f, F)$$

Proof. First, note that HS is injective on morphisms. Let $(f, F) : (U, X) \to (V, Y)$ and $(g, G) : (V, Y) \to (W, Z)$ be DZ-morphisms. We then need to show that a composition may be carried out in DZ such that

$$\mathsf{HS}((g, G) \circ (f, F)) = \mathsf{HS}(g, G) \circ \mathsf{HS}(f, F)$$

Together with injectivity of HS, this will imply associativity of this newly-defined composition from the associativity of composition in $\mathbf{Rel}$. Call (h, H) the would-be composite $(g, G) \circ (f, F)$. We may show that the above equation amounts that, for every global elements u, x, w and z, we have

$$\begin{gathered} \exists v, y \quad v = f(\langle u, \mathrm{next}(y) \rangle) \wedge x = F(\langle u, y \rangle) \wedge w = g(\langle v, \mathrm{next}(z) \rangle) \wedge y = G(\langle v, z \rangle) \\ \Leftrightarrow \\ w = h(\langle u, \mathrm{next}(z) \rangle) \wedge x = H(\langle u, z \rangle) \end{gathered}$$

Substituting equalities, note that the top proposition is true if and only if

$$y \quad = \quad G(\langle f(\langle u, \mathrm{next}(y) \rangle), z \rangle)$$

By Lemma 6.1.5, this means that there is a unique auxiliary map $h' : U \times Z \to Y$ such that $h'(\langle u, z \rangle) = y$ for every u, v. Then, the above equivalence means that we necessarily have

$$h(\langle u, \mathrm{next}(z) \rangle) = g(f(\langle u, \mathrm{next}(h'(\langle u, z \rangle)) \rangle)) \qquad \text{and} \qquad H(\langle u, z \rangle) = F(\langle u, h'(\langle u, z \rangle) \rangle)$$

which may be taken as definition of h and H from h' and basic cartesian combinators. □

We then equip DZ with a monoidal product. Here we diverge from the usual practice in game semantics and take this product to be synchronous rather than asynchronous. The reason for this choice is that we are more interested in products of automata reminiscent of Dialectica, rather than trying to model the fine-grained behaviour of general purpose programming languages.

Definition 6.2.2. *The category* DZ *is equipped with a symmetric monoidal product* $(\otimes, \mathbf{I})$*. The bifunctor* $\otimes$ *is defined as follows*

$$\begin{array}{rcccl} (U, X) & , & (V, Y) & \mapsto & (U \times V, X \times Y) \\ (f, F) & , & (g, G) & \mapsto & \begin{pmatrix} \langle f \circ \langle \pi_1 \circ \pi_1, \blacktriangleright (\pi_1 \circ \pi_2) \rangle, g \circ \langle \pi_2 \circ \pi_1, \blacktriangleright (\pi_2 \circ \pi_2) \rangle \rangle \\ \langle F \circ \langle \pi_1 \circ \pi_1, \pi_1 \circ \pi_2 \rangle, G \circ \langle \pi_2 \circ \pi_1, \pi_2 \circ \pi_2 \rangle \rangle \end{pmatrix} \end{array}$$

and the unit is $\mathbf{I} = (1, 1)$*.*

Note that this choice of unit means that a P-strategy in the simulation game $\mathbf{I} \to (U, X)$ are in bijective correspondence with P-strategies $s : U^{\blacktriangleright X}$ in the game (U, X).

This choice of monoidal product gives rise to a monoidal closed structure over DZ; let us sketch why that is on an intuitive level before formally proving it. Considering two zigzag games (U, X) and (V, Y), a P-strategy in the simulation game $(U, X) \to (V, Y)$ is a pair

$$f : U \times \blacktriangleright Y \to V \qquad\qquad F : U \times Y \to X$$

Using the natural isomorphism $A^B \cong (B \multimap A)^{\blacktriangleright B}$ in $\mathbb{S}$ and the fact that $\blacktriangleright$ preserves cartesian products, those are in bijective correspondence with pairs

$$\blacktriangleright (U \times Y) \to U \multimap V \qquad\qquad \blacktriangleright (U \times Y) \to (U \times Y) \multimap X$$

and thus, by pairing, these correspond to a single morphisms

$$\blacktriangleright (U \times Y) \to (U \multimap V) \times (U \times Y \multimap X)$$

i.e., P-strategies in the game $((U \multimap V) \times (U \times Y \multimap X), U \times Y)$. This game shall thus be the object part of our monoidal closure.

Lemma 6.2.3. *The category* $(\mathsf{DZ}, \otimes, \mathbf{I})$ *is monoidal closed.*

Proof. As sketched above, we set

$$(U, X) \multimap (V, Y) \quad := \quad ((U \times Y \multimap V) \times (Y \multimap X), U \times Y)$$

The evaluation map $\mathrm{ev}_{(U,X),(V,Y)} : ((U, X) \multimap (V, Y)) \otimes (U, X) \to (V, Y)$ is thus as a pair of $\mathbb{S}$-morphisms

$$\begin{array}{rrcl} \mathrm{ev}^0_{(U,X),(V,Y)} : & (((U \multimap V) \times (U \times Y \multimap X)) \times U) \times \blacktriangleright Y & \to & V \\ \mathrm{ev}^1_{(U,X),(V,Y)} : & (((U \multimap V) \times (U \times Y \multimap X)) \times U) \times Y & \to & X \end{array}$$

These morphisms are actually pointwise; those two components are obtained respectively as the image of

$$\begin{array}{rcl} (((U \multimap V) \times (U \times Y \multimap X)) \times U) \times \blacktriangleright Y & \to & V \\ (((f_n, F_n), u_n), y_n) & \mapsto & f_n(u_n) \\ (((U \multimap V) \times (U \times Y \multimap X)) \times U) \times Y & \to & X \\ (((f_n, F_n), u_n), y_n) & \mapsto & F_n(u_n, y_n) \end{array}$$

by the inclusion functor $\mathbf{FinSet}^{\mathbb{N}^{\mathrm{op}}} \to \mathbb{S}$. Using the basic combinators we introduced for $\mathbb{S}$, this amounts to setting

$$\begin{array}{rcl} \mathrm{ev}^0 & = & \mathrm{ev}_{\multimap} \circ \langle \pi_1 \circ \pi_1 \circ \pi_1, \pi_2 \circ \pi_1 \rangle \\ \mathrm{ev}^1 & = & \mathrm{ev}_{\multimap} \circ \langle \pi_2 \circ \pi_1 \circ \pi_1, \langle \pi_2 \circ \pi_1, \pi_2 \rangle \rangle \end{array}$$

It remains to be checked that, for every triple of zigzag games (U, X), (V, Y) and (W, Z), there exists a unique map $\Lambda(F, f)$ making the following diagram commute.

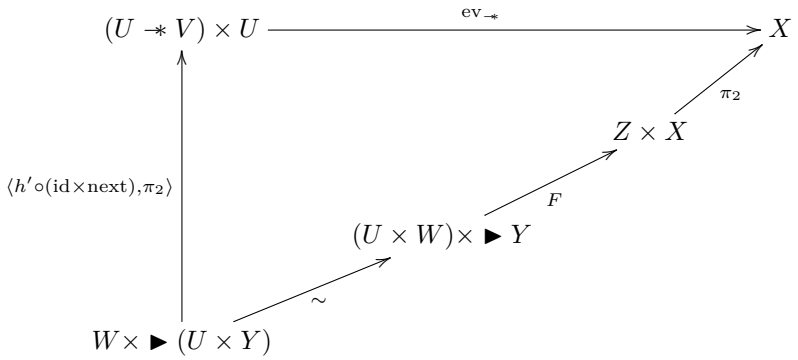
$$\begin{array}{ccc} ((U, X) \multimap (V, Y)) \otimes (U, X) & \xrightarrow{\mathrm{ev}} & (V, Y) \\ {\scriptstyle \Lambda(F,f) \otimes \mathrm{id}} \uparrow & \nearrow_{F,f} & \\ (W, Z) \otimes (U, X) & & \end{array}$$

This amounts to showing that there exists a unique triple of $\mathbb{S}$-maps

$$\begin{array}{rrcl} h : & (W \times \blacktriangleright Y) \times \blacktriangleright U & \to & U \multimap V \\ h' : & W \times \blacktriangleright (U \times Y) & \to & U \times Y \multimap X \\ H : & W \times (U \times Y) & \to & Z \end{array}$$

such that the following diagrams commute

$$\begin{array}{ccc} (U \multimap V) \times U & \xrightarrow{\mathrm{ev}_{\multimap}} & V \\ {\scriptstyle \langle h \circ (\mathrm{id} \times \mathrm{next}), \pi_2 \rangle} \uparrow & \nearrow_{f} & \\ (W \times \blacktriangleright Y) \times U & \xrightarrow{\sim} & (U \times W) \times \blacktriangleright Y \end{array}$$



and $H = \pi_1 \circ F$. H is uniquely determined and by Lemma 6.1.8, so are h and h'. □

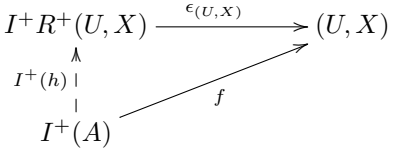
At this point, we have equipped DZ with enough structure to interpret multiplicative intuitionistic linear logic. Now, let us show that DZ has an exponential. As before, we are going to obtain a ! through a LNL adjunction. To this end, note that there is an inclusion functor $I^+ : \mathbb{S} \to \mathsf{DZ}$ defined as follows

$$\begin{array}{rccc} I^+ : & \mathbb{S} & \to & \mathsf{DZ} \\ & A & \mapsto & (A, 1) \\ & f : A \to B & \mapsto & (f \circ \pi_1, !) : (A, 1) \to (B, 1) \end{array}$$

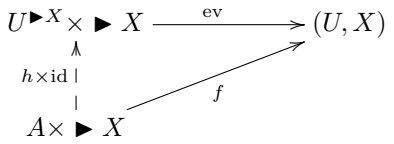
Lemma 6.2.4. *The functor I^+ is part of an LNL-adjunction. Its right adjoint $R^+ : \mathsf{DZ} \to \mathbb{S}$ is defined as follows on objects.*

$$\begin{array}{rccc} R^+ : & \mathsf{DZ} & \to & \mathbb{S} \\ & (U, X) & \mapsto & U^{\blacktriangleright X} \end{array}$$

Proof. R^+ being defined on objects, in order to show that it extends to a functor In order to show that this adjunction exists, it suffices to provide, for every object (U, X) of DZ a counit map $\epsilon_{(U,X)} : I^+(R^+(U, X)) \to (U, X)$ such that, for every map $f : I^+(A) \to (U, X)$, there exists a unique $h : A \to R^+(U, X)$ making the following diagram commute



Define the first component of $\epsilon_{(U,X)}$ to be the evaluation map of $\mathbb{S}$ $\mathrm{ev} : U^{\blacktriangleright X} \times \blacktriangleright X \to U$. Note that the second component of every arrow of this diagram is necessarily trivial



This is exactly the diagram witnessing that $U^{\blacktriangleright X}$ is an internal hom in $\mathbb{S}$; h is thus uniquely determined to be the curryfication $\Lambda(f)$.

It is rather clear that I^+ is strong monoidal, as

$$I^+(A \times B) = (A \times B, 1) \cong (A \times B, 1 \times 1) = I^+(A) \otimes I^+(B)$$

and the unit is preserved on the nose. Thus, by Lemma 5.1.7, I^+ is part of an LNL-adjunction. □

Now that we have enough structure to interpret IMELL, we can go a bit further and show that we may interpret full intuitionistic linear logic with both exponential modalities. First, as per Remark 5.1, we identify our two monoidal structures to $\otimes$. Then, we note that there is also a contravariant functor.

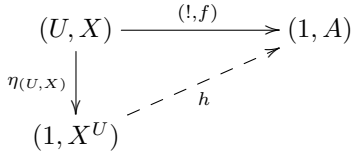
$$\begin{array}{rccc} I^- : & \mathbb{S}^{\mathrm{op}} & \to & \mathsf{DZ} \\ & A & \mapsto & (1, A) \\ & f : A \to B & \mapsto & (!, f \circ \pi_2) : (1, A) \to (1, B) \end{array}$$

Unsurprisingly, it turns out that I^- is strong monoidal and has a left adjoint R^-.

Lemma 6.2.5. *The functor I^- is part of an oplax symmetric monoidal adjunction. Its left adjoint $R^- : \mathsf{DZ} \to \mathbb{S}^{\mathrm{op}}$ is defined as follows on objects.*

$$\begin{array}{rccc} R^- : & \mathsf{DZ} & \to & \mathbb{S}^{\mathrm{op}} \\ & (U, X) & \mapsto & X^U \end{array}$$

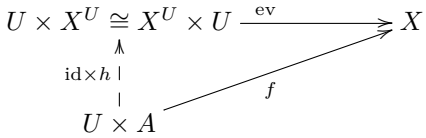
Proof. The proof is analogous to the proof of Lemma 6.2.4. To show that R^- extends to a left adjoint to I^-, it suffices to exhibit for every object (U, X) a morphism $\eta_{(U,X)} : (U, X) \to (1, X^U)$ such that, for every $(!, f) : (U, X) \to (1, A)$ in DZ, there exists a unique h making the following diagram commute



Note that the first components of the above morphisms are all trivial. Define the second component of $\eta_{(U,X)}$ to be the transpose of the evaluation map of $\mathbb{S}$

$$\eta_{(U,X)} = \mathrm{ev} \circ \langle \pi_2, \pi_1 \rangle : U \times X^U \to U$$

. Unfolding the definition in $\mathbb{S}$, it means that there should be a unique h making the following diagram commute.



This is immediate from the cartesian-closed structure of $\mathbb{S}$. □

Theorem 6.2.6. DZ *is equipped with a* FIMELL *structure.*

Proof. Consider all the structure described so far and set $! = R^+ \circ I^+$ and $? = R^- \circ I^-$. To conclude, it remains to show that we have natural transformations

$$I^+(U) \otimes ?(V, Y) \;\to\; ?(I^+(U) \otimes (V, Y)) \qquad \text{and} \qquad !((U, X) \otimes I^-(Y)) \;\to\; !(U, X) \otimes I^-(Y)$$

Unwinding the definitions and suppressing obvious isomorphisms $A \times 1 \cong A$, it means providing DZ-maps

$$(U, Y^V) \to (1, Y^{U \times V}) \qquad \text{and} \qquad (U^{\blacktriangleright(X \times Y)}, 1) \to (U^{\blacktriangleright X}, Y)$$

Suppressing the trivial component, it amounts to providing $\mathbb{S}$-morphisms

$$U \times Y^{U \times V} \to Y^V \qquad \text{and} \qquad U^{\blacktriangleright(X \times Y)} \times \blacktriangleright Y \to U^{\blacktriangleright X}$$

which are given by partial evaluation. □

6.2.2 The $\mathfrak{Dial}^{\blacktriangleright}$ construction

We now explore how to build $\mathsf{FOFIMELL}$-fibrations over $\mathbb{S}$ from zigzag games. While our ultimate goal is to start from an arbitrary fibration p over $\mathbb{S}$ and "enrich it" with computational content, it is useful to consider what happens for the trivial fibration $\mathrm{id} : \mathbb{S} \to \mathbb{S}$. It turns out that $\mathfrak{Dial}^{\blacktriangleright}(\mathrm{id})$ may be obtained by a generic construction applied to DZ: the *comonoid indexing*. The basic idea is that one may build a generalization of the simple fibration for monoidal categories $(\mathbb{L}, \otimes, \mathbf{I})$ on objects which carry a comonoid structure. The important point is that the comonoid structure captures the part of the cartesian structure which is required, that is, comonoids. This generalized construction thus requires a monoidal functor $(\mathbb{C}, \times, 1) \to (\mathbb{L}, \otimes, \mathbf{I})$, making such a choice of comonoids, as input.

Construction 6.2.7. *Let $L : (\mathbb{C}, \times, 1) \to (\mathbb{L}, \otimes, \mathbf{I})$ be a strong monoidal functor. There is a split fibration $\overline{L} : \mathbb{C}^{\mathrm{op}} \to \mathfrak{Cat}$ obtained as follows:*

- **Objects:** *if A is an object of $\mathbb{C}$, the category $\overline{L}(A)$ consists of:*
  - **Objects:** *an object X of $\mathbb{C}$*

– **Morphisms:** *a morphism $f : X \to Y$ in $\overline{L}(A)$ is a map $L(A) \otimes X \to Y$ in $\mathbb{L}$. Note that since $\mathbb{C}$ is cartesian, there is an induced map $\overline{f} : L(A) \otimes X \to L(A) \otimes Y$ defined as follows:*

$$L(A) \otimes X \longrightarrow L(A \times A) \otimes X \longrightarrow L(A) \otimes (L(A) \otimes X) \xrightarrow{\mathrm{id} \otimes f} L(A) \otimes Y$$

– **Composition:** *given morphisms $f : L(A) \otimes X \to Y$ and $g : L(A) \otimes Y \to Z$, the composite is defined as $g \circ \overline{f}$.*

- **Morphisms:** *if $s : A \to B$ is a $\mathbb{C}$-morphism, then $\overline{L}(s) : \overline{L}(B) \to \overline{L}(A)$ is the functor acting as identity on objects and by precomposition on morphisms: given a $\overline{L}(B)$-morphism $f : L(B) \otimes X \to Y$, we have*

$$\overline{L}(s)(f) = f \circ (L(s) \otimes \mathrm{id})$$

When L is the identity functor $(\mathbb{C}, \times, 1) \to (\mathbb{C}, \times, 1)$, then $\overline{L}$ is the simple fibration. Now, note that any LNL-adjunction $L \dashv R$ gives rise to a fibration $\overline{L}$, which also sits in a fibered LNL-adjunction, where the non-linear fibration is merely the simple fibration. Similarly, fibered monoidal closure of $\overline{L}$ with respect to the induced symmetric monoidal product may be derived from the monoidal closure of $\mathbb{L}$. However, we shall only use Construction 6.2.7 as a guideline to define indexed zigzag game while it may be worthwhile to explore the general structure of $\overline{L}$, this does not seem not allow to easily derive the FOFIMELL of $\mathfrak{Dial}^{\blacktriangleright}(p)$ for arbitrary p[2]. We thus merely unfold the definition of indexed zigzag games obtained by applying Construction 6.2.7 to the setting of zigzag games.

Definition 6.2.8. *Let A be on object of $\mathbb{S}$. The category of A-*indexed zigzag game *is defined as follows:*

- **Objects:** *a pair of objects (U, X) of $\mathbb{S}$.*

- **Morphisms:** *a morphism $(U, X) \to (V, Y)$ is a pair of morphisms*

$$f : A \times U \times \blacktriangleright X \to V \qquad\qquad F : A \times U \times X \to Y$$

Up to obvious isomorphism, (f, F) may be regarded as a P-strategy in the zigzag game

$$(A, 1) \otimes (U, X) \;= (A \times U, X) \quad \longrightarrow \quad (V, Y)$$

- **Composition:** *given morphisms $(f, F) : (U, X) \to (V, Y)$ and $(g, G) : (V, Y) \to (W, Z)$, the composition $(h, H) = (g, G) \circ (f, F)$ is intuitively computed by making two strategies by simulating a play over three "boards": the left board $A \times U \times X$, the middle board $V \times Y$ and the right board $W \times Z$. Calling respectively $(a_n)_{n\in\mathbb{N}}, (u_n)_{n\in\mathbb{N}}, (x_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}, (w_n)_{n\in\mathbb{N}}$ and $(z_n)_{n\in\mathbb{N}}$ the produced sequences, a round may be*

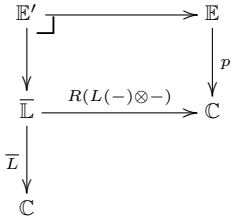
  – *First, O plays $a_n \in A_n$ and $u_n \in U_n$ on the left board, to which the strategy answers with $v_n = f_n(a_n, u_n, x_{n-1}) \in V_n$ on the middle board, which gets propagated to $w_n = g_n(a_n, v_n, y_{n-1})$ on the right board.*

  – *Then, O plays a legal move z_n, enabling proponent to compute $y_n = G_n(a_n, w_n, z_n) \in Y_n$ on the middle board, which gets propagated to $z_n = F_n(a_n, w_n, z_n) \in Z_n$.*

  The composition computes this strategy, implicitly hiding the interaction on the "middle board" and thus producing functions

$$h : A \times U \times \blacktriangleright Z \to W \qquad\qquad H : A \times U \times Z \to X$$

[2]The temptation here would be to study the fibration obtained by composing the arrows on the left handside column.



However, this does no seem to coincide with $\mathfrak{Dial}^{\blacktriangleright}(p)$ when $\mathbb{C} = \mathbb{S}$ and $\mathbb{L} = \mathsf{DZ}$.

From a more formal point of view, (h, H) is obtained by taking the first components of the unique tuple

$$\begin{pmatrix} h & : A \times U \times \blacktriangleright Z \to W \\ H & : A \times U \times Z \to X \\ \widetilde{v} & : A \times U \times \blacktriangleright Z \to V \\ \widetilde{y} & : A \times U \times Z \to Y \end{pmatrix}$$

of morphisms satisfying the following equations

$$\begin{array}{lcl} h & = & g \circ \langle \pi_1, \widetilde{v}, \pi_3 \rangle \\ H & = & F \circ \langle \pi_1, \pi_2, \widetilde{y} \rangle \\ \widetilde{v} & = & f \circ \langle \pi_1, \pi_2, H \circ (\mathrm{id} \times \mathrm{id} \times \mathrm{next}) \rangle \\ \widetilde{y} & = & G \circ \langle \pi_1, \widetilde{v}, \pi_3 \rangle \end{array}$$

Definition 6.2.9. *Let $p : \mathbb{E} \to \mathbb{S}$ be a fibration. The total category $\mathfrak{Dial}^{\blacktriangleright}(\mathbb{E})$ of the associated fibration $\mathfrak{Dial}^{\blacktriangleright}(p)$ is defined as follows:*

- **Objects:** *objects are triples (A, U, X, φ) such that A, U and X are objects of $\mathbb{S}$ and φ belongs to $p_{A \times U \times X}$ (same as $\mathfrak{Dial}(p)$). We write sometimes write such triples $(a : A, u : U, x : X, \varphi(a, u, x))$.*
- **Morphisms:** *morphisms from $\Phi = (a : A, u : U, x : X, \varphi(a, u, x))$ to $\Psi = (b : B, v : V, y : Y, \psi(b, v, y))$ are tuples $(s, f, F, \alpha) : \Phi \to \Psi$ where*
  - *$s : A \to B$ is a $\mathbb{S}$-morphism.*
  - *$f : A \times U \times \blacktriangleright Y \to V$ and $F : A \times U \times Y \to X$ are $\mathbb{S}$-morphisms; thus (f, F) is a morphism of A-indexed games $(U, X) \to (V, Y)$.*
  - *$\alpha : \varphi(a, u, F(a, u, y)) \to \psi(s(a), f(a, u, \mathrm{next}(y)), y)$ is a $p_{A \times U \times Y}$-morphism. Intuitively, α is a proof that (f, F) maps winning strategies to winning strategies.*
- **Composition:** *given*

  $$(s, f, F, \alpha) : (a : A, u : U, x : X, \varphi(a, u, x)) \to (b : B, v : V, y : Y, \psi(b, v, y)) \quad \text{and}$$
  $$(t, g, G, \beta) : (b : B, v : V, y : Y, \psi(b, v, y)) \to (c : C, w : W, z : Z, \phi(c, w, z))$$

  the composite consists of:
  - *the synchronous function $t \circ s : A \to C$.*
  - *the functions $h : A \times U \times \blacktriangleright Z \to W$ and $H : A \times U \times Z \to X$ are defined as the composition of the A-indexed game morphisms (f, F) and (g, G) as outlined in Definition 6.2.8.*
  - *borrowing the notation $\widetilde{v} : A \times U \times \blacktriangleright Z \to V$ and $\widetilde{y} : A \times U \times Z \to Y$ from the definition of composition in zigzag games (Definition 6.2.8), we may obtain by substitution p-morphisms $\widetilde{\alpha} = \langle \pi_1, \pi_2, \widetilde{y} \rangle^* \alpha$ and $\widetilde{\beta} = \langle s \circ \pi_1, \widetilde{v}, \pi_3 \rangle^* \beta$*

    $$\begin{array}{rcl} \varphi(a, u, F(a, u, \widetilde{y}(a, u, z))) & \to & \psi(s(a), f(a, u, \mathrm{next}(\widetilde{y}(a, u, z))), \widetilde{y}(a, u, z)) \\ \psi(s(a), \widetilde{v}(a, u, \mathrm{next}(z)), G(s(a), \widetilde{v}(a, u, \mathrm{next}(z)), z)) & \to & \phi(t(s(a)), g(s(a), \widetilde{v}(a, u, z), \mathrm{next}(z)), z) \end{array}$$

    Note that the domain and codomain are equal since $\widetilde{v} = f \circ \langle \pi_1, \pi_2, \mathrm{next} \circ \widetilde{y} \rangle$ and $\widetilde{y} = G \circ \langle \pi_1, \widetilde{v}, \pi_3 \rangle$; hence, the last component of the composite is $\widetilde{\beta} \circ \widetilde{\alpha}$.

The fibration itself $\mathfrak{Dial}^{\blacktriangleright}(p) : \mathfrak{Dial}^{\blacktriangleright}(\mathbb{E}) \to \mathbb{S}$ is defined as the projection on the first component.

The definition of $\mathfrak{Dial}^{\blacktriangleright}(p)$ allows for more elaborate morphisms than $\mathfrak{Dial}(p)$, so there is an obvious inclusion fibred functor $I^{\mathfrak{Dial}^{\blacktriangleright}} : \mathfrak{Dial}(p) \to \mathfrak{Dial}^{\blacktriangleright}(p)$. This functor is part of an adjunction, from which the aforementioned monad $\mathbf{fix}_{\blacktriangleright} : \mathfrak{Dial}(p) \to \mathfrak{Dial}(p)$ may be recovered.

Lemma 6.2.10. *$I^{\mathfrak{Dial}^{\blacktriangleright}}$ has a right adjoint $J^{\mathfrak{Dial}^{\blacktriangleright}} : \mathfrak{Dial}^{\blacktriangleright}(p) \to \mathfrak{Dial}(p)$ defined as follows on objects.*

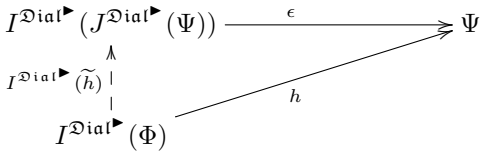
$$\begin{pmatrix} a : A, u : U, x : X \\ \varphi(a, u, x) \end{pmatrix} \longmapsto \begin{pmatrix} a : A, \widetilde{u} : U^{\blacktriangleright X}, x : X \\ \psi(a, \widetilde{u}(\mathrm{next}(x)), x) \end{pmatrix}$$

Moreover, the adjunction $I^{\mathfrak{Dial}^{\blacktriangleright}} \dashv J^{\mathfrak{Dial}^{\blacktriangleright}}$ induces the monad $\mathbf{fix}_{\blacktriangleright} : \mathfrak{Dial}(p) \to \mathfrak{Dial}(p)$.

Proof. To show that $J^{\mathfrak{Dial}^{\blacktriangleright}}$ extends to a fiberwise right adjoint to $I^{\mathfrak{Dial}^{\blacktriangleright}}$, it suffices to show that for every

$$\Phi = \begin{pmatrix} a : A, u : U, x : X \\ \varphi(a, u, x) \end{pmatrix} \quad \mathfrak{Dial}(p)\text{-predicate}$$
$$\Psi = \begin{pmatrix} a : A, v : V, y : Y \\ \psi(a, v, y) \end{pmatrix} \quad \mathfrak{Dial}^{\blacktriangleright}(p)\text{-predicate}$$

there is a map $\epsilon : I^{\mathfrak{Dial}^{\blacktriangleright}}(J^{\mathfrak{Dial}^{\blacktriangleright}}(\Psi)) \to \Psi$ such that, for every map $h : I^{\mathfrak{Dial}^{\blacktriangleright}}(\Phi) \to \Psi$, there exists a unique $\widetilde{h} : \Phi \to J^{\mathfrak{Dial}^{\blacktriangleright}}(\Psi)$ such that the following diagram commute.



The map

$$\epsilon : \begin{pmatrix} a : A, f : V^{\blacktriangleright Y}, y : Y \\ \psi(a, \mathrm{ev}(f, \mathrm{next}(y)), y) \end{pmatrix} \to \begin{pmatrix} a : A, v : V, y : Y \\ \psi(a, v, y) \end{pmatrix}$$

is given as the following tuple $(\epsilon_1, \epsilon_2, \epsilon_3)$:

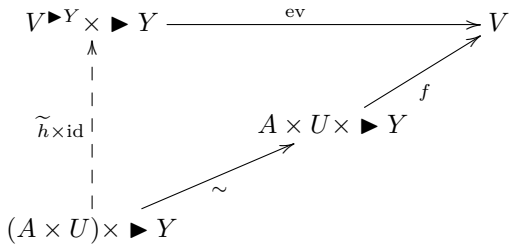
- ϵ_1 is the composite

$$A \times V^{\blacktriangleright Y} \times \blacktriangleright Y \xrightarrow{\langle \pi_2, \pi_3 \rangle} V^{\blacktriangleright Y} \times \blacktriangleright Y \xrightarrow{\mathrm{ev}} V$$

- ϵ_2 is the last projection $A \times V^{\blacktriangleright Y} \times Y \to Y$.

- $\epsilon_3 : \psi(a, \mathrm{ev}(f, \mathrm{next}(y)), y) \to \psi(a, \mathrm{ev}(f, \mathrm{next}(y)), y)$ is the identity.

Now, setting $h = (\mathrm{id}, f, F, \alpha)$ and $\widetilde{h} = (\mathrm{id}, \widetilde{f}, \widetilde{F}, \widetilde{\alpha})$, having the universal property amounts to having $\widetilde{F} = F$, the following diagram commute



and $\widetilde{\alpha} = \alpha$. This uniquely determines $\widetilde{h}$ since $\mathbb{S}$ is cartesian-closed, and thus h is also uniquely determined.

This establishes that we have for each fiber a right ajoint to $I^{\mathfrak{Dial}^{\blacktriangleright}}$. We may then conclude by checking that the Beck-Chevalley condition is satisfied as per Lemma 5.2.18. This tedious but straightforward verification is left to the reader. □

Similarly to the $\mathfrak{Dial}$ construction, $\mathfrak{Dial}^{\blacktriangleright}$ inherits monoidal products from p.

Lemma 6.2.11. *Suppose that $p : \mathbb{E} \to \mathbb{S}$ has a monoidal structure $(\otimes, unit)$. $\mathfrak{Dial}^{\blacktriangleright}(p)$ inherits a monoidal structure, whose product, also denoted $\otimes$, has the following object component.*

$$\begin{pmatrix} a : A, u : U, x : X \\ \varphi(a, u, x) \end{pmatrix}, \begin{pmatrix} a : A, v : V, y : Y \\ \psi(a, v, y) \end{pmatrix} \mapsto \begin{pmatrix} a : A, (u, v) : U \times V, (x, y) : X \times Y \\ \varphi(a, u, x) \otimes \psi(a, v, y) \end{pmatrix}$$

Furthermore, if $\mathfrak{Dial}(p)$ is equipped with the monoidal structure from Lemma 5.3.11, $I^{\mathfrak{Dial}^{\blacktriangleright}} \dashv J^{\mathfrak{Dial}^{\blacktriangleright}}$ is a lax monoidal adjunction.

Proof. The monoidal structure is defined as in Lemma 5.3.11. It is rather obvious that $I^{\mathfrak{Dial}^{\blacktriangleright}}$ is strong monoidal. The unit is preserved, up to canonical isomorphism, by $J^{\mathfrak{Dial}^{\blacktriangleright}}$. As for the lax structure on binary products, it arises from a family of maps

$$\begin{pmatrix} a : A, (\widetilde{u}, \widetilde{v}) : U^{\blacktriangleright X} \times V^{\blacktriangleright Y}, (x, y) : X \times Y \\ \varphi(a, (\mathrm{ev}(\widetilde{u}, \mathrm{next}(x)), \mathrm{ev}(\widetilde{v}, \mathrm{next}(y))), (x, y) \end{pmatrix} \to \begin{pmatrix} a : A, f : (U \times V)^{\blacktriangleright (X \times Y)}, (x, y) : X \times Y \\ \varphi(a, \mathrm{ev}(f, \mathrm{next}(x, y)), (x, y)) \end{pmatrix}$$

induced in turns by the obvious (non-invertible) map $U^{\blacktriangleright X} \times V^{\blacktriangleright Y} \to (U \times V)^{\blacktriangleright (X \times Y)}$. □

$\mathfrak{Dial}^{\blacktriangleright}(p)$ also inherits monoidal closure from p. However, contrary to $\mathfrak{Dial}(p)$, we do not rely on the cartesian closure of the base $\mathbb{S}$ to define the monoidal closure. Instead, we use the pointwise arrow.

Lemma 6.2.12. *Suppose that $p : \mathbb{E} \to \mathbb{S}$ has a monoidal closed structure $(\otimes, \mathbf{I})$. Then, $\mathfrak{Dial}^{\blacktriangleright}(p)$ inherits a monoidal closed structure. The monoidal product is given as per Lemma 6.2.11, and the object part of the functor $(a : A, v : V, y : Y, \psi(a, v, y)) \multimap - : \mathfrak{Dial}(p)_A \to \mathfrak{Dial}(p)_A$ is*

$$\left(\begin{array}{c} a : A, u : U, x : X \\ \varphi(a, u, x) \end{array} \right) \mapsto \left(\begin{array}{c} a : A, (f, F) : (U \twoheadrightarrow V) \times ((U \times Y) \twoheadrightarrow X), (u, y) : U \times Y \\ \varphi(a, u, \mathrm{ev}_{\twoheadrightarrow}(F, \langle u, y \rangle)) \multimap \psi(a, \mathrm{ev}_{\twoheadrightarrow}(f, u), y) \end{array} \right)$$

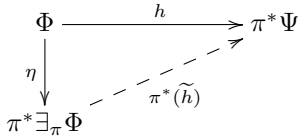
Proof. The proof is similar to the one presented in Lemma 5.3.13, except that the pointwise function space $\twoheadrightarrow$ is used instead of the cartesian-closed structure of $\mathbb{S}$. □

Lemma 6.2.13. *Suppose that p has two monoidal structures $(\otimes, \mathbf{I})$ and $(\parr, \bot)$, as well as a distributivity law $\mathbf{dist}_{\varphi,\psi,\phi} : \varphi \otimes (\psi \parr \phi) \to (\varphi \otimes \psi) \parr \phi$. Then $I^{\mathfrak{Dial}^{\blacktriangleright}}$ maps the vertical distributivity law of Lemma 5.3.12 to a distributivity law between the relevant monoidal structures of $\mathfrak{Dial}^{\blacktriangleright}$.*

Lemma 6.2.14. *The fibration $\mathfrak{Dial}^{\blacktriangleright}(p)$ has simple sums and simple products. Given a projection $\pi : A \times B \to A$ and an object $(U, X, \varphi) : A \times B$, the object component of the functors $\exists_\pi, \forall_\pi$ are*

$$\begin{array}{rcccc} \exists_\pi : & \left(\begin{array}{c} (a, b) : A \times B, u : U, x : X \\ \varphi(a, b, u, x) \end{array} \right) & \mapsto & \left(\begin{array}{c} a : A, (u, b) : U \times B, x : X \\ \varphi(a, b, u, x) \end{array} \right) \\ \forall_\pi : & \left(\begin{array}{c} (a, b) : A \times B, u : U, x : X \\ \varphi(a, b, u, x) \end{array} \right) & \mapsto & \left(\begin{array}{c} a : A, f : B \twoheadrightarrow U, (x, b) : X \times B \\ \varphi(a, v, \mathrm{ev}_{\twoheadrightarrow}(f, b), x) \end{array} \right) \end{array}$$

Proof. This time around, one cannot use the decomposition $\mathfrak{Dial}(p) \cong \mathfrak{Sum}(\mathfrak{Prod}(p))$, so we need to prove that from scratch. Let us start with $\exists_\pi$. To show that the definition on objects extends to a left adjoint to π^*, it suffices to exhibit, for every $\mathfrak{Dial}^{\blacktriangleright}(p)$ predicate Φ over $A \times B$ a (vertical) map $\eta : \Phi \to \pi^* \exists_\pi \Phi$ such that, for every map $h : \Phi \to \pi^* \Psi$, there exists a unique (vertical) $\widetilde{h} : \exists_\pi \Phi \to \Psi$ making the following diagram commute.



Writing

$$\begin{array}{rcl} \Phi & = & ((a, b) : A, u : U, x : X, \varphi(a, b, u, x)) \\ \Psi & = & (a : A, v : V, y : Y, \psi(a, v, y)) \\ h & = & (\mathrm{id}, f, F, \alpha) \end{array}$$

we have the following, where the first line is a canonical vertical isomorphism

$$\begin{array}{rcl} \pi^* \exists_\pi \Phi & \cong & ((a, b) : A \times B, (u, b') : U \times B, x : X, \varphi(a, b', u, x)) \\ \pi^* \Psi & = & ((a, b) : A \times B, v : V, y : Y, \psi(a, v, y)) \end{array}$$

The components η_0, η_1, η_2 of the map η are given as follows:

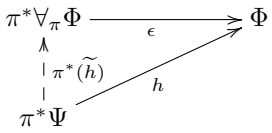
- $\eta_0 : (A \times B) \times U \times \blacktriangleright X \to B \times U$ is given by pairing the obvious projections: $\langle \pi_2 \circ \pi_1, \pi_2 \rangle$.
- $\eta_1 : (A \times B) \times U \times X \to X$ is simply the last projection.
- η_2 is then the identity $\varphi(a, b, u, x) \to \varphi(a, b, u, x)$.

Let us suppose that a map $\widetilde{h} = (\mathrm{id}, \widetilde{f}, \widetilde{F}, \widetilde{\alpha}) : \exists_\pi \Phi \to \Psi$ make the above diagram commute. This means that we necessarily have

$$\begin{array}{rcl} \widetilde{f} & = & f \circ \langle \langle \pi_1, \pi_2 \circ \pi_2 \rangle, \pi_1 \circ \pi_2, \pi_3 \rangle \\ \widetilde{F} & = & F \circ \langle \langle \pi_1, \pi_2 \circ \pi_2 \rangle, \pi_1 \circ \pi_2, \pi_3 \rangle \\ \widetilde{\alpha} & = & \alpha \end{array}$$

This in turn can obviously be taken to be the definition of $\widetilde{h}$. The Beck-Chevalley condition is straightforward to check.

Now, let us turn to $\forall_\pi$. Taking the notations, we now need a map $\epsilon : \pi^*\forall_\pi\Phi \to \Phi$, such that, for every map $h : \pi^*\Psi \to \Phi$, there exists a unique map $\widetilde{h}$ making the following diagram commute.



The components $\epsilon_0, \epsilon_1, \epsilon_2$ of the map ϵ are given as follows:

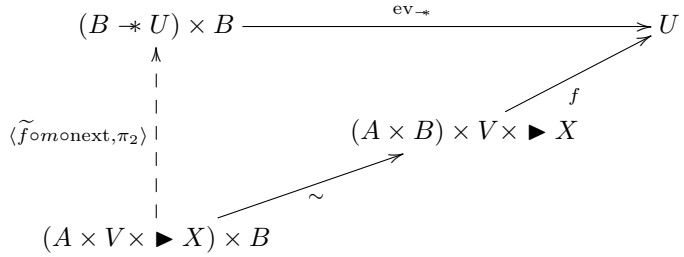
- $\epsilon_0 : (A \times B) \times (B \multimap U) \times \blacktriangleright X \to U$ is given by first projecting onto $(B \multimap U) \times B$ and then pointwise evaluation.

$$(A \times B) \times (B \multimap U) \times \blacktriangleright (X \times B) \xrightarrow{\langle \pi_2, \pi_2 \circ \pi_1 \rangle} (B \multimap U) \times B \xrightarrow{\mathrm{ev}_{\multimap}} U$$

- $\epsilon_1 : (A \times B) \times (B \multimap U) \times X \to X \times B$ is the map $\langle \pi_3, \pi_2 \circ \pi_1 \rangle$.

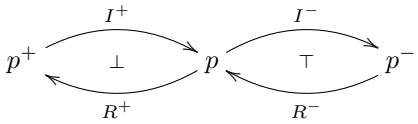
- Then $\epsilon_2 : \varphi(a, b, \mathrm{ev}_{\multimap}(f, b), x) \to \varphi(a, b, \mathrm{ev}_{\multimap}(f, b), x)$ is the identity.

Now, let us suppose that a map $\widetilde{h} = (\mathrm{id}, \widetilde{f}, \widetilde{F}, \widetilde{\alpha}) : \Psi \to \forall_\pi\Phi$ making the above diagram commute. Unravelling the definition, this enforces that the following diagram commute.

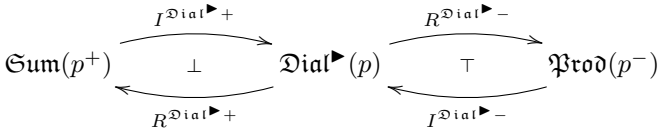


where m is the obvious isomorphism $(A \times V \times \blacktriangleright X) \times \blacktriangleright B \to A \times V \times \blacktriangleright (X \times B)$. By Lemma 6.1.8, $\widetilde{f}$ is thus uniquely determined. Beyond that, it also enforces $\widetilde{F} = F \circ \langle \langle \pi_1, \pi_2 \circ \pi_3 \rangle, \pi_2, \pi_1 \circ \pi_3 \rangle$ and $\widetilde{\alpha} = \alpha$. We leave the checking of the Beck-Chevalley condition to the interested reader. □

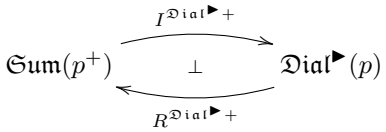
Theorem 6.2.15. *Assume a* FOFIMELL *fibration* (p^+, p, p^-) *using the following string of monoidal adjunctions for exponential modalities.*



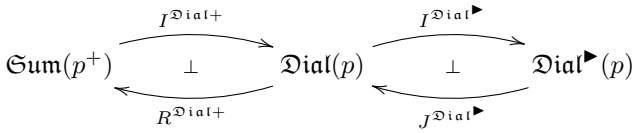
Then, this FOFIMELL *fibration may be lifted to another* FOFIMELL*-fibration* $(\mathfrak{Sum}(p^+), \mathfrak{Dial}^{\blacktriangleright}(p), \mathfrak{Prod}(p^-))$.



Proof. The groundwork pertaining to the propositional structure of $\mathfrak{Dial}^{\blacktriangleright}(p)$ having been laid in the previous lemmas, we turn to the exponential structure. The lax monoidal adjunction between $\mathfrak{Sum}(p^+)$ and $\mathfrak{Dial}^{\blacktriangleright}(p)$ is recovered by composing the lax monoidal adjunction of Theorem 6.2.15 together with monoidal adjunction between $\mathfrak{Dial}(p) \to \mathfrak{Dial}^{\blacktriangleright}(p)$ alluded to in Lemma 6.2.10.



=



Since this is a composition of monoidal adjunctions, we recover a monoidal adjunction. The induced comonad $! = R^{\mathfrak{Dial}^{\blacktriangleright}+} \circ I^{\mathfrak{Dial}^{\blacktriangleright}+}$ acts as follows on objects:

$$!(a : A, u : U, x : X, \varphi(a, u, x)) \quad = \quad (a : A, f : U^{\blacktriangleright X}, * : 1, !\forall x^X \ \varphi(a, \mathrm{ev}(f, \mathrm{next}(x)), x))$$

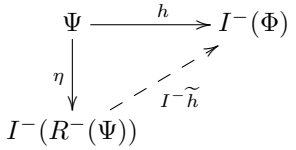
The oplax monoidal adjunction corresponding to ? cannot be recovered as a composition of functors we defined so far, so we shall define directly an oplax monoidal adjunction $R^- \dashv I^-$ between $\mathfrak{Dial}^{\blacktriangleright}(p)$ and $\mathfrak{Prod}(p)$, which is to be composed with the image of the adjunction between p and p^- by $\mathfrak{Prod}$. On objects I^- and R^- are defined as follows.

$$\begin{array}{lcl} I^-(a : A, x : X, \varphi(a, x)) & = & (a : A, * : 1, x : X, \varphi(a, x)) \\ R - (a : A, u : U, x : X, \varphi(a, u, x)) & = & (a : A, g : X^U, \exists u^U \ \varphi(a, u, \mathrm{ev}(g, u))) \end{array}$$

The action of I^- on morphism is rather straightforward, while R^- is much more involved. Let us show that the map on objects defined above extends to a left adjoint to I^- by appealing to Lemma 5.2.18. To this end, consider

$$\begin{array}{rcll} \Phi & = & \left(\begin{array}{c} a : A, x : X \\ \varphi(a, x) \end{array} \right) & \text{a } \mathfrak{Prod}(p)\text{-predicate} \\ \Psi & = & \left(\begin{array}{c} a : A, v : V, y : Y \\ \psi(a, v, y) \end{array} \right) & \text{a } \mathfrak{Dial}^{\blacktriangleright}(p)\text{-predicate} \end{array}$$

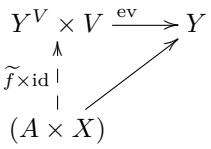
We need to exhibit a $\mathfrak{Dial}^{\blacktriangleright}(p)$ map $\eta : \Psi \to I^-(R^-(\Psi))$ such that, for every $h : \Psi \to I^-(\Phi)$, there exists a unique $\mathfrak{Prod}(p)$-map $\widetilde{h}$ making the following diagram commute



The map η has components (η_1, η_2, η_3) defined as follows

- $\eta_1 : A \times V \times \blacktriangleright Y^V \to 1$ is trivial.
- $\eta_2 : A \times V \times Y^V \to Y$ is the evaluation map precomposed with $\langle \pi_3, \pi_2 \rangle$.
- η_3 is the identity $\varphi(a, v, \mathrm{ev}(f, v)) \to \varphi(a, v, \mathrm{ev}(f, v))$.

Writing $h = (\mathrm{id}, f, !, \alpha)$ and $\widetilde{h} = (\mathrm{id}, \widetilde{f}, \widetilde{\alpha})$, the above diagram commuting amounts to making



commute and $\widetilde{\alpha} = \alpha$. This uniquely determines $\widetilde{h}$ and show that I^- has a fiberwise left adjoint. One needs to check the Beck-Chevalley condition in Lemma 5.2.18 to conclude that R^- is a fibred left adjoint. As usual, this straightforward exercise is left to the reader.

Before moving on, let us spell out the action of $? = R^{\mathfrak{Dial}^{\blacktriangleright}-} \circ I^{\mathfrak{Dial}^{\blacktriangleright}-}$ on objects of $\mathfrak{Dial}^{\blacktriangleright}(p)$.

$$?(a : A, u : U, x : X, \varphi(a, u, x)) \quad = \quad (a : A, * : 1, \widetilde{x} : X^U, ?\exists u^U \ \varphi(a, u, \mathrm{ev}(\widetilde{x}, u)))$$

As in Theorem 5.3.15, $\mathfrak{Sum}(p^+)$ has all simple products since $\mathbb{S}$ is cartesian-closed and p^+ has simple products by Lemma 5.3.7. Similarly, $\mathfrak{Prod}(p^-)$ has all simple sums.

All that remains to be shown is that we have the following vertical natural transformations, where φ and ψ are $\mathfrak{Dial}^{\blacktriangleright}(p)$ predicates.

$$!\varphi \otimes ?\psi \quad \longrightarrow \quad ?(!\varphi \otimes \psi) \qquad\qquad !(\varphi \parr ?\psi) \quad \longrightarrow \quad !\varphi \parr ?\psi$$

Working in the fiber over A and expanding the definitions, it means we should have the following vertical natural transformations.

$$\left(\begin{array}{c} a:A,\quad f:U^{\blacktriangleright X},\quad g:Y^V \\ \\ !\forall x^X\ \varphi(a,\mathrm{ev}(f,\mathrm{next}(x)),x) \\ \otimes \\ ?\exists v^V\ \psi(a,v,\mathrm{ev}(f,v)) \end{array}\right) \longrightarrow \left(\begin{array}{c} a:A,\quad *:1,\quad h:Y^{U^{\blacktriangleright X}\times V} \\ \\ ?\exists(i,v)^{U^{\blacktriangleright X}\times V} \left[\begin{array}{c} !\forall x^X\ \varphi(a,\mathrm{ev}(i,\mathrm{next}(x)),x) \\ \otimes \\ ?\exists v^V\ \psi(a,v,\mathrm{ev}(h,\langle i,v\rangle)) \end{array}\right] \end{array}\right)$$

$$\left(\begin{array}{c} a:A,\quad f:U^{\blacktriangleright(X\times Y^V)},\quad *:1 \\ \\ !\forall(x,g)^{X\times Y^V} \left[\begin{array}{c} \varphi(a,\mathrm{ev}(f,\mathrm{next}(\langle x,g\rangle)),x) \\ \parr \\ ?\exists v^V\ \psi(a,v,\mathrm{ev}(g,v)) \end{array}\right] \end{array}\right) \longrightarrow \left(\begin{array}{c} a:A,\quad h:U^{\blacktriangleright X},\quad i:Y^V \\ \\ !\forall x^X\ \varphi(a,\mathrm{ev}(h,\mathrm{next}(x)),x) \\ \parr \\ ?\exists v^V\ \psi(a,v,\mathrm{ev}(i,v)) \end{array}\right)$$

Let us focus on the first one. The $\mathbb{S}$-level part of the morphism is induced by the unique map $A\times U^{\blacktriangleright X}\to 1$ and the obvious partial evaluation map.

$$A\times U^{\blacktriangleright X}\times Y^{U^{\blacktriangleright X}\times V}\longrightarrow U^{\blacktriangleright X}\times Y^{U^{\blacktriangleright X}\times V}\longrightarrow Y^V$$

At the level of propositions, it thus suffices to give a proof in p of the following implication.

$$\begin{array}{c} !\forall x^X\ \varphi(a,\mathrm{ev}(f,\mathrm{next}(x)),x) \\ \otimes \\ ?\exists v^V\ \psi(a,v,\mathrm{ev}(h,\langle f,v\rangle)) \end{array} \multimap\quad ?\exists(i,v)^{U^{\blacktriangleright X}\times V}\left[\begin{array}{c} !\forall x^X\ \varphi(a,\mathrm{ev}(i,\mathrm{next}(x)),x) \\ \otimes \\ ?\exists v^V\ \psi(a,v,\mathrm{ev}(h,\langle i,v\rangle)) \end{array}\right]$$

Deriving the entailment in the FIMELL sequent calculus is done almost exactly as in the proof of Theorem 5.3.15. Let us just notice that the existential variable i is witnessed by f in the derivation. □

6.2.3 Elimination of double linear negation

Before moving on with the characterization theorem, let us notice that as for $\mathfrak{Dial}$ over most reasonable bases $\mathbb{B}$, $\mathfrak{Dial}^{\blacktriangleright}(p)$ is never $*$-autonomous for trivial cardinality reasons. However, similarly to $\mathfrak{Dial}$ over **Set**, the canonical maps

$$\varphi\quad\multimap\quad(\varphi\multimap\bot)\multimap\bot$$

have retracts.

Theorem 6.2.16. *If p is a* FOFIMELL*-fibration eliminating double linear negations, so is $\mathfrak{Dial}(p)$ if $\mathcal{C}=$ **Set**, assumed to satisfy the axiom of choice, or* **FinSet**.

Proof. The proof takes heavy inspiration from the proof of Theorem 5.3.16. Computing the linear double-negation gives a similar result, where the pointwise exponential plays the rôle of the internal homset in the aforementioned proof: if $\Phi=(a:A,u:U,x:X,\varphi(a,u,x))$ is a predicate of $\mathfrak{Dial}^{\blacktriangleright}(p)$, $(\Phi\multimap\bot)\multimap\bot$ is vertically isomorphic to

$$\big(a:A,F:(U\multimap X)\multimap U,f:U\multimap X,(\varphi(a,\mathrm{ev}_{-\!*}(F,f),\mathrm{ev}_{-\!*}(f,\mathrm{ev}_{-\!*}(F,f)))\multimap\bot)\multimap\bot\big)$$

Making similar simplifying assumptions on the shape of the proof $(\Phi\multimap\bot)\multimap\bot\multimap\Phi$ that we want to obtain as in the proof of Theorem 5.3.16, we only need to provide $\mathbb{S}$-morphisms $h:((U\multimap X)\multimap U)\to U$ and $H:((U\multimap X)\multimap U)\times X\to U\multimap X$ such that, for every global elements $F:1\to(U\multimap X)\multimap U$ and $x:1\to X$ we have

$$\mathrm{ev}_{-\!*}\circ\langle F,H\circ\langle F,x\rangle\rangle=h\circ F\qquad\text{and}\qquad\mathrm{ev}_{-\!*}\circ\langle H\circ\langle F,x\rangle,\mathrm{ev}_{-\!*}\circ\langle F,H\circ\langle F,x\rangle\rangle\rangle=x$$

But in fact, we can aim for h and H being given by pointwise exponentials. This means that if we have sequences $(\widetilde{h}_n:U_n^{X_n^{U_n}}\to U_n)_{n\in\mathbb{N}}$ and $(\widetilde{H}_n:U_n^{X_n^{U_n}}\times X_n\to X_n^{U_n})_{n\in\mathbb{N}}$ such that, for every sequences $(F_n:X_n^{U_n}\to U_n)_{n\in\mathbb{N}})$ and $(x_n:X_n)_{n\in\mathbb{N}}$

$$F_n(H_n(F_n,x_n))=h_n(F_n)\qquad\text{and}\qquad H_n(F_n,x_n)(F_n(H_n(F_n,x_n)))=x_n$$

then we are done by setting $h=\mathrm{ev}_{-\!*}\circ\langle(\_\mapsto\widetilde{h}_n)_{n\in\mathbb{N}},\mathrm{id}\rangle$ and $H=\mathrm{ev}_{-\!*}\circ\langle(\_\mapsto\widetilde{H}_n)_{n\in\mathbb{N}},\mathrm{id}\rangle$. But notice that the proof of Theorem 5.3.16 gives suitable H_n and h_n for each n, so we may reconstruct the sequences. □

$$
\begin{array}{rcll}
(\mathtt{t}=\mathtt{t}')^D & := & (\mathtt{t}=\mathtt{t}')_D & := \quad \mathtt{t}=\mathtt{t}' \\
(\varphi\otimes\psi)^D(a) & := & \exists\langle u,v\rangle\forall\langle x,y\rangle.\ (\varphi\otimes\psi)_D(\langle u,v\rangle,\langle x,y\rangle,a) & := \\
 & & & \quad \exists\langle u,v\rangle\forall\langle x,y\rangle.\ \varphi_D(u,x,a)\otimes\psi_D(v,y,a) \\
(\varphi\parr\psi)^D(a) & := & \exists\langle u,v\rangle\forall\langle x,y\rangle.\ (\varphi\parr\psi)_D(\langle u,v\rangle,\langle x,y\rangle,a) & := \\
 & & & \quad \exists\langle u,v\rangle\forall\langle x,y\rangle.\ \varphi_D(u,x,a)\parr\psi_D(v,y,a) \\
(\varphi\multimap\psi)^D(a) & := & \exists\langle f,F\rangle\forall\langle u,y\rangle.\ (\varphi\multimap\psi)_D(\langle f,F\rangle,\langle u,y\rangle,a) & := \\
 & & & \quad \exists\langle f,F\rangle\forall\langle u,y\rangle.\ \varphi_D(u,\mathrm{ev}_{\multimap *}(F,\langle uy\rangle),a)\multimap\psi_D(\mathrm{ev}_{\multimap *}(f,u),y,a) \\
(\exists w.\varphi)^D(a) & := & \exists\langle u,w\rangle\forall x.\ (\exists w.\varphi)_D(\langle u,w\rangle,x,a) & := \quad \exists\langle u,w\rangle\forall x.\ \varphi_D(u,x,\langle a,w\rangle) \\
(\forall w.\varphi)^D(a) & := & \exists f\,\forall\langle x,w\rangle.\ (\forall w.\varphi)_D(f,\langle x,w\rangle,a) & := \quad \exists f\,\forall\langle x,w\rangle.\ \varphi_D(\mathrm{ev}_{\multimap *}(f,w),x,\langle a,w\rangle) \\
(!\varphi)^D(a) & := & \exists U.\ (!\varphi)_D(u,-,a) & := \quad \exists U.\ !\forall x.\ \varphi_D(\mathrm{ev}(U,\mathrm{next}(x)),x,a) \\
(?\varphi)^D(a) & := & \forall X.\ (?\varphi)_D(-,X,a) & := \quad \forall X.\ ?\exists u.\ \varphi_D(u,\mathrm{ev}(X,u),a)
\end{array}
$$

Figure 6.1: The Dialectica-like translation for FOFIMELL (types are left implicit).

6.3 The characterization theorem

Definition 6.3.1. *A* FOFIMELL *fibration p is said to satisfy*

- LSAC *when the following natural transformation is a isomorphism.*

$$\exists f^{A\multimap *B}\ \forall a^A\ \varphi(a,\mathrm{ev}_{\multimap *}(f,a)) \qquad\longrightarrow\qquad \forall a^A\ \exists b^B\ \varphi(a,b) \tag{16}$$

- SDEXP *when the following natural transformations are isomorphisms.*

$$\exists f^{A\blacktriangleright B}!\ \forall b^B!\varphi(\mathrm{ev}(f,\mathrm{next}(b)),b) \longrightarrow \exists a^A\ !\forall b^B\ \varphi(a,b) \tag{17}$$

$$?\exists a^A\ \forall b^B\ ?\varphi(a,b) \longrightarrow \forall f^{B^A}\ ?\exists a^A\ ?\varphi(a,\mathrm{ev}(f,a)) \tag{18}$$

Theorem 6.3.2 (Soundness)**.** *If p is an arbitrary* FOFIMELL *fibration, then $\mathfrak{Dial}(p)$ is a* FOFIMELL+ LSIP + LSAC + SDEXP *fibration. Furthermore, if p satisfies* PEXP*, so does $\mathfrak{Dial}(p)$.*

Proof. The proof is very similar to the proof of Theorem 5.4.2; we already know that $\mathfrak{Dial}(p)$ is a FOFIMELL fibration whenever p is by Theorem 5.3.15, one only needs to check that the additional axioms LSIP + LSAC + SDEXP are satisfied to prove the first half of the statement; the required isomorphisms are still immediate in most cases.

Now, let us assume that p satisfies PEXP and show that $\mathfrak{Dial}(p)$ also does.

- For the axiom

$$?!\Psi \longrightarrow !?\Psi$$

we need to provide a natural proof scheme of

$$?\exists u^U!\forall f^{X^U}\psi(a,u,\mathrm{ev}(f,u)) \quad\longrightarrow\quad !\forall x^X?\exists g^{U^{\blacktriangleright X}}\psi(a,u,x)$$

Similarly as to what happens in Theorem 5.3.15, it suffices to provide natural proofs of

$$\begin{array}{rcl}
\exists u^U!\varphi(a,u) & \vdash & !\exists u^U\varphi(a,u) \\
?\forall x^X\phi(a,x) & \vdash & \forall x^X?\varphi(a,x) \\
\rho^{\exists\forall,\forall\exists}:\quad \exists u^U\forall f^{X^U}\psi(a,u,\mathrm{ev}(f,u)) & \vdash & \forall x^X\exists g^{U^{\blacktriangleright X}}\psi(a,\mathrm{ev}(g,\mathrm{next}(x)),x)
\end{array}$$

and consider the corresponding axiom $\lambda_\phi^{?,!}:?!\phi\to!?\phi$ in p. Save for $\rho^{\exists\forall,\forall\exists}$, all the relevant maps are given as in Theorem 5.3.15. For $\rho^{\exists\forall,\forall\exists}$, using the universal properties of $\exists$ and $\forall$, it amounts to proving

$$\forall f^{X^U}\psi(u,\mathrm{ev}(f,u))\longrightarrow\exists g^{U^{\blacktriangleright X}}\psi(\mathrm{ev}(g,\mathrm{next}(x)),x)$$

The witnesses for f and g are the constant functions built from x and u respectively.

□

Theorem 6.3.3. *A* FOFIMELL *fibration p over $\mathbb{S}$ satisfying* LSIP, LSAC, PEXP *and* SDEXP *has, for every* MFOLL *predicate φ, an equivalence.*

$$\varphi(a) \qquad \leftrightarrow \qquad \exists u\, \forall x\, \varphi_D(u, x, a)$$

Proof. Similarly to Theorem 5.4.4, the proof goes by induction over the syntax of φ. $\otimes, \parr, \exists, ?$ and the equality are handled exactly in the same manner, so we only treat $\forall, \multimap$ and $!$. The formulas φ_D are deterministic as per Definition 5.4.5. Note that the proof for $\forall$ and $\multimap$ are exactly analogous to the one given in Theorem 5.4.4, except that the pointwise arrow is used, along with the axiom LSAC instead of of the genuine function space of $\mathbb{S}$ and the axiom LAC (which does not hold in $\mathfrak{Dial}^{\blacktriangleright}(p)$ in general). The clause for $!$ is handled through SDEXP instead of DEXP.

- **Case** $\forall a^A\, \varphi(a)$ by induction, it suffices to prove the following equivalence.

$$\forall b^B \exists u^U\, \forall x^X\, \varphi_D(u, x, a, b) \qquad \leftrightarrow \qquad \exists u^U\, \forall (x, f)^{X \times U \multimap B} \varphi_D(u, x, a, \mathrm{ev}_{\multimap}(f, x))$$

  which is immediate using LSAC.

- **Case** $\varphi(a) \multimap \psi(a)$**:** by the induction hypothesis, it suffices to construct an equivalence induced by the following string of isomorphisms

$$\begin{array}{rl}
\big(\exists u^U\, \forall x^X\, \varphi_D(u, x, a)\big) \multimap \exists v^V\, \forall y^Y\, \psi_D(v, y, a) & \\
\simeq & \\
\forall u^U \big((\forall x^X\, \varphi_D(u, x, a)) \multimap \exists v^V\, \forall y^Y\, \psi_D(v, y, a)\big) & \\
\simeq & \text{By LSIP, 4.} \\
\forall u^U \exists v^V \big((\forall x^X\, \varphi_D(u, x, a)) \multimap \forall y^Y\, \psi_D(v, y, a))\big) & \\
\simeq & \text{By LSAC.} \\
\exists f^{U \multimap V} \forall u^U \big((\forall x^X\, \varphi_D(u, x, a)) \multimap \forall y^Y\, \psi_D(\mathrm{ev}_{\multimap}(f, u), y, a))\big) & \\
\simeq & \\
\exists f^{U \multimap V} \forall (u, y)^{U \times Y} \big((\forall x^X\, \varphi_D(u, x, a)) \multimap \psi_D(\mathrm{ev}_{\multimap}(f, u), y, a))\big) & \\
\simeq & \text{By LSIP, 5.} \\
\exists f^{U \multimap V} \forall (u, y)^{U \times Y} \exists x^X\, \varphi_D(u, x, a)) \multimap \psi_D(\mathrm{ev}_{\multimap}(f, u), y, a)) & \\
\simeq & \text{By LAC.} \\
\exists (f, F)^{(U \multimap V) \times (U \times Y \multimap X)} \forall (u, y)^{U \times Y} \exists x^X\, \varphi_D(u, \mathrm{ev}_{\multimap}(F, \langle u, y\rangle, a)) \multimap \psi_D(\mathrm{ev}_{\multimap}(f, u), y, a)) &
\end{array}$$

- **Case** $!\varphi(a)$**:** by the induction hypothesis, it suffices to exhibit an equivalence

$$!(\exists u^U\, \forall x^X\, \varphi_D(u, x, a)) \qquad \leftrightarrow \qquad \exists u^U\, !\forall x^X \varphi_D(u, x, a)$$

  which is given by axiom 14 from SDEXP and the fact that φ_D is deterministic.

□

Chapter 7

Revisiting LSFOM

Chapter 6 adapted the construction of Dialectica categories as found in de Paiva's PhD thesis [21] to logics over a category $\mathbb{S}$ of higher-order synchronous functions. In contrast, the logic LSFOM studied in Chapter 4 corresponds to a fibration over Mealy which is only a subcategory of $\mathbb{S}^{\text{fin}}$. The goal of this chapter is to show that the $\mathfrak{Dial}^{\blacktriangleright}$ construction may be adapted to fibrations over Mealy while restricting to a notion of finite-state realizers. This allows to build a model of LSFOM, which is elementarily equivalent to the one presented in Chapter 4, starting from the syntactic fibration arising from FOM. Then, following the ideas laid out in Chapter 6, we define an extension LSFOM^{+} which enriches LSFOM with axioms allowing to prove a characterization theorem. This in turn, combined with the Büchi-Landweber theorem yields a proof of completeness of the extended theory LSFOM^{+}.

Section 7.1 is devoted to building a bridge between the category $\mathbb{S}$ of higher-order synchronous functions and the category of f.s. causal functions Mealy. We do so by identifying an inductively defined fragment of $\mathbb{S}$ that was used to define the category of zigzag games and the $\mathfrak{Dial}^{\blacktriangleright}$ construction, and define a syntactic subcategory $\mathbb{S}^{\text{fin}}$ of $\mathbb{S}$ specifically omitting the higher-order features of $\mathbb{S}$ (internal homsets, evaluation and curryfication of functions). We then show that this category may be adequately represented in Mealy. Then, building on this material, Section 7.2 discusses how to adapt the $\mathfrak{Dial}^{\blacktriangleright}$ construction to fibrations over $\mathbb{S}^{\text{fin}}$ and obtain a construction taking as input a fibration over Mealy. This is in particular applied to the syntactic fibration arising from FOM to build a fibration modelling LSFOM. Finally, Section 7.3 exploits the material of Section 6.3 to define LSFOM^{+} and prove its completeness. This material is adapted from [57][1].

As this chapter is chiefly concerned with adapting and applying techniques developed in Chapter 6 for $\mathbb{S}$ to $\mathbb{S}^{\text{fin}}$ we shall skip all proofs that are straightforward adaptation of those found in previous chapters. As a result, this chapter is not self-contained; the reader solely interested in the LSFOM^{+} but not the higher-order setting will find [57] to be a more direct presentation.

7.1 Relating $\mathbb{S}$ and Mealy

The objective of this section is to isolate a subcategory of $\mathbb{S}$, which we shall call $\mathbb{S}^{\text{fin}}$, allowing to carry out a significant subset of the constructions examined in Chapter 6 without necessitating the cartesian-closed structure of $\mathbb{S}$. To be more precise, we are looking for a category $\mathbb{S}^{\text{fin}}$ incorporating most of the internal syntax of $\mathbb{S}$ as well as faithful functors

$$\mathsf{Mealy} \rightleftarrows \mathbb{S}^{\text{fin}} \longrightarrow \mathbb{S}$$

Furthermore, we want these functors to play well with fibred structures above Mealy and $\mathbb{S}^{\text{fin}}$: the internal structure of $\mathbb{S}^{\text{fin}}$ will allow to define a restriction $\mathfrak{Dial}^{\blacktriangleright}$ for fibrations over $\mathbb{S}^{\text{fin}}$, which we then want to convert to a construction over fibrations over Mealy. This latest informal requirement leads us to consider the so-called *Karoubi envelope* Kar(Mealy) of Mealy. After defining Karoubi-envelope for an arbitrary category in a concrete manner, we argue that they play nice with fibrations possessing a notion of equality. We then define $\mathbb{S}^{\text{fin}}$ and show that it is a full subcategory of Kar(Mealy).

Karoubi envelopes Here we give the basic definition of the Karoubi envelope $\mathrm{Kar}(\mathbb{C})$ of a category $\mathbb{C}$, sometimes called the Karoubi-completion[10]. This generic construction enriches the

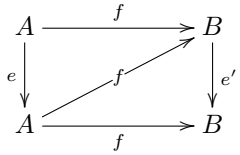
[1] In that article, MSO(M) roughly correspond to FOM,LMSO to LSFOM and LMSO($\mathfrak{C}$) to LSFOM^{+}.

category $\mathbb{C}$ with new objects so that *every idempotent splits*; this is in fact the "smallest" such category in a precise sense and $\mathrm{Kar}(-)$ should be seen as a closure operator over $\mathfrak{Cat}$. The general properties of the Karoubi envelope do not really concern us too much as we are only interested[2] in adding certain objects to Mealy corresponding to the $\blacktriangleright$ operator of $\mathbb{S}$. Therefore, we only define the basic construction of $\mathrm{Kar}(-)$.

Definition 7.1.1. *Let $\mathbb{C}$ be a category. An* idempotent *of $\mathbb{C}$ is a morphism $e : B \to B$ of $\mathbb{C}$ such that $e \circ e = e$. A* section-retraction pair *$(s, r) : A \to B$ is a pair of morphisms $s : A \to B$ (the section) and $r : B \to A$ (the retraction) such that $r \circ s = \mathrm{id}_A$. The idempotent e is said to be* split *if there exists a section-retraction pair (s, r) such that $s \circ r = e$.*

Definition 7.1.2. *Let $\mathbb{C}$ be a category. The* Karoubi envelope $\mathrm{Kar}(\mathbb{C})$ *is the category defined as follows:*

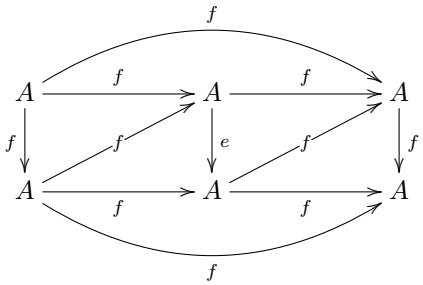
- **Objects:** *the objects are pairs (A, e) consisting of an object A of $\mathbb{C}$ and an idempotent $e : A \to A$.*
- **Morphisms:** *a morphism from $e : A \to A$ to $e' : B \to B$ is a morphism $f : A \to B$ such that $f \circ e = f = e' \circ f$.*



The identity over $e : A \to A$ is e itself and composition is the composition in $\mathbb{C}$.

For each category $\mathbb{C}$ There is an obvious full and faithful inclusion functor $I : \mathbb{C} \to \mathrm{Kar}(\mathbb{C})$, sending an object A to the pair (A, id_A). However, there is in general no obvious functor going the other way around.

Remark. *In $\mathrm{Kar}(\mathbb{C})$, all idempotents split as advertised. If $f : (A, e) \to (A, e)$ is an idempotent of $\mathrm{Kar}(\mathbb{C})$, then f is an idempotent in $\mathbb{C}$ and (A, f) an object of $\mathrm{Kar}(\mathbb{C})$. Then, (f, f) is a section-retraction pair between (A, e) and (A, f) in $\mathrm{Kar}(\mathbb{C})$ as seen from the commutative diagram below.*



The outer triangles commute because f is idempotent and the inner triangles commute because f is a morphism $e \to e$.

Let us also remark that if $\mathbb{C}$ has cartesian products and a terminal object, so does $\mathrm{Kar}(\mathbb{C})$. The terminal object object of $\mathrm{Kar}(\mathbb{C})$ is the unique map $! : 1 \to 1$ in $\mathbb{C}$. Given two idempotents $e : A \to A$ and $f : B \to B$, the cartesian product is given by the componentwise $e \times f : A \times B \to A \times B$, with $e \circ \pi_1 : e \times f \to e$ and $f \circ \pi_2 : e \times f \to f$ as first and second projections in $\mathrm{Kar}(\mathbb{C})$.

Fibrations over $\mathbb{C}$ and $\mathrm{Kar}(\mathbb{C})$. We now briefly discuss how to move between fibrations over $\mathbb{C}$ and $\mathrm{Kar}(\mathbb{C})$. Given a fibration $p : \mathbb{E} \to \mathrm{Kar}(\mathbb{C})$, we shall consider the change of base $I^*(p)$ along the inclusion $I : \mathbb{C} \to \mathrm{Kar}(\mathbb{C})$. This case amounts to asking that the predicates of $I^*(p)$ be those of p who may only range over objects of $\mathbb{C}$. It is rather obvious that most logical properties and structure of p such as monoidal closure and quantification are preserved when going to $I^*(p)$.

Turning a fibration $p : \mathbb{E} \to \mathbb{C}$ into a reasonable fibration over $\mathrm{Kar}(\mathbb{C})$ is a bit more involved. The basic idea is that the predicate φ of the new fibration $\mathrm{Kar}(p)$ over an object (A, e) of $\mathrm{Kar}(\mathbb{C})$ should be only considered up-to substitution by e. Therefore, a vertical morphism $\varphi \to \psi$ over e in $\mathrm{Kar}(p)$ should be thought of as a morphism $e^*\varphi \to e^*\psi$. For completeness' sake, we first give a definition which does not reference any cleavage of p.

[2] Another (equivalent) presentation of the Karoubi construction is also given in [3], where the property of splitting idempotent is not the main issue. Similar to our case, this construction is a simple way of adding certain subobjects to a category.

Definition 7.1.3. *Given $p : \mathbb{E} \to \mathbb{C}$, define a functor* $\mathrm{Kar}(p) : \mathbb{E}' \to \mathrm{Kar}(\mathbb{C})$*, with* $\mathbb{E}'$ *defined as follows:*

- **Objects:** *cartesian morphisms $\alpha : \varphi \to \varphi'$ such that $p(\alpha)$ is idempotent in $\mathbb{C}$.*
- **Morphisms:** *$\mathbb{E}'$-morphisms from $\alpha : \varphi \to \varphi'$ to $\beta : \psi \to \psi'$ are $\mathbb{E}$-morphisms $\varphi \to \psi$. Composition is the same as in $\mathcal{E}$*

The functor $\mathrm{Kar}(p)$ *is then defined as follows: for a $\mathbb{E}'$-object,* $\mathrm{Kar}(p)(\alpha) = p(\alpha)$*, and for a morphism $\gamma : \mathrm{dom}(\alpha) \to \mathrm{dom}(\beta)$, we take* $\mathrm{Kar}(p)(\gamma) = p(\beta) \circ p(\gamma) \circ p(\alpha)$*.*

In essence, an object $\alpha : \varphi \to \varphi'$ of $\mathbb{E}'$ should be understood as a substitution of the underlying idempotent into the formula φ. In logical terms, when reasoning internally to $\mathrm{Kar}(p)$ about a predicate $\varphi(x)$ over some idempotent e, one is reasoning about $\varphi(e(x))$ in p.

Lemma 7.1.4. $\mathrm{Kar}(p)$ *is a fibration.*

Proof. Let $e : A \to A$ and $e' : B \to B$ be two objects of $\mathrm{Kar}(\mathbb{C})$, $f : e \to e'$ a morphism of $\mathrm{Kar}(\mathbb{C})$ and $\alpha : \varphi \to \varphi'$ a p-cartesian morphism above e'. Since p is a fibration, let $\gamma : \psi' \to \varphi$ be a p-cartesian morphism above f and $\beta : \psi \to \psi'$ a p-cartesian morphism above e. Then $\gamma \circ \beta : \beta \to \alpha$ is p-cartesian by Lemma 5.2.3. It is then straightforward to check that $\gamma \circ \beta$ is also $\mathrm{Kar}(p)$-cartesian. □

Note that if we have a cleavage, a pair (e, φ) consisting of an object $e : A \to A$ of $\mathrm{Kar}(\mathbb{C})$ and a p-predicate φ over A can be regarded as the lift of e with target φ; furthermore, all objects of $\mathbb{E}'$ are vertically isomorphic to such objects. In presence of cleavage determining the substitution functors, one may rather adopt the following definition.

Definition 7.1.5. *Given $p : \mathbb{E} \to \mathbb{C}$, define a fibration* $\mathrm{Kar}(p) : \mathbb{E}' \to \mathrm{Kar}(\mathbb{C})$*, with* $\mathbb{E}'$ *defined as follows:*

- **Objects:** *pairs (e, φ) such that $e : A \to A$ is an idempotent of $\mathbb{C}$ and $p(\varphi) = A$.*
- **Morphisms:** *$\mathbb{E}'$-morphisms from (e, φ) to (f, ψ) are $\mathbb{E}$-morphisms $e^*\varphi \to f^*\psi$. Composition is the same as in $\mathbb{E}$.*

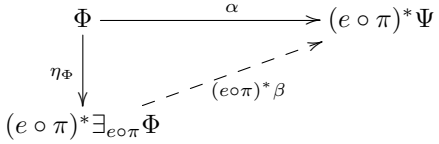
The functor $\mathrm{Kar}(p)$ *is then defined as follows: for a $\mathbb{E}'$-object,* $\mathrm{Kar}(p)(e, \varphi) = e$*, and for a morphism $\gamma : \mathrm{dom}(\alpha) \to \mathrm{dom}(\beta)$, we take* $\mathrm{Kar}(p)(\gamma) = p(\beta) \circ p(\gamma) \circ p(\alpha)$*.*

The definition of fibred functor generalizes to pairs of functors for fibrations over different bases: given two fibration $p : \mathbb{E} \to \mathbb{C}$ and $q : \mathbb{E}' \to \mathbb{C}'$, a morphism form p to q is a pair (F, G) such that F is a functor $\mathbb{C} \to \mathbb{C}'$ and G a functor $\mathbb{E} \to \mathbb{E}'$ such that $F \circ p = q \circ G$ and G sends p-cartesian morphisms to q-cartesian morphisms. According to this definition, there is such a pair of functors from $p : \mathbb{E} \to \mathbb{C}$ to $\mathrm{Kar}(p)$: the first component is given by the embedding $I : \mathbb{C} \to \mathrm{Kar}(\mathbb{C})$ and the second functor simply sends the object φ of $\mathbb{E}$ to (id, φ) in $\mathbb{E}^*$ and applies the functor id^* on arrows.

Later on, we are only interested in this construction for a fibration posetal p, namely, the syntactical fibration associated to FOM. In that case, this fibred inclusion preserves the logical structure that p carries, such as the monoidal closure, equalities, the exponentials and the simple quantifications. Although we have not checked the details, we conjecture the same holds for non-posetal fibrations. We treat the simple sums and leave checking the rest of the construction to the interested reader.

Lemma 7.1.6. *Suppose $\mathbb{C}$ has cartesian products and that $p : \mathbb{E} \to \mathbb{C}$ is a posetal fibration with simple sums. Then, so does* $\mathrm{Kar}(p)$*.*

Proof. Let A and B be objects of $\mathbb{C}$, $\pi : A \times B \to A$ a projection in $\mathbb{C}$, $e : A \to A$ and $e' : B \to B$ be idempotents of $\mathbb{C}$. We first prove that the substitution functor $(e \circ \pi)^* : \mathrm{Kar}(p)_e \to \mathrm{Kar}(p)_{e \times f}$ has a left adjoint $\exists_{e \circ \pi}$. To this end, in the general case, we would need to show that for every object $\Phi = (e \times f, \varphi)$ of $\mathrm{Kar}(p)_{e \times f}$, there is an object $\exists_{e \circ \pi}\Phi$ and a map $\eta_\Phi : \Phi \to (e \circ \pi)^* \exists_{e \circ \pi}\Phi$ such that, for every object Ψ of $\mathrm{Kar}(p)_e$ and map $\alpha : \Phi \to \pi^*\Psi$, there is a (unique) β such that the following commutes



We take $\exists_{e\circ\pi}\Phi = (e, \exists_\pi(e\times f)^*\varphi)$. Then, translating the above diagram in p and recalling it is posetal, it means that we have a map $\alpha : (e\times f)^*\varphi \to (e\times f)^*(e\circ\pi)^*\psi$ and that we should exhibit a map $\beta : e^*\exists_\pi(e\times f)^*\varphi \to e^*\psi$. By the general properties of fibrations, we have $(e\times f)^*(e\circ\pi)^*\psi \cong \pi^*e^*\psi$ and, using the Beck-Chevalley property in p, $e^*\exists_\pi(e\times f)^*\varphi \cong \exists_\pi(e\times f)^*\varphi$. Furthermore, since p has simple sums, α postcomposed by the first isomorphisms yield a map $\widetilde{\beta} : \exists_\pi(e\times f)^*\varphi \to e^*\psi$. We may then conclude by precomposing by the second isomorphism.

Thus far, we have shown that all substitution functors associated with a projection $(e\circ\pi)^*$ have a left adjoint $\exists_{e\circ\pi}$. Now it remains to show that the Beck-Chevalley property holds for them. To this end, let $e' : A' \to A'$ be another idempotent, $g : A \to A'$ a morphism from e to e' in $\mathrm{Kar}(\mathbb{C})$ and consider the pullback square in $\mathrm{Kar}(\mathbb{C})$

$$\begin{array}{ccc} e\times f & \xrightarrow{e\circ\pi} & e \\ {\scriptstyle g\times\mathrm{id}}\downarrow & & \downarrow{\scriptstyle g} \\ e'\times f & \xrightarrow{e'\circ\pi} & e' \end{array}$$

We need to show that for every object $\Phi = (e'\times f, \varphi)$, we have a vertical map

$$g^*\exists_{e'\circ\pi}\Phi \;\to\; \exists_{e\circ\pi}(g\times\mathrm{id})^*\Phi$$

in $\mathrm{Kar}(p)$. It means having a suitable map

$$e^*g^*\exists_\pi(e'\times f)^*\varphi \;\to\; e^*\exists_\pi(e\times f)^*(g\times\mathrm{id})^*\varphi$$

Using the equality $g\circ e = g$ and the pseudo-functoriality of substitution, this amounts to having a map

$$g^*\exists_\pi(e'\times f)^*\varphi \;\to\; e^*\exists_\pi(g\times f)^*\varphi$$

Then, using the Beck-Chevalley property in p on both sides and pseudo-functoriality of substitution with the additional equality $e'\circ g = g$, it suffices to have a map

$$\exists_\pi(g\times f)^*\varphi \;\to\; \exists_\pi(g\times f)^*\varphi$$

which is given by the identity. □

An exponential-free fragment of $\mathbb{S}$ The major issue that prevents us from applying the $\mathfrak{Dial}^{\blacktriangleright}$ construction to the logic FOM and recover a FOFIMELL-fibration is the lack of exponentials, that is, of λ-abstraction and application in the term language. However, the bare $\mathfrak{Dial}^{\blacktriangleright}$ without the unrestricted exponentials ! and ? does not use the internal homsets in the base $\mathbb{S}$. We thus define inductively a subcategory $\mathbb{S}^{\mathrm{fin}}$ of $\mathbb{S}$ which has enough objects and morphisms to carry out the $\mathfrak{Dial}^{\blacktriangleright}$ construction.

Definition 7.1.7. *Call $\mathbb{S}^{\mathrm{fin}}$ the subcategory of $\mathbb{S}$ whose objects and morphisms are inductively generated from the syntax of Figure 7.1.*

As a subcategory of $\mathbb{S}$, $\mathbb{S}^{\mathrm{fin}}$ also has chosen cartesian products, the parametric fixpoint combinator featured in Corollary 6.1.6 and the notion of pointwise exponentials that still satisfies the universal property of Lemma 6.1.8. It therefore contains all of the features of $\mathbb{S}$ used in defining $\mathfrak{Dial}^{\blacktriangleright}$, except the internal homsets. In order to interpret FOM in the classical fibration of global objects over $\mathbb{S}^{\mathrm{fin}}$, it suffices to show that we can embed the category Mealy of alphabets and f.s. synchronous functions in $\mathbb{S}^{\mathrm{fin}}$.

Lemma 7.1.8. *There is a faithful functor*[3] $J : \mathsf{Mealy} \to \mathbb{S}^{\mathrm{fin}}$.

Proof. Given that composition and pointwise lifting of functions over alphabets are part of the syntax of $\mathbb{S}^{\mathrm{fin}}$, the discussion in Subsection 2.1.2 show that we mostly need to need to show that the fixpoint operator $\mathbf{fix}_b$ of Mealy is encodable in $\mathbb{S}^{\mathrm{fin}}$. To do so, consider a morphism $f : \Sigma^\omega\times\Gamma^\omega \to \Gamma^\omega$ and $b\in\Gamma$. In $\mathbb{S}^{\mathrm{fin}}$, consider the composite $\widetilde{f}$

$$\widetilde{f} : \Sigma^\omega\times \blacktriangleright(\Gamma^\Gamma)^\omega \xrightarrow{\mathrm{id}\times(\mathrm{ev}(-,b))^\omega} \Sigma^\omega\times\blacktriangleright\Gamma^\omega \xrightarrow{\Lambda_{\multimap}(f)} (\Gamma^\Gamma)^\omega$$

Then it is straightforward to see that $\mathbf{fix}_b(f)$ in Mealy and $(\mathrm{ev}(-,b))^\omega\circ\mathbf{fix}(\widetilde{f})$ in $\mathbb{S}^{\mathrm{fin}}$ implement the same underlying functions in $\mathbb{S}$. To define formally J over morphisms, one may thus exploit this translation of $\mathbf{fix}_b$ in $\mathbb{S}^{\mathrm{fin}}$ and the normal form given in Lemma 2.1.11. □

[3] J will turn out to be full.

Objects

$$A, B, \cdots ::= 1 \mid A \times B \mid \Sigma^\omega \mid \blacktriangleright A \mid A \multimap B \qquad \text{with } \Sigma \in \mathbf{FinSet}$$

Morphisms

$$\frac{}{\mathrm{id} : A \to A} \qquad \frac{f : A \to B \qquad g : B \to C}{g \circ f : A \to C}$$

$$\frac{f : \Sigma \to \Gamma \qquad \text{in } \mathbf{FinSet}}{f^\omega : \Sigma^\omega \to \Gamma^\omega}$$

$$\frac{f : A \to B \qquad g : A \to C}{\langle f, g \rangle : A \to B \times C} \qquad \frac{}{\pi_i : A_1 \times A_2 \to A_i}$$

$$\frac{}{\mathrm{next} : A \to \blacktriangleright A} \qquad \frac{f : A \times \blacktriangleright B \to B}{\mathbf{fix}(f) : A \to B}$$

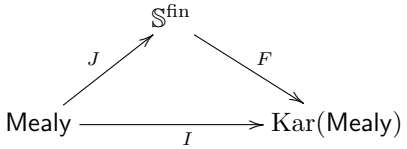
$$\frac{}{\mathbf{dist}_{\blacktriangleright,\times} : \blacktriangleright (A \times B) \to \blacktriangleright A \times \blacktriangleright B} \qquad \frac{}{\mathbf{dist}^{-1}_{\blacktriangleright,\times} : \blacktriangleright A \times \blacktriangleright B \to \blacktriangleright (A \times B)}$$

$$\frac{}{\mathrm{ev}_{\multimap} : (A \multimap B) \times A \to B} \qquad \frac{f : A \times B \to C}{\Lambda_{\multimap}(f) : A \times \blacktriangleright B \to B \multimap C}$$

Figure 7.1: An internal syntax for $\mathbb{S}^{\mathrm{fin}}$

Now, conversely, we need to show that $\mathbb{S}^{\mathrm{fin}}$ embeds into Kar(Mealy).

Lemma 7.1.9. *Conversely, there is a full and faithful functor $F : \mathbb{S}^{\mathrm{fin}} \to \mathrm{Kar}(\mathsf{Mealy})$ such that $I = F \circ J$.*



Proof. The functor F is not canonical, in the sense that it will rely on a choice of a default letter for each non-empty set A. Let us write $\epsilon(A) \in \Sigma$ for this choice. The definition of F is further complicated by the fact that the structure of the pointwise exponential $- \multimap -$ cannot be adequately represented in Kar(Mealy) in all generality, but only for objects coming from $\mathbb{S}^{\mathrm{fin}}$. The definition of F will thus occupy for the remainder of this section.

For objects, we have to define first an auxiliary map triple of maps $\langle G, \widetilde{s}, \widetilde{r} \rangle$ where

- $G : \mathbb{S}^{\mathrm{fin}}_0 \to \mathbf{FinSet}_0$ associate to every object of $\mathbb{S}^{\mathrm{fin}}$ a non-empty alphabet.
- A sequence of maps $\widetilde{s} : 1 \to A \multimap G(A)^\omega$ for all objects A of $\mathbb{S}^{\mathrm{fin}}$, henceforth seen as a sequence of maps $\widetilde{s}_{A,n} : A_n \to G(A)$.
- A $\mathbb{S}$-map $\widetilde{r} : 1 \to G(A)^\omega \multimap A$ for all objects A of $\mathbb{S}^{\mathrm{fin}}$, henceforth seen as a sequence of maps $\widetilde{r}_{A,n} : G(A) \to A_n$.

The basic idea is that $\widetilde{s}$ and $\widetilde{r}$ will then be regarded as section-retraction pair $A \to G(A)^\omega$, which shall ultimately yield an idempotent in Mealy. The definition of the triple goes by recursion over the object of $\mathbb{S}^{\mathrm{fin}}$:

- For an arbitrary alphabet Σ, we set $G_0(\Sigma^\omega) = \Sigma$ and $\widetilde{r}_{\Sigma^\omega} = \widetilde{s}_{\Sigma^\omega} = \widetilde{e}_{\Sigma^\omega}$ to be the constant word $\mathrm{id}^\omega \in (\Sigma^\Sigma)^\omega$.
- If we have $G(A) = \Sigma$ and $G(B) = \Gamma$, we set $G(A \multimap B) = \Gamma^\Sigma$ and

$$\widetilde{s}_{A \multimap B,n}(f) \;=\; \widetilde{s}_{B,n} \circ f \circ \widetilde{r}_{A,n} \qquad \widetilde{r}_{A \multimap B,n}(f) \;=\; \widetilde{r}_{B,n} \circ f \circ \widetilde{s}_{A,n} \qquad \widetilde{e}_{A \multimap B,n}(f) \;=\; \widetilde{e}_{B,n} \circ f \circ \widetilde{e}_{B,n}$$

- If we have $G(A) = \Sigma$ and $G(B) = \Gamma$, we set $G(A \times B) = \Sigma \times \Gamma$ and $\widetilde{s}, \widetilde{r}$ and $\widetilde{e}$ are obtained functorially.

- We set $G_0(\blacktriangleright A) = G_0(A)$. Setting $a = \epsilon(G_0(A))$, we then have

$$\begin{array}{llll} \widetilde{s}_{\blacktriangleright A,0}(*) &= a & \widetilde{r}_{\blacktriangleright A,0}(a') &= * \\ \widetilde{s}_{\blacktriangleright A,n+1} &= \widetilde{s}_{A,n} & \widetilde{r}_{\blacktriangleright A,n+1} &= \widetilde{r}_{A,n} \end{array} \qquad \widetilde{e}_{\blacktriangleright A,0}(a') = a \qquad \widetilde{e}_{\blacktriangleright A,n+1} = \widetilde{e}_A$$

By induction, we may easily check that, for every $n \in \mathbb{N}$, that the composite $\widetilde{r}_{A,n} \circ \widetilde{s}_{A,n}$ is equal to the identity. This implies that the word $(\widetilde{e}_{A,n})_{n\in\mathbb{N}} = (\widetilde{s}_{A,n} \circ \widetilde{e}_{A,n})_{n\in\mathbb{N}}$ only has idempotent letters. Then, one also checks that $\widetilde{e}_A$ is computable by a finite-state Mealy machine $\widetilde{e}_A : 1 \to (G(A)^{G(A)})^\omega$:

- if $A = \Sigma^\omega$, then e_A is constantly equal to the identity; therefore it is given by a single-state Mealy machine.
- if $A = B \twoheadrightarrow C$, $\widetilde{e}_A = m^\omega \circ \langle \widetilde{e}_B, \widetilde{e}_C \rangle$ where m is the function

$$\begin{array}{rlll} m : & G(B)^{G(B)} \times G(C)^{G(C)} & \to & (G(B) \times G(C))^{G(B)\times G(C)} \\ & (f, g) & \mapsto & f \times g \end{array}$$

  Note that in this case, it is crucial that we build some $\widetilde{e}_A : 1 \to (G(A)^{G(A)})^\omega$ rather than the corresponding idempotent $e_A : G(A)^\omega \to G(A)^\omega$.
- if $A = B \times C$, $\widetilde{e}_A = \widetilde{e}_B \times \widetilde{e}_C$ and we can conclude since Mealy has cartesian products.
- if $A = \blacktriangleright B$, then $e_A = \mathbf{cons}_{-\mapsto\epsilon(G(B))} \circ e_B$ and thus belongs to Mealy. Note that we need to use one more state to implement e_A from e_B.

At this juncture, we are almost ready to give F on objects. Note that the morphism ev_{-*} at object Σ^ω is the lifting ev^ω, where $\mathrm{ev} : \Sigma^\Sigma \times \Sigma$ is the evaluation map in **FinSet**. $F(A)$ on objects is then be given by the composite map e_A

$$G(A)^\omega \cong 1^\omega \times G(A)^\omega \xrightarrow{\widetilde{e}_A \times \mathrm{id}} (G(A)^{G(A)})^\omega \times G(A)^\omega \cong (G(A)^{G(A)} \times G(A))^\omega \xrightarrow{\mathrm{ev}^\omega} G(A)^\omega$$

which is easily seen to be finite-state an idempotent after the above discussion. The intermediate step through $\widetilde{e}$ is necessary because of the pointwise arrow $- \twoheadrightarrow -$, for which a direct inductive definition of F is not possible. The intuitive reason behind this is that, as mentioned in Remark 6.1, $- \twoheadrightarrow -$ is *not* functorial over $\mathbb{S}$ and cannot even be extended to $\mathrm{Kar}(\mathsf{Mealy})$ in a reasonable way.

Now, let us define F on morphisms. Some care is needed because of the inductive definition of $\mathbb{S}^{\mathrm{fin}}$: Figure 7.1 presents a syntax for $\mathbb{S}^{\mathrm{fin}}$, which is actually quotiented by the equalities arising from its interpretation in $\mathbb{S}$. To fix ideas, call (abusively) $[A, B]_{\mathbb{S}^{\mathrm{fin}-\mathrm{syn}}}$ the set of syntactic terms from object A to object B We first define a family of maps $H_{A,B} : [A, B]_{\mathbb{S}^{\mathrm{fin}-\mathrm{syn}}} \to [G(A), G(B)]_{\mathsf{Mealy}}$ by recursion over the syntax.

- H should preserve composition and identities, so $H(f \circ g) = H(f) \circ H(g)$ and $H(\mathrm{id}) = \mathrm{id}$.
- H is meant to preserve the cartesian product and all of the morphisms coming from the inclusion **FinSet**. Hence, we set

$$H(\langle f, g \rangle) = \langle H(f), H(g) \rangle \qquad H(f^\omega) = f^\omega$$

- next : $A \to \blacktriangleright A$ is mapped to the causal map $\mathbf{cons}_{\epsilon G_0(A)}$ in Mealy
- The maps $\mathbf{dist}_{\blacktriangleright,\times} : \blacktriangleright (A \times B) \to \blacktriangleright A \times \blacktriangleright B$ and $\mathbf{dist}_{\blacktriangleright,\times}$ are mapped to the identity *in* $\mathrm{Kar}(\mathsf{Mealy})$.
- If $f : A \times \blacktriangleright B \to B$ is a $\mathbb{S}^{\mathrm{fin}}$ map, $\mathbf{fix}(f) : A \to B$ is mapped to the causal map $\mathbf{fix}_{\epsilon(G_0(B))}(F(f))$.
- We set $H(\mathrm{ev}_{-*}) = \mathrm{ev}^\omega$, that is, the image evaluation map of **FinSet** by the inclusion **FinSet** $\to \mathsf{Mealy}$.
- Finally, suppose that we have a map $f : A \times B \to C$ for which $H(f)$ is already defined to be induced by a finite-state machine

$$\mathcal{M} = (Q, q^\iota, \partial) : \Sigma^\omega \times \Gamma^\omega \to \Theta^\omega$$

where $G(A) = \Sigma$, $G(B) = \Gamma$ and $G(C) = \Theta$. We define $H(\Lambda_{-*}(f))$ to be the causal function induced by the following Mealy machine:

$$\mathcal{M}' = (1 + Q \times \Gamma, \mathsf{inl}(*), \partial') : \Sigma^\omega \times \Gamma^\omega \to (\Theta^\Gamma)^\omega$$

where

$$\begin{array}{lcl} \pi_1(\partial'((a,b),\mathsf{inl}(*)))(b') & = & \pi_1(\partial((a,b'),q^\iota)) \\ \pi_1(\partial'((a,b),\mathsf{inr}(q,b'))) & = & \pi_1(\partial((a,b''),\pi_2(\partial((a,b'),q)))) \\ \pi_2(\partial'((a,b),\mathsf{inl}(*))) & = & \mathsf{inr}(q^\iota, b) \\ \pi_2(\partial'((a,b),\mathsf{inr}(q,b'))) & = & \mathsf{inr}(\pi_2(\partial((a,b'),q)), b) \end{array}$$

Writing $[\![-]\!]$ for the family of maps $[A,B]_{\mathbb{S}^{\mathrm{fin-syn}}} \to [A,B]_{\mathbb{S}^{\mathrm{fin}}}$, the map H extends F to a functor if we show that:

- H is functorial: for any pair of terms $(f,g) \in [A,B]_{\mathbb{S}^{\mathrm{fin-syn}}} \times [B,C]_{\mathbb{S}^{\mathrm{fin-syn}}}$, we have

$$H(g \circ f) = H(g) \circ H(f) \qquad\qquad H(\mathrm{id}) = \mathrm{id}$$

- H is compatible with the quotient $[\![-]\!]$: for every pair of terms $f, g \in [A,B]_{\mathbb{S}^{\mathrm{fin-syn}}}$

$$[\![f]\!] = [\![g]\!] \;\Rightarrow\; H(f) = H(g)$$

- H sends terms to morphisms in Kar(Mealy): for every $f \in [A,B]_{\mathbb{S}^{\mathrm{fin-syn}}}$,

$$e_B \circ H(f) = H(f) = H(f) \circ e_A$$

The functoriality is obvious by definition of H. The latter two claims derive from the following equality in $\mathbb{S}$ for every $f \in [A,B]_{\mathbb{S}^{\mathrm{fin-syn}}}$:

$$H(f) \;=\; s_B \circ I([\![f]\!]) \circ r_A$$

which is proven by an easy induction on the structure of f. The first claim is then immediate and the second follows from the equalities $e_A = s_A \circ r_A$ and $r_A \circ s_A = \mathrm{id}$.

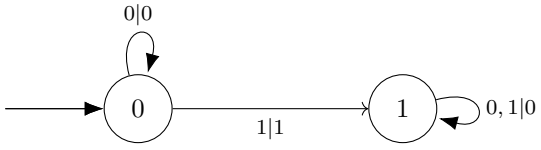
Finally, it is straightforward to check that $F \circ J = I$: on objects, it maps the alphabet Σ is mapped by the identity on Σ^ω on both sides. On morphisms, this follows from $\square$

The above proof is necessarily a bit tedious; while we use Kar(Mealy) as a convenient category to embed $\mathbb{S}^{\mathrm{fin}}$, it should once again be stressed that, as for the more convenient topos of trees $\mathbb{T}$ with respect to $\mathbb{S}$, there is no suitable notion of pointwise arrow $- \multimap -$ definable over Kar(Mealy). Regarding all of these categories as subcategories of $\mathbb{T}$, it is in fact easy to check that Kar(Mealy) has objects which are not members of $\mathbb{S}$, even up to isomorphism.

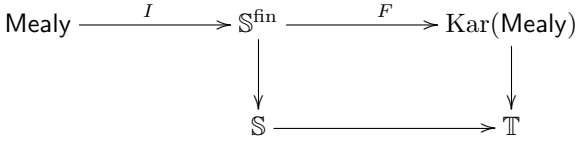
Example 7.1.10. *The unique object (up to isomorphism) $\mathbb{N}_\infty$ of $\mathbb{T}$ characterized by*

$$\mathbb{N}_\infty \cong 1 + \blacktriangleright \mathbb{N}_\infty$$

can be seen as the subobject of 2^ω defined as the codomain of an idempotent $2^\omega \to 2^\omega$ defined through the following finite-state machine



To sum up, we have the following diagram in $\mathfrak{Cat}$ where the vertical arrows are faithful functors and horizontal arrows are full and faithful; this reflects that the first row corresponds morally to f.s. causal functions while the second lifts the finite-state restriction.



7.2 Restricting the translation $\mathfrak{Dial}^{\blacktriangleright}$ to Mealy

With the discussion of the previous section, we are now ready to discuss how to build a FOFIMLL-fibration over the category Mealy provided an arbitrary boolean fibration $p : \mathbb{E} \to \mathsf{Mealy}$. For our purpose, it is helpful to think of p as arising from either the syntactic fibration of FOM, or the standard model as described in Example 5.2.12.

The first step is to move from p to a fibration over $\mathbb{S}^{\mathrm{fin}}$. This can be done in two steps: first by considering $\mathrm{Kar}(p)$, which is a fibration over $\mathrm{Kar}(\mathsf{Mealy})$ and then by change of base along the inclusion functor $F : \mathbb{S}^{\mathrm{fin}} \to \mathrm{Kar}(\mathsf{Mealy})$ defined in Lemma 7.1.9. Call the fibration thus obtained $\overline{p} := F^*(\mathrm{Kar}(p))$. Then one can consider a variant of the $\mathfrak{Dial}^{\blacktriangleright}$ construction which operates on fibrations over $\mathbb{S}^{\mathrm{fin}}$. To do so, first notice that while object and strategies of DZ are made up of general $\mathbb{S}$-morphisms and objects as per Definition 6.2.1, there is no harm in restricting to $\mathbb{S}^{\mathrm{fin}}$ for the whole technical development up until Lemmas 6.2.4 and 6.2.5. This is reasonable as those Lemmas are concerned with full exponentials, which we do not expect to have. Call $\mathsf{DZ}_{\mathrm{fin}}$ this category of zigzag games with finite-memory strategies. Using the definition of $\mathsf{DZ}_{\mathrm{fin}}$ instead of DZ, one may similarly alter the definition of indexed zigzag games (Definition 6.2.8) and the general $\mathfrak{Dial}^{\blacktriangleright}$ construction (Definition 6.2.9). Similarly, call $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}$ the expected construction for fibrations over $\mathbb{S}^{\mathrm{fin}}$. To finally obtain a fibration over Mealy, we may use the change of base along the functor $J : \mathsf{Mealy} \to \mathbb{S}^{\mathrm{fin}}$ (Lemma 7.1.8) to obtain the fibration $J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))$. This chain of transformations is summarized in the following picture.

$$\begin{array}{ccccccccc}
\mathbb{E} & & \mathbb{E}' & & \mathbb{E}'' & & \mathbb{E}''' & & \mathbb{E}'''' \\
\downarrow{\scriptstyle p} & \longmapsto & \downarrow{\scriptstyle \mathrm{Kar}(p)} & \longmapsto & \downarrow{\scriptstyle \overline{p}} & \longmapsto & \downarrow{\scriptstyle \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})} & \longmapsto & \downarrow{\scriptstyle J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))} \\
\mathsf{Mealy} & & \mathrm{Kar}(\mathsf{Mealy}) & & \mathbb{S}^{\mathrm{fin}} & & \mathbb{S}^{\mathrm{fin}} & & \mathsf{Mealy}
\end{array}$$

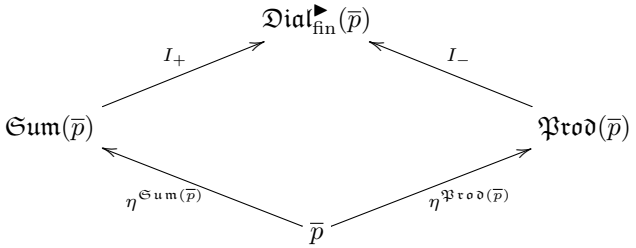
As mentioned above, it is rather straightforward to check that most of these maps preserve the logical structure of the various fibrations involved, save for the middle map $\overline{p} \mapsto \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$.

Assuming that $\overline{p}$ is a boolean, cartesian-closed fibration with equalities and simple quantifications. In particular, $(\overline{p}, \overline{p}, \overline{p})$ certainly has a structure of FOFIMELL-fibration where we take $\otimes$ to be the classical conjunction $\wedge$ (the fiberwise product in $\overline{p}$), $\parr$ to be the classical disjunction $\vee$ (the fiberwise coproduct in $\overline{p}$) and the fibred functors $\overline{p} \to \overline{p}$ part of the adjunctions defining ! and ? to be the identities. While Theorem 6.2.15 fails to apply, one can adapt Lemmas 6.2.14, 6.2.13, 6.2.12 and 6.2.11 to $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$ as those do not make use of the internal homsets of $\mathbb{S}$. This may be summarized in the following statement.

Lemma 7.2.1. *The fibration* $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$

- *has symmetric monoidal products* $\otimes$ *and* $\parr$ *with a distribution law* $\Phi \otimes (\Psi \parr \Theta) \to (\Phi \otimes \Psi) \parr \Theta$.
- *is monoidal closed with respect to* $\otimes$.
- *has simple quantifications* $\forall_\pi$ *and* $\exists_\pi$.
- *has equalities* $\exists_{\delta \times \mathrm{id}}$.

This accounts for the logical rules of LSFOM coming from full intuitionistic multiplicative linear logic and first-order quantifications. The crucial difference with the higher-order setting is that, while we still have fibred inclusion functors $I_+ : \mathfrak{Sum}(\overline{p}) \to \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$ and $I_- : \mathfrak{Prod}(\overline{p}) \to \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$, they do not admit adjoints allowing to interpret the exponential modalities over all $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$-predicates. However, as the naming of the inclusion functors suggest, those fibrations are tied to the polarity system of LSFOM. To take full advantage of this correspondence, let us recall that we also have inclusion functors $\eta^{\mathfrak{Sum}(\overline{p})} : \overline{p} \to \mathfrak{Sum}(\overline{p})$ (first defined in Section 5.3) and $\eta^{\mathfrak{Prod}(\overline{p})} : \overline{p} \to \mathfrak{Prod}(\overline{p})$ sitting in the following commuting diagram in $\mathfrak{Fib}(\mathbb{S}^{\mathrm{fin}})$.



The intuition here is that the polarity of a formula of LSFOM will be ultimately interpreted

- as a $\overline{p}$-predicate if it is deterministic.

- as a $\mathfrak{Sum}(\overline{p})$-predicate if it is positive.

- as a $\mathfrak{Prod}(\overline{p})$-predicate if it is negative.

Ultimately, all these predicates can thus be interpreted as $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$-predicates thanks to the embeddings. However, the main purpose of this diagram is to account for the stabilities of positive/negative/deterministic predicates under various connectives and the definition of the restricted exponential modalities.

For the second aspect, the restricted exponential modality $? : \mathfrak{Sum}(\overline{p}) \to \mathfrak{Sum}(\overline{p})$ arise from the adjunction $\eta^{\mathfrak{Sum}(p)} \dashv \exists^{\overline{p}}$ outlined in Lemma 5.3.8. It remains to be checked that $\exists^{\overline{p}} : (\mathfrak{Sum}(\overline{p}), \parr, \bot) \to (\overline{p}, \vee, \bot)$ is oplax monoidal. Recalling that $\overline{p}$ is necessarily preposetal (so we do not have to care about coherence issues), this amounts to checking that for arbitrary FOM predicates $\varphi(a^A, u^U)$ and $\psi(a^A, u^V)$, we have

$$(\exists u^U.\varphi(a,u)) \ \vee \ (\exists v^V.\psi(a,v)) \quad \Rightarrow \quad \exists (u,v)^{U\times V}.\varphi(a,u) \vee \psi(a,v)$$

Thankfully, this always hold because the interpretation of every object of $\mathbb{S}^{\mathrm{fin}}$, and a fortiori U and V, are non-empty (i.e., there exists concrete morphisms $1 \to A$ for every object A of $\mathbb{S}^{\mathrm{fin}}$). Dually, it can also be shown that the adjunction $\forall^{\overline{p}} \dashv \eta^{\mathfrak{Prod}(\overline{p})}$ can be enriched to a LNL-adjunction as $\forall^{\overline{p}} : (\mathfrak{Prod}(\overline{p}), \otimes, \mathbf{I}) \to (\overline{p}, \wedge, 1)$ is lax monoidal. It should be stressed that it is only because the base $\mathbb{S}^{\mathrm{fin}}$ has no non-empty sets of global objects that the maps making $\exists^{\overline{p}}$ and $\forall^{\overline{p}}$ respectively oplax and lax monoidal may be defined at all, and that the associated coherence comes down to $\overline{p}$ being posetal; either of these requirements is atypical when studying general fibrations.

Finally the stability under polarized connectives of the three subfibrations can be obtained as straightforward computations, keeping in mind that an object $(a : A, u : U, x : X, \varphi(a,u,x))$ is equivalent to

- some $I_+(\Phi)$ if $X \simeq 1$.

- some $I_-(\Phi)$ if $U \simeq 1$.

- some $I_+(\eta^{\mathfrak{Sum}(\overline{p})}(\Phi)) = I_-(\eta^{\mathfrak{Prod}(\overline{p})}(\Phi))$ if $U \simeq X \simeq 1$.

However, it is also interesting to note that this connectives also live at the level of the subfibration $\overline{p}, \mathfrak{Sum}(\overline{p})$ and $\mathfrak{Prod}(\overline{p})$ without necessarily needing to mention $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$.

- $\overline{p}$ features the propositional connectives $\wedge$, $\vee$ and $\Rightarrow$ which are interpreted as $\otimes$, $\parr$ and $\multimap$.

- $\mathfrak{Sum}(\overline{p})$ features the monoidal products $\otimes$ and $\parr$, as well as simple sums $\exists_\pi$.

- Dually, $\mathfrak{Prod}(\overline{p})$ has simple products $\forall_\pi$ in addition to the monoidal products $\otimes$ and $\parr$.

All of these connectives are preserved by the embedding functors $\eta^{\mathfrak{Sum}(\overline{p})}, \eta^{\mathfrak{Prod}(\overline{p})}, I_+$ and I_-. The only polarized connective which is not accounted for by this discussion is the linear arrow $\multimap$. At this juncture, it is only a functor $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})^{\mathrm{op}} \times \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}) \to \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$ which is readily seen to restrict to maps of objects $\mathfrak{Prod}(\overline{p})^{\mathrm{op}} \times \mathfrak{Sum}(\overline{p}) \to \mathfrak{Sum}(\overline{p})$ and $\mathfrak{Sum}(\overline{p})^{\mathrm{op}} \times \mathfrak{Prod}(\overline{p}) \to \mathfrak{Prod}(\overline{p})$. Contrary to the situation over $\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})$, there is no obvious characterization of these restrictions as right adjoints to $- \otimes \Phi$ due to a polarity mismatch. In this case, it is helpful to recall the decomposition of the arrow $\Phi \multimap \Psi \simeq (\Phi \multimap \bot) \parr \Psi$ of classical linear logic. While this isomorphism does not hold for full intuitionistic linear logic, this will for poralized predicates. At the level of semantics, this can be seen as arising from linear negation functors between $\mathfrak{Sum}(\overline{p})$ and $\mathfrak{Prod}(\overline{p})$.

Lemma 7.2.2. *Suppose that $\overline{p}$ is a boolean fibration. There are linear negation functors*

$$(-)^\perp \ : \ \mathfrak{Sum}(\overline{p}) \ \to \mathfrak{Prod}(\overline{p})^{\mathrm{op}} \qquad\qquad (-)^\perp \ : \ \mathfrak{Prod}(\overline{p}) \ \to \mathfrak{Sum}(\overline{p})^{\mathrm{op}}$$

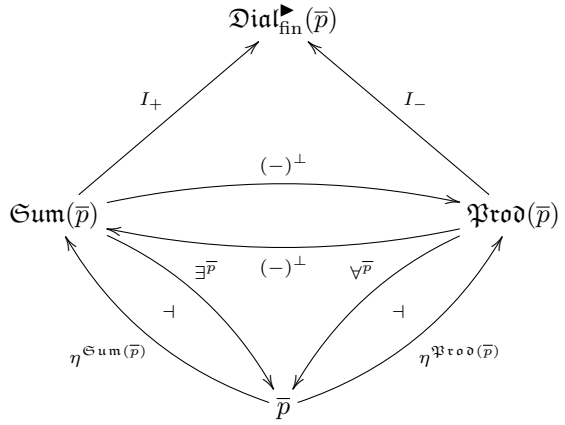
such that $(-)^\perp, ((-)^\perp)^{\mathrm{op}}$ are part of equivalence of categories between $\mathfrak{Sum}(\overline{p})$ and $\mathfrak{Prod}(\overline{p})$. Furthermore $I_+(\Phi^\perp) \simeq I_+(\Phi) \multimap \bot$ and $I_-(\Phi^\perp) \simeq I_-(\Phi) \multimap \bot$.

Proof. On objects, those functors are defined using by using the same objects for the witnesses/counterwitnesses and negating the $\overline{p}$ predicates. Similarly, morphisms, which are in all cases pairs (f, α) of some $\mathbb{S}^{\mathrm{fin}}$ map $f : A \times U \to V$ and some proof $\alpha : \varphi \to \psi$ in $\overline{p}$ see formally little changes: the first component stays the same and the second turns into a proof of the contrapositive $\neg\psi \to \neg\varphi$.

$$\begin{array}{rccc}
(-)^\perp : & \mathfrak{Sum}(\overline{p}) & \to & \mathfrak{Prod}(\overline{p})^{\mathrm{op}} \\
& (a : A, u : U, \varphi(a,u)) & \mapsto & (a : A, u : U, \neg\varphi(a,u)) \\
& \left(\begin{array}{c} f : A \times U \to V \\ \alpha : \varphi(a,u) \to \psi(a, f(a,u))) \end{array} \right) & \mapsto & \left(\begin{array}{c} f : A \times U \to V \\ \widetilde{\alpha} : \neg\psi(a, f(a,u)) \to \neg\varphi(a,u) \end{array} \right)
\end{array}$$

Then, it is fairly easy to check that $(a : A, u : U, \varphi(a,u))^{\perp\perp} = (a : A, u : U, \neg\neg\varphi(a,u))$, and since $\overline{p}$ is boolean, there is a unique isomorphism $\neg\neg\varphi(a,u) \simeq \varphi(a,u)$ making both pairs $((-)^{\perp}, ((-)^{\perp})^{\mathrm{op}})$ part of equivalence of fibrations. □

With these functors, we can recover the polarized linear arrows (up to isomorphism) by considering the functor $(-)^{\perp} \parr - : \mathfrak{Prod}(\overline{p})^{\mathrm{op}} \times \mathfrak{Sum}(\overline{p}) \to \mathfrak{Sum}(\overline{p})$ and its dual. Summarizing the discussion above, we obtain the following functors, with the embeddings $I_+, I_-, \eta^{\mathfrak{Sum}(\overline{p})}$ and $\eta^{\mathfrak{Prod}(\overline{p})}$ preserve all the functors sharing the same notation (up to isomorphism).



$$
\begin{array}{lrcl}
-\otimes- \\ -\parr- : & \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})^2 & \to & \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}) \\
 & \mathfrak{Sum}(\overline{p})^2 & \to & \mathfrak{Sum}(\overline{p}) \\
 & \mathfrak{Prod}(\overline{p})^2 & \to & \mathfrak{Prod}(\overline{p}) \\
 & \overline{p}^2 & \to & \overline{p} \\
 & & & \\
- \multimap - : & \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})^{\mathrm{op}} \times \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}) & \to & \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}) \\
 & \mathfrak{Prod}(\overline{p})^{\mathrm{op}} \times \mathfrak{Sum}(\overline{p}) & \to & \mathfrak{Sum}(\overline{p}) \\
 & \mathfrak{Sum}(\overline{p})^{\mathrm{op}} \times \mathfrak{Prod}(\overline{p}) & \to & \mathfrak{Prod}(\overline{p}) \\
 & \overline{p}^{\mathrm{op}} \times \overline{p} & \to & \overline{p} \\
 & & & \\
\exists_\pi : & \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})_{A\times B} & \to & \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})_{A} \\
 & \mathfrak{Sum}(\overline{p})_{A\times B} & \to & \mathfrak{Sum}(\overline{p})_{A} \\
 & & & \\
\forall_\pi : & \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})_{A\times B} & \to & \mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p})_{A} \\
 & \mathfrak{Prod}(\overline{p})_{A\times B} & \to & \mathfrak{Prod}(\overline{p})_{A}
\end{array}
$$

With this discussion, it is now rather straightforward to interpret LSFOM. Furthermore, all of the constructions presented here can be carried out very syntactically as we may pick the syntactic fibration of FOM as p to build $J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))$. To ground the discussion, let us mention that this can be seen as a purely syntactic translation. In this syntactic interpretation, a LSFOM formula $\varphi(a^{A^\omega})$ over alphabet A is mapped to a triple

- an alphabet U_φ of P-moves.
- an alphabet X_φ of O-moves.
- a FOM-formula $\varphi_D(u^{U_\varphi^\omega}, x^{X_\varphi^\omega}, a^{A^\omega})$ over alphabet $U_\varphi \times X_\varphi \times A$.

The precise mapping is given in Figure 7.2, where ev_{-*} is abusively used to denote term for a Mealy machine implementing $F(\mathrm{ev}_{-*})$ [4]. It should come as no surprise that this latest translation is but a restriction of the translation given in Figure 6.1, up to forgetting the linear structure via the map $\lfloor - \rfloor$. Now proofs of entailments between LSFOM formulas $\varphi(a) \to \psi(a)$ in $J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))$ can be regarded as pairs (f, F) of f.s. causal functions such that

$$\varphi_D(u, F(a,u,y), a) \vdash \psi_D(f(a, u, \mathbf{cons}_{\epsilon(Y)}(y)), y, a)$$

is derivable in FOM[5]. In particular, if φ and ψ are both deterministic, we have $\varphi_D = \lfloor \varphi \rfloor$ and $\psi_D = \lfloor \psi \rfloor$ by a straightforward induction and the entailment $\varphi \to \psi$ holds in $J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))$ if and only if $\varphi \vdash \psi$ is derivable in FOM. As all the additional axioms of LSFOM on top of polarized double linear negation elimination are deterministic and that their erasure correspond to FOM axioms, this establishes that the interpretation of Figure 6.1 is sound with respect to LSFOM. This is formalized through the following theorem.

Theorem 7.2.3. *If $\varphi(a) \vdash \psi(a)$ is derivable in* LSFOM*, then there exists a pair (f, F) of finite-state causal functions such that $\varphi_D(u, F(a,u,y), a) \vdash \psi_D(f(a, u, \mathbf{cons}_{\epsilon(Y)}(y)), y, a)$ is derivable in* FOM*.*

[4] There is little noise coming from the change of bases between $\mathbb{S}^{\mathrm{fin}}$ and Mealy. This may be explained by the fact that the $\blacktriangleright$ operator does not appear in the alphabets U_φ and X_φ, although it plays a crucial rule when interpreting the cut rules and proofs. This is why the direct definition of this interpretation given in [57] did not mention $\blacktriangleright$ for types but crucially used the notion of eagerness when discussing proofs.

[5] It should be noted that, officially, not all such $f : (A \times U \times Y)^\omega \to V^\omega$ may be part of a $J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))$-proof as they should be obtained as the image of some $\widetilde{f} : A^\omega \times U^\omega \times \blacktriangleright Y^\omega \to V^\omega$, meaning that we should have $f \circ (\mathrm{id} \times \mathrm{id} \times e_{\blacktriangleright Y^\omega}) = f$. However, as $e_{\blacktriangleright Y^\omega} \circ \mathbf{cons}_{\epsilon(Y)} = \mathrm{id}$ by definition, this is not a limiting factor as any pair (f, F) satisfying the entailment above may be safely replaced with $f \circ (\mathrm{id} \times \mathrm{id} \times e_{\blacktriangleright Y^\omega}, F)$

$$
\begin{array}{llll}
U_{\mathbf{I}} := U_{\bot} := U_{\mathtt{t}=\mathtt{u}} := X_{\mathbf{I}} := X_{\bot} := X_{\mathtt{t}=\mathtt{u}} := 1 & & & \\
U_{\varphi\otimes\psi} & := & U_{\varphi\parr\psi} := U_{\varphi} \times U_{\psi} & X_{\varphi\otimes\psi} := X_{\varphi\parr\psi} := X_{\varphi} \times X_{\psi} \\
U_{\varphi\multimap\psi} & := & U_{\psi}^{U_{\varphi}} \times X_{\varphi}^{U_{\varphi}\times X_{\psi}} & X_{\varphi\multimap\psi} := U_{\varphi} \times X_{\psi} \\
U_{\exists x^{B^\omega}.\varphi} & := & U_{\varphi} \times B & X_{\exists x^{B^\omega}.\varphi} := X_{\varphi} \\
U_{\forall x^{B^\omega}.\varphi} & := & U_{\varphi}^{B} & X_{\forall x^{B^\omega}.\varphi} := X_{\varphi} \times B \\
U_{!\varphi^-} & := & U_{\varphi^-} \ (\simeq 1) & X_{!\varphi^-} := 1 \\
U_{!\varphi^+} & := & U_{\varphi^+} & X_{!\varphi^+} := X_{\varphi^+} \ (\simeq 1) \\
U_{?\varphi^-} & := & U_{\varphi^-} \ (\simeq 1) & X_{?\varphi^-} := X_{\varphi^-} \\
U_{?\varphi^+} & := & 1 & X_{?\varphi^+} := X_{\varphi^+} \ (\simeq 1)
\end{array}
$$

$$
\begin{array}{rcl}
(\mathtt{t}(a) = \mathtt{u}(a))_D(*,*,a) & := & \mathtt{t}(a) = \mathtt{u}(a) \\
(\varphi \otimes \psi)_D((u,v),(x,y),a) & := & \varphi_D(u,x,a) \wedge \varphi_D(v,y,a) \\
(\varphi \parr \psi)_D((u,v),(x,y),a) & := & \varphi_D(u,x,a) \vee \varphi_D(v,y,a) \\
(\varphi \multimap \psi)_D((f,F),(u,y),a) & := & \varphi_D(u, \mathrm{ev}_{-*}(F,(u,y)),a) \Rightarrow \varphi_D(\mathrm{ev}_{-*}(f,u),y,a) \\
(\exists b.\varphi(a,b))_D((u,b),x,a) & := & \varphi_D(u,x,(a,b)) \\
(\forall b.\varphi(a,b))_D(f,x,a) & := & \varphi_D(\mathrm{ev}_{-*}(f,b),x,(a,b)) \\
(!\varphi^-)_D(*,*,a) & := & \forall x.\varphi_D^-(*,x,a) \\
(!\varphi^+)_D(u,*,a) & := & \varphi_D^+(u,xa) \\
(?\varphi^-)_D(*,x,a) & := & \varphi_D^-(*,x,a) \\
(?\varphi^+)_D(*,*,a) & := & \exists u.\varphi_D^+(u,*,a)
\end{array}
$$

Figure 7.2: The syntactic interpretation of LSFOM in FOM.

It should be stressed that the interpretation of proofs underlying Theorem 7.2.3 is computationally straightforward: terms for the pair of finite-state causal functions may be read off in linear time from the proof tree in LSFOM. Of course, one should also keep in mind that the state space of the underlying Mealy machine might not be linear in the size of the terms due to the use of pairing and composition.

If we are interested in realizing a single formula with no free variables, the statement of Theorem 7.2.3 may be simplified. In such a case, by taking the antecedent to be $\mathbf{I}$ and conclusion φ, the second component of the pair (f,F) is trivial while $f : X^\omega \to U^\omega$ must satisfy $\forall x^{X^\omega} \varphi_D(f(\mathbf{cons}_{\epsilon(X)}(x)),x)$. But this is equivalent to having an eager f.s. causal function $g : X^\omega \to U^\omega$ such that $\forall x^{X^\omega} \varphi_D(g(x),x)$: given f, g is obtained as $f \circ \mathbf{cons}_{\epsilon(X)}$ and conversely, for every eager g and letter $x \in X$ there exists f such that $g = f \circ \mathbf{cons}_x$. We therefore have the following:

Corollary 7.2.4. *For any* LSFOM *sentence* φ*, if* $\mathsf{LSFOM} \vdash \varphi$*, then there exists an eager f.s. function* $f : X_\varphi^\omega \to U_\varphi^\omega$ *such that* $\mathsf{FOM} \vdash \forall x.\varphi_D(f(x),x)$.

Theorem 7.2.3 is ultimately a syntactic version of Theorem 4.3.4, whose proof we had postponed; the latter is now easily derivable from the former by noticing that, for any LSFOM predicates $\varphi(a)$ and $\psi(a)$, we have $[\![\varphi(a)]\!] \Vdash [\![\psi(a)]\!]$ if and only if there exists a pair (f,F) of f.s. functions such that $\varphi_D(u,F(a,u,y),a) \vdash \psi_D(f(a,u,\mathbf{cons}_{\epsilon(Y)}(y),y,a)$; this is proven by induction over the syntax of φ and ψ by inspecting the translation into alternating uniform automata and FOM predicates. Let us also note that thanks to this syntactic Dialectica-like interpretation, we could have also derived soundness of LSFOM with respect to Church's synthesis (Lemma 4.3.6) without referring to the alternating automata model of Chapter 4.

7.3 A complete extension of LSFOM

Now, as advertised in the introduction, we leverage the characterization theorem proved in Chapter 6 to give an extension LSFOM^+ of LSFOM which is sound with respect to $J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))$ (as well as the automata model of Chapter 4) and *complete*. What this means can be understood in two ways, which are equivalent via the Büchi-Landweber theorem (Theorem 2.3.1).

- For every sentence φ, if φ is valid in $J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))$, then $\mathsf{LSFOM}^+ \vdash \varphi$.
- For every sentence φ, either $\mathsf{LSFOM}^+ \vdash \varphi$ or $\mathsf{LSFOM}^+ \vdash \varphi \multimap \bot$.

We privilege the latter characterization in the sequel.

LSFOM^+ is formally defined as the system

Linear semi-intuitionistic principles (LSIP) (where a is not free in ψ)

$$\begin{array}{ccc}
\forall a\,(\varphi^-(a) \otimes \psi^-) & \multimap & (\forall a\,\varphi^-(a)) \otimes \psi^- \\
\forall a\,(\varphi^-(a) \parr ?\psi^-) & \multimap & (\forall a\,\varphi^-(a)) \parr \psi^- \\
(\exists a\,\varphi(a)) \parr \psi & \multimap & \exists a\,(\varphi(a) \parr \psi) \\
\psi^- \multimap \exists a\,\varphi^-(a)) & \multimap & \exists a\,(\psi^- \multimap \varphi^-(a)) \\
(\forall a\,\varphi^\pm(a)) \multimap \psi^\pm & \multimap & \exists a\,(\varphi^\pm(a) \multimap \psi^\pm)
\end{array}$$

Linear synchronous axiom of choice (LSAC)

$$\forall a^{A^\omega}\ \exists b^{B^\omega}\ \varphi(a,b) \quad \multimap \quad \exists f^{(B^A)^\omega}\ \forall a^{A^\omega}\ \varphi(a, \mathrm{ev}_{-*}(f,a))$$

Figure 7.3: Additional axioms of LSFOM$^+$

- whose formulas are the same as LSFOM (Figure 4.1)
- whose basic deduction rules are the same as LSFOM (Figure 4.2)
- whose axioms are those of LSFOM (Figure 4.3) augmented with the axioms of Figure 7.3 corresponding to suitable restrictions of the axioms LSIP and LSAC (given in Definition 6.3.1) to the formulas of LSFOM. It should be noted that the suitable restriction to SDEXP and PEXP clauses already appear in the axiomatization of LSFOM in the more general forms $\varphi^+ \multimap !\varphi^+$ and $?\varphi^- \multimap \varphi^-$..

Given that the soundness of those additional axioms in the fibration $J^*(\mathfrak{Dial}^{\blacktriangleright}_{\mathrm{fin}}(\overline{p}))$ may be established by a straightforward adaptation of Theorem 6.3.2, we readily admit the following extension of Corollary 7.2.4 to LSFOM$^+$.

Theorem 7.3.1. *For any* LSFOM *sentence* φ*, if* LSFOM$^+ \vdash \varphi$*, then there exists an eager f.s. function* $f : X_\varphi^\omega \to U_\varphi^\omega$ *such that* FOM $\vdash \forall x.\varphi_D(f(x), x)$*.*

At this point, we can forget about the models and concentrate on proving completeness for LSFOM$^+$. To this end, we consider the translation of formulas outlined in Figure 6.1, restricted to the language of LSFOM$^+$. We do not repeat the figure as our official definition for φ_D is nothing but the $(-)^L$-translation of the definition given in Figure 7.2. Replaying the proof of Theorem 6.3.3 to LSFOM$^+$, we obtain the following characterization theorem.

Theorem 7.3.2. *For any* LSFOM *formula* $\varphi(a)$*,* LSFOM$^+$ *proves the linear equivalence*

$$\varphi(a) \quad \multimap\!\!\multimap \quad \exists u^{U^\omega}.\forall x^{X^\omega}.\varphi_D(u,x,a)$$

where $U = U_\varphi$ *and* $X = X_\varphi$*.*

Noting in particular that $\varphi_D = \lfloor \varphi_D \rfloor^L$, this latest theorem is the key statement that allow to derive the completeness of LSFOM$^+$ thanks to the Büchi-Landweber theorem. Before proceeding, we first need to prove a couple of crucial properties. First and foremost, we show that LSFOM$^+$ admits double linear negation elimination. This is not an official axiom of LSFOM$^+$, although it is valid in the models we considered (Theorem 6.2.16).

Theorem 7.3.3. *For any formula* φ*,* LSFOM *proves* $((\varphi \multimap \bot) \multimap \bot) \multimap \varphi$*.*

Proof. We use Theorem 7.3.2 for the formula $((\varphi \multimap \bot) \multimap \bot) \multimap \varphi$. Thus, it suffices to show that LSFOM$^+$ derives

$$\exists(f,F)\forall(h,x)\ \big(\varphi_D(\mathrm{ev}_{-*}(h, \mathrm{ev}_{-*}(F,(a,h,x))), \mathrm{ev}_{-*}(F,(a,h,x)), a)\ \multimap \varphi_D(\mathrm{ev}_{-*}(f,(a,h)),x,a)\big)$$

which is easy if there exists functions $f : U^{X^U} \to U$ and $F : U^{X^U} \times X \to X^U$ such that $h(F(h,x)) = f(h)$ and $F(h,x) = x$ for every h and x. Such functions are exhibited in the proof of Theorem 6.2.16. □

A corollary of Theorem 7.3.3 is that derivation of classical linear logic are admissible in LSFOM$^+$. In particular, it means that we may dualize all of is theorems.

Corollary 7.3.4. *The following is derivable in* LSFOM^+ *for any formula* $\varphi(a,b)$

$$\forall f^{(B^A)^\omega}.\exists a^{A^\omega}.\varphi(a,\mathrm{ev}_{-*}(f,a)) \ \vdash \ \exists a^{A^\omega}.\forall b^{B^\omega}.\varphi(a,b)$$

Proof. Dualize the axiom LSAC thanks to Theorem 7.3.3. □

Lemma 7.3.5. *For any formula* $\varphi(a,b)$ *and a term* $\mathtt{t}(a)$ *whose denotation is a eager f.s. function* $A^\omega \to B^\omega$*, the following is derivable in* LSFOM^+

$$\forall a^{A^\omega}.\varphi(a,\mathtt{t}(a)) \ \vdash \ \exists b^{B^\omega}.\forall a^{A^\omega}.\varphi(a,b)$$

Proof. Thanks to Corollary 7.3.4, it suffices to show

$$\forall a^{A^\omega}.\varphi(a,\mathtt{t}(a)) \ \vdash \ \forall g^{(A^B)^\omega}.\exists b^{B^\omega}.\varphi(\mathrm{ev}_{-*}(g,b),b)$$

to conclude. Now consider the equation

$$h(g) = [\![\mathtt{t}]\!](\mathrm{ev}_{-*}(g,h(g)))$$

for h a f.s. causal function $(A^B)^\omega \to B^\omega$. Thanks to Lemma 2.1.9, there is a unique h satisfying this equation. Consider a term $\mathtt{h}(g)$ such that $[\![\mathtt{h}]\!] = h$. Then LSFOM proves that

$$\forall g^{(A^B)^\omega}.\mathtt{h}(g) = \mathtt{t}(\mathrm{ev}_{-*}(g,h(g)))$$

Now assume that $\forall a^{A^\omega}.\varphi(a,\mathtt{t}(a))$ holds and that fix g; it suffices to show that $\varphi(\mathrm{ev}_{-*}(g,\mathtt{h}(g)),\mathtt{h}(g))$ holds. Instanciating our hypothesis with $a = \mathrm{ev}_{-*}(g,\mathtt{h}(g))$, we have $\varphi(\mathrm{ev}_{-*}(g,\mathtt{h}(g)),\mathtt{t}(\mathrm{ev}_{-*}(g,\mathtt{h}(g))))$, which is what we want up to the provable equation above. □

We are now ready to prove the completeness theorem.

Theorem 7.3.6. *Let* φ *be a* LSFOM *sentence. Then either* $\mathsf{LSFOM}^+ \vdash \varphi$ *or* $\mathsf{LSFOM}^+ \vdash \varphi \multimap \bot$.

Proof. Let φ be a closed LSFOM-formula and $\varphi_D(u,x)$ be the body of its Dialectica interpretation. We apply Büchi-Landweber Theorem 2.3.1 to the FOM-formula $\lfloor\varphi_D(u,x)\rfloor$. There are two cases.

- Either there exists an eager term $\mathtt{u}(x)$ denoting an *eager* f.s. causal function $X^\omega \to U^\omega$ such that $(\forall b)\neg\lfloor\varphi_D(\mathtt{u}(b),b)\rfloor$ holds. We then proceed as follows.

FOM	$\vdash$	$\lfloor\neg\varphi_D(\mathtt{u}(x),x)\rfloor$	
LSFOM	$\vdash$	$\lfloor\neg\varphi_D(\mathtt{u}(x),x)\rfloor^L$	By Lemma 4.1.6
LSFOM	$\vdash$	$\varphi_D(\mathtt{u}(x),x) \multimap \bot$	Since $\lfloor\neg\varphi_D(\mathtt{u}(x),x)\rfloor^L = \varphi_D(\mathtt{t}(x),x)$
LSFOM	$\vdash$	$\forall x.\varphi_D(\mathtt{u}(x),x)$	$\forall$-right
LSFOM^+	$\vdash$	$\exists u.\forall x.\varphi_D(u,x)$	By Lemma 7.3.5, since $\mathtt{t}(x)$ is eager
LSFOM^+	$\vdash$	φ	By Characterization (Theorem 7.3.2)

- Otherwise, there exists a term $\mathtt{x}(u)$ denoting a f.s. causal function $U^\omega \to X^\omega$ such that $(\forall u^\tau)\neg\lfloor\varphi_D(u,\mathtt{x}(u))\rfloor$ holds. Note that

$$\neg\lfloor\varphi_D(u,\mathtt{x}(u))\rfloor \quad = \quad \lfloor\varphi_D(u,\mathtt{x}(u)) \multimap \bot\rfloor$$

We then conclude as follows.

FOM	$\vdash$	$\lfloor\varphi_D(u,\mathtt{x}(u)) \multimap \bot\rfloor$	
LSFOM	$\vdash$	$\lfloor\varphi_D(u,\mathtt{x}(u)) \multimap \bot\rfloor^L$	By Lemma 4.1.6
LSFOM	$\vdash$	$\varphi_D(u,\mathtt{x}(u)) \multimap \bot$	Since $\lfloor\neg\varphi_D(u,\mathtt{x}(u))\rfloor^L = \varphi_D(u,\mathtt{x}(u)) \multimap \bot$
LSFOM	$\vdash$	$\exists x.\varphi_D(u,x) \multimap \bot$	$\exists$-right
LSFOM	$\vdash$	$\forall u.\exists x.\varphi_D(u,x) \multimap \bot)$	$\forall$-right
LSFOM^+	$\vdash$	$\exists g^{(U^X)^\omega}.\forall u^{U^\omega}\varphi_D(u,\mathrm{ev}_{-*}(g,u)) \multimap \bot$	By (LSAC)
LSFOM^+	$\vdash$	$\exists g^{(U^X)^\omega}.\forall u^{U^\omega}(\varphi \multimap \bot)_D(u,g)$	
LSFOM^+	$\vdash$	$\varphi \multimap \bot$	By Characterization (Theorem 7.3.2)

□

Part II

Proof-theoretic strength of $\mathsf{MSO}(\omega)$

This part of the thesis is meant to take a complementary approach to the question of constructivity of MSO over ω. While part I was concerned with studying weak enough subsystems of $\mathsf{MSO}(\omega)$ to obtain effective witnessing properties, this second part is concerned with the foundational strength necessary to characterize the classical theory of $\mathsf{MSO}(\omega)$. To do so, we study the decidability argument for $\mathsf{MSO}(\omega)$ through the lens of *Reverse Mathematics*, a research programme launched by Friedman whose purpose is to classify the strength of various everyday mathematical statement in terms of subsystems of second-order arithmetic.

Our findings are as follows: firstly, determinisation of infinite word automata is no stronger than complementation, at least in the sense of implication over RCA_0. Secondly, decidability of MSO over $(\mathbb{N}, \leq)$ implies both complementation and determinisation. Finally, the use of Ramsey- or König-like principles in proofs of Büchi's theorem is mostly spurious in the sense that the versions that are actually needed follow from a very limited set-existence principle, namely mathematical induction for properties expressed by Σ^0_2 formulae. More precisely, we prove:

Theorem 7.3.7. *Over* RCA_0*, the following statements are equivalent:*

1. *the principle of mathematical induction for* Σ^0_2 *formulae (denoted* Σ^0_2-IND*),*
2. *the Additive Ramsey Theorem over* $\mathbb{N}$ *(see Definition 8.1.3),*
3. *complementation for Büchi automata: there exists an algorithm which for each nondeterministic Büchi automaton* $\mathcal{A}$ *outputs a Büchi automaton* $\mathcal{B}$ *such that for every infinite word* α*,* $\mathcal{B}$ *accepts* α *exactly if* $\mathcal{A}$ *does not accept* α*,*
4. *the decidability of the depth-n fragment of the* MSO *theory of* $(\mathbb{N}, \leq)$ *(where* $n \geq 5$ *is a natural number).*

Furthermore, each of 1.–4. implies:

5. *determinisation of Büchi automata: there exists an algorithm which for each nondeterministic Büchi automaton* $\mathcal{A}$ *outputs a deterministic Rabin automaton* $\mathcal{B}$ *such that for every infinite word* α*,* $\mathcal{B}$ *accepts* α *exactly if* $\mathcal{A}$ *accepts* α*.*

Büchi's decidability theorem admits several generalizations. The most important one, due to Rabin [59] states that the MSO theory of the infinite binary tree is decidable. The proof goes through a translation to tree automata. As in Büchi's decidability theorem, the crucial step is to show that tree automata may be effectively complemented. Similarly, while the proof yields a complementation algorithm, the proof of soundness of this alogrithm is highly non-constructive: it relies crucially on the the determinisation theorem (5 above) and the positional determinacy of parity games. As shown in [41], Rabin's theorem is much stronger than Büchi's from the point of view of Reverse Mathematics. This motivates the quest for intermediate cases: are there any structure whose MSO theory

- interprets MSO over $(\mathbb{N}, <)$
- is interpreted in MSO over the full binary tree
- whose decidability is not provable from Büchi's theorem and does not prove Rabin's theorem?

A class of natural candidates is given by countable linear orders. As all linear orders embedd into $\mathbb{Q}$, it is therefore natural to ask for the axiomatic strength of the decidability theorem for MSO over $\mathbb{Q}$. Although we do not settle the question, it exhibits lower bounds showing that proving the decidability of MSO over countable orders require strictly more strength than Büchi's decidability theorem. We also investigate the additive Ramsey theorem over $\mathbb{Q}$, a core ingredient in Shelah's deciability proof [63] of MSO over $\mathbb{Q}$; we show it to be equivalent to the "shuffle lemma" from [14] and Σ^0_2-IND. This also answers Question 5.5 raised in [24].

Chapter 8 gives a short introduction to Reverse Mathematics and the basic Ramsey-like principles studied afterwards. The bulk of the material of this part is contained in Chapter 9, which offers a rather precise Reverse Mathematical characterization of Büchi's decidability theorem and related automata-theoretic theorems. Finally Chapter 10 discusses our preliminary investigation into the axiomatic strength of MSO over the rationals and open questions.

This work was done in collaboration with Leszek Kołodziejczyck, Henryk Michalewski and Michał Skrzypczak. Chapter 9 incorporates large parts of a joint paper [42].

Chapter 8

Background on reverse mathematics, finite semigroups and Ramsey theory

8.1 Preliminaries related to Ramsey theory

8.1.1 Ordered Ramsey principle

Given a set X, write $[X]^2$ for the set of unordered pairs of X, that is, the subset of $\mathcal{P}(X)$ containing sets of cardinalities exactly 2. When X is a subset of a totally ordered set such as $\mathbb{N}$, we will sometimes identify elements of $[X]^2$ with pairs $(x, y) \in X^2$ such that $x < y$.

Definition 8.1.1. Ordered Ramsey's Theorem *for pairs states that if* $(P, \preceq)$ *is a finite partial order and* $C\colon [\mathbb{N}]^2 \to P$ *is a colouring such that for every* $i<j<k$ *we have* $C(i,j) \succeq C(i,k)$*, then there exists an infinite homogeneous set* $I \subseteq \mathbb{N}$*, i.e.* $C(i,j) = C(i',j')$ *for all* $(i,j),(i',j') \in [I]^2$*.*

8.1.2 Additive Ramsey principles

Ramsey-style principles play an important rôle in proofs of decidability of MSO over various infinite structures. In the context of linear orders, we are interested mainly in the following two *additive Ramsey Theorems*, which assumes a semigroup structure on the set of colours:

- the additive Ramsey Theorem over $\mathbb{N}$ (which easily generalizes to any countable ordinal), postulating the existence of an unbounded homogeneous set,

- the additive Ramsey Theorem over $\mathbb{Q}$ (and other dense orders), postulating the existence of an interval with a dense homogeneous subset.

In [42], we showed that additive Ramsey over $\mathbb{N}$ is equivalent to Σ^0_2-IND, which is exactly the principle needed to prove complementation for Büchi automata and thus the decidability of each fixed-depth fragment of MSO over $\mathbb{N}$. Below, we show that additive Ramsey over $\mathbb{Q}$ and a related principle are also equivalent to Σ^0_2-IND. This time, however, the equivalence will imply that additive Ramsey over $\mathbb{Q}$ is much weaker than the axioms needed to prove decidability of MSO over $\mathbb{Q}$.

8.1.3 Additive Ramsey over $\mathbb{N}$

Definition 8.1.2. *Let* $(P, \leq_P)$ *be an order and* $(S, \cdot)$ *a finite semigroup. Let* $\alpha : [P]^2 \to S$*. If* e *is the neutral element of* S_1*, we extend* α *by setting* $\alpha(x,x) = e$ *for every* $x \in P$*. The colouring* α *is called* additive *if and only if for all* $x, y, z \in P$ *satisfying* $x \leq_P y \leq_P z$ *we have* $\alpha(x,y) \cdot \alpha(y,z) = \alpha(x,z)$*.*

Note that if a set $H \subseteq P$ has at least 2 elements and is *homogeneous* for an additive colouring α, i.e. for some $e \in S$ we have $\alpha(x,y) = e$ for all $(x,y) \in [H]^2$, then e is an idempotent in the semigroup S.

Definition 8.1.3 (Additive Ramsey's Theorem)**.** Additive Ramsey's Theorem *is the following statement: for every finite semigroup* $(S, *)$ *and every colouring* $C\colon [\mathbb{N}]^2 \to S$ *such that for every* $i<j<k$ *we have* $C(i,j) * C(j,k) = C(i,k)$*, there exists an infinite homogeneous set* $I \subseteq \mathbb{N}$*. That is, there is a fixed colour* a *such that for every* $(i,j) \in [I]^2$*,* $C(i,j) = a$*.*

8.1.4 Ramseyan principles over $\mathbb{Q}$

In [63], one of the critical combinatorial lemmas in the proof of decidability of MSO over $\mathbb{Q}$ is an additive Ramsey Theorem over $\mathbb{Q}$. In [14], that theorem does not make an appearance, but a principle which we call the *Shuffle Lemma* takes its place.

Definition 8.1.4. *The* additive Ramsey Theorem over $\mathbb{Q}$ *is the following statement (originally proved in [63]): "for any finite semigroup* S *and any additive colouring* $\alpha : [\mathbb{Q}]^2 \to S$*, there exists a homogeneous set* H *which is dense in* $]x,y[$ *for some* $x < y \in \mathbb{Q}$*".*

Given a linear order $(P, \leq_P)$ and a function $\alpha : P \to \Sigma$, we say that a value $a \in \Sigma$ *occurs densely* in α if for every $x, y \in P$ there exists $z \in]x,y[$ such that $\alpha(z) = a$. We call α a *shuffle* if and only if for every $a \in \Sigma$, either a is not in the image of α or a occurs densely in α. If the image of α is some set X, we say that α is an *X-shuffle*. We say that α *contains a shuffle* if there exist $x, y \in P$ with $x < y$ such that $\alpha\big|_{]x,y[}$ is a shuffle.

Definition 8.1.5. *The* Shuffle Lemma *is the following statement: "for every* $\alpha : \mathbb{Q} \to \Sigma$ *with* Σ *finite,* α *contains a shuffle."*

8.2 Basics of Reverse Mathematics

Reverse mathematics [68] is a framework for studying the strength of axioms needed to prove theorems of countable mathematics, that is, the part of mathematics concerned with objects that can be represented using no more than countably many bits of information. This typically means integers, sets of integers and real numbers.

The basic idea of reverse mathematics is to analyse mathematical theorems in terms of subsystems of a strong axiomatic theory known as second-order arithmetic. The two-sorted language of second-order arithmetic, L_2, contains *first-order* variables $x, y, z, \ldots$ (or $i, j, k, \ldots$), intended to range over natural numbers, and *second-order* variables $X, Y, Z, \ldots$, intended to range over sets of natural numbers. L_2 includes the usual arithmetic functions and relations $+, \cdot, \leq, 0, 1$ on the first-order sort, and the $\in$ relation which has one first-order and one second-order argument.

The language L_2 is very expressive: already in weak fragments of Z_2, the first-order sort can be used to encode arbitrary finite objects and the second-order sort can encode even such objects as complete separable metric spaces, continuous functions between them, and Borel sets within them (cf. [68, Chapters II.5, II.6, and V.3]). Moreover, the theory Z_2 is powerful enough to prove almost all theorems from a typical undergraduate course that are expressible in L_2. In fact, the basic observation underlying reverse mathematics [68] is that many important theorems are equivalent to various fragments of Z_2, where the equivalence is proved in some specific weaker fragment, referred to as the *base theory*.

Remark. *In this part, all models under consideration are Tarski models. A model for* L_2 *is given by a tuple* $(X, Y, +, \times, 0_X, 1_X)$ *where* X *interprets the natural numbers and* $Y \subseteq \mathcal{P}(X)$ *interprets sets of natural numbers. The* standard *model of* L_2 *is* $(\omega, \mathcal{P}(\omega), +, \cdot, <, 0, 1)$*.*

Notational convention. From this point onwards, we will use the letter $\mathbb{N}$ to denote the natural numbers as formalised in second-order arithmetic, that is, the domain of the first-order sort. On the other hand, the symbol ω will stand for the concrete, or standard, natural numbers. For instance, given a theory T and a formula $\varphi(x)$, "T proves $\varphi(n)$ for all $n \in \omega$" will mean "$\mathrm{T} \vdash \varphi(0), \mathrm{T} \vdash \varphi(1), \ldots$", which does not imply $\mathrm{T} \vdash \forall x \in \mathbb{N}.\, \varphi(x)$.

8.3 Full second-order arithmetic

Full second-order arithmetic, Z_2, has axioms of three types ([68][Definition I.2.4]):

1. axioms pertaining to the basic (in)equational properties of natural numbers, the operations $+, \cdot$ and the order.

$$\begin{aligned}
&n+1 \neq 0\\
&n+1 = m+1 \Rightarrow n = m\\
&m+0 = m\\
&m+(n+1) = (m+n)+1\\
&m \cdot 0 = 0\\
&m \cdot (n+1) = (m \cdot n) + m\\
&\neg m < 0\\
&m < n+1 \Rightarrow m = n \vee m < n
\end{aligned}$$

2. comprehension axioms for each $\varphi(x)$ is an arbitrary formula of L_2 not containing the variable X but possibly other parameters; they state that there exists a set containing exactly the numbers $n \in \mathbb{N}$ such that $\varphi(n)$.

$$\forall \bar{Y}\, \forall \bar{y}\, \exists X\, \forall x\, \big(x \in X \Leftrightarrow \varphi(x, \bar{Y}, \bar{y})\big),$$

3. induction axioms for each $\varphi(x)$ (possibly with other parameters).

$$\forall \bar{Y}\, \forall \bar{y}\, \varphi(0, \bar{Y}, \bar{y}) \wedge (\forall n\, (\varphi(n, \bar{Y}, \bar{y}) \Rightarrow \varphi(n+1, \bar{Y}, \bar{y}))) \Rightarrow \forall n\, \varphi(n, \bar{Y}, \bar{y})$$

Quantifier hierarchies. Typical fragments of Z_2 are defined in terms of quantifier hierarchies whose definitions we now recall. A formula is Σ^0_n if it has the form $\exists \bar{x}_1\, \forall \bar{x}_2\, \ldots\, \mathsf{Q} \bar{x}_n .\, \psi$, where the $\bar{x}_i$'s are blocks of first-order variables, the shape of Q depends on the parity of n, and ψ is Δ^0_0, i.e. contains only bounded first-order quantifiers. A formula is Π^0_n if it is the negation of a Σ^0_n formula. A formula is *arithmetical* if it contains only first-order quantifiers (second-order parameters are allowed).

A formula is Σ^1_n if it has the form $\exists \bar{X}_1\, \forall \bar{X}_2\, \ldots\, \mathsf{Q} \bar{X}_n .\, \psi$, where the $\bar{X}_i$'s are blocks of second-order variables, the shape of Q depends on the parity of n, and ψ is arithmetical. A formula is Π^1_n if it is the negation of a Σ^1_n formula.

In practice, we say that a formula is Σ^i_n / Π^i_n if it equivalent to a Σ^i_n / Π^i_n formula in the axiomatic theory we are working in at a given point.

The Σ^0_n-IND scheme. In the sequel we study a extensions of RCA_0 obtained by strengthening the induction scheme to formulae beyond Σ^0_1. In general, for $n \in \omega$, the axiom scheme Σ^0_n-IND is defined like Σ^0_1-IND, but with the induction formula φ allowed to be Σ^0_n rather than just Σ^0_1. For each n, $\mathsf{RCA}_0 + \Sigma^0_n$-IND is equivalent to $\mathsf{RCA}_0 + \Pi^0_n$-IND, where the latter is defined in the natural way, as well as to the least number principle for Σ^0_n or Π^0_n formulae (cf. [68, Chapter II.3]).

Two important principles provable from Σ^0_n-IND are Σ^0_n-*collection*:

$$\forall \bar{Z}\, \forall \bar{z}\, \big[\forall x \leq t\, \exists y.\, \varphi(x, y, \bar{Z}, \bar{z})\big] \Rightarrow \exists w\, \forall x \leq t\, \exists y \leq w.\, \varphi(x, y, \bar{Z}, \bar{z}),$$

for φ in Σ^0_n, and *bounded* Σ^0_n-*comprehension*:

$$\forall \bar{Y}\, \forall \bar{y}\, \forall w\, \exists X\, \forall x\, (x \in X \Leftrightarrow x \leq w \wedge \varphi(x, \bar{Y}, \bar{y})),$$

for φ in Σ^0_n. The combination of the two yields *strong* Σ^0_n-*collection*:

$$\forall \bar{Z}\, \forall \bar{z}\, \forall t\, \exists w\, \forall x \leq t\, \big[\exists y.\, \varphi(x, y, \bar{Z}, \bar{z}) \Rightarrow \exists y \leq w.\, \varphi(x, y, \bar{Z}, \bar{z})\big].$$

For each n, the theory $\mathsf{RCA}_0 + \Sigma^0_{n+1}$-IND is strictly stronger than $\mathsf{RCA}_0 + \Sigma^0_n$-IND (cf. e.g. [26, Theorem IV.1.29]). However, note that the minimal model (ω, Dec) of RCA_0 satisfies $\mathsf{RCA}_0 + \Sigma^0_n$-IND for all n, because an induction axiom is always true in a model with first-order universe ω.

Definition of RCA_0. The usual base theory in reverse mathematics is RCA_0, which guarantees only the existence of decidable sets. RCA_0 is defined by restricting the comprehension scheme to Δ^0_1-comprehension, which takes the form:

$$\forall \bar{Y}\, \forall \bar{y}\, \big[\forall x\, (\varphi(x, \bar{Y}, \bar{y}) \Leftrightarrow \neg \psi(x, \bar{Y}, \bar{y})) \Rightarrow \exists X\, \forall x\, (x \in X \Leftrightarrow \varphi(x, \bar{Y}, \bar{y}))\big],$$

where both φ and ψ are Σ^0_1 and do not contain X. For technical reasons, it is necessary to strengthen the induction axiom to Σ^0_1-IND, that is, the axiom scheme consisting of the sentences

$$\forall \bar{Y}\, \forall \bar{y}\, \big[\varphi(0, \bar{Y}, \bar{y}) \wedge \forall x\, \big(\varphi(x, \bar{Y}, \bar{y}) \Rightarrow \varphi(x+1, \bar{Y}, \bar{y})\big) \Rightarrow \forall x.\, \varphi(x, \bar{Y}, \bar{y})\big]$$

for φ in Σ^0_1. The scheme Σ^0_1-IND makes it possible to define sequences by primitive recursion (cf. [68, Theorem II.3.4]): given some x_0 and a function $f\colon \mathbb{N} \to \mathbb{N}$, RCA_0 proves that there is a unique sequence $(x_i)_{i\in\mathbb{N}}$ such that $x_{i+1} = f(x_i)$ for each i.

RCA_0 has a unique minimal model in the sense of embeddability. This minimal model is (ω, Dec), where Dec is the family of decidable subsets of ω.

The big five Reverse Mathematics classifies the strength of theorems by comparing them against the axiomatic power of subsystems of arithmetic. It turned out that plenty theorems of mathematics formalized in second-order arithmetic happen to be equivalent, over the weak base theory RCA_0, one of five subsystems of arithmetic, the so-called *big five*, given here by order of increasing strength:

- WKL_0 is RCA_0 extended with *Weak König's Lemma*, which states that every infinite binary tree admits an infinite branch. In particular, WKL_0 implies that there exists a non-computable set.

- ACA_0 (*Arithmetical Comprehension Axiom*) extends RCA_0 by allowing comprehension for Σ^0_1 formulas. This imply in particular that comprehension and induction also hold for all arithmetical formulas.

- ATR_0 (*Arithmetical Transfinite Recursion*) extends ACA_0 by allowing transfinite constructin over well-orders; we dispense with giving the formal definition of ATR_0 as we shall not encounter it again in the sequel.

- Π^1_1-CA_0 extends ACA_0 with the comprehension scheme for Π^1_1 formulas.

Additive Ramsey and Bounded-width König. Two prominent extensions of RCA_0 are related to weak forms of important nonconstructive set existence principles: König's Lemma and Ramsey's Theorem.

Weak König's Lemma is the statement: "for every k, every infinite tree contained in $\{0, 1, \ldots, k\}^*$ has an infinite branch". The theory obtained by adding this statement to RCA_0 is known as WKL_0. This is the minimal theory supporting all sorts of "compactness arguments" in combinatorics, topology, analysis, and elsewhere (cf. [68, Chapter IV]).

The theory RT^2_2 extends RCA_0 by an axiom expressing *Ramsey's Theorem for pairs and two colours*[1]: "for every 2-colouring of $[\mathbb{N}]^2$ there exists an infinite homogeneous set". $\mathsf{RT}^2_{<\infty}$ is defined similarly but allowing k-colourings for each $k \in \mathbb{N}$.

Both RT^2_2 and $\mathsf{RT}^2_{<\infty}$ are known to be incomparable with WKL_0 in the sense of implication over RCA_0 [30, 46]. WKL_0, RT^2_2, and $\mathsf{RT}^2_{<\infty}$ are all false in the minimal model (ω, Dec) of RCA_0, see [37, 43]. Much more on these theories can be found in [29].

In this paper, we study specific restricted versions of $\mathsf{RT}^2_{<\infty}$ and WKL_0 which play a role in proofs of Büchi's theorem. Recall that a *semigroup* is a set S with an associative operation $*\colon S \times S \to S$.

Definition 8.3.1 (Bounded-width König's Lemma)**.** Bounded-width König's Lemma *is the following statement: for every finite set Q and every graph G whose vertices belong to $Q \times \mathbb{N}$ and whose edges are all of the form $((q, i), (q', i+1))$ for some $q, q' \in Q$, $i \in \mathbb{N}$, if there are arbitrarily long finite paths in G starting in some vertex $(q, 0)$, then there is an infinite path in G starting in $(q, 0)$.*

Notice that Bounded-width König's Lemma applied to a graph G is essentially the same as Weak König's Lemma applied to the tree obtained by the so-called unraveling of G (in particular, Bounded-width König's Lemma is provable in WKL_0). However, we feel that the graph formulation is more natural to express.

Some restrictions of Weak König's Lemma equivalent to the Bounded-width version have been independently studied in [69]

[1] By $[X]^2$ we denote the set of unordered pairs of elements of X.

Chapter 9

Büchi's decidability theorem

We carry out a reverse-mathematical study of the results around Büchi's theorem. We have two main aims in mind. One is to compare complementation, determinisation and decidability of MSO in terms of logical strength. The other aim is to clarify the role of Ramsey's Theorem and König's Lemma in proofs of Büchi's theorem and the related facts about automata. This seems interesting in light of the fact that the usual formulation of Ramsey's Theorem for pairs and the so-called Weak König's Lemma (the form of König's Lemma most commonly needed in practice) are known to be incomparable over RCA_0 [30, 46].

Our findings are as follows: firstly, determinisation of infinite word automata is no stronger than complementation, at least in the sense of implication over RCA_0. Secondly, decidability of MSO over $(\mathbb{N}, \leq)$ implies both complementation and determinisation. Finally, the use of Ramsey- or König-like principles in proofs of Büchi's theorem is mostly spurious in the sense that the versions that are actually needed follow from a very limited set-existence principle, namely mathematical induction for properties expressed by Σ^0_2 formulae.

Theorem 7.3.7. *Over* RCA_0*, the following statements are equivalent:*

1. *the principle of mathematical induction for* Σ^0_2 *formulae (denoted* Σ^0_2-IND*),*
2. *the Additive Ramsey Theorem over* $\mathbb{N}$ *(see Definition 8.1.3),*
3. *complementation for Büchi automata: there exists an algorithm which for each nondeterministic Büchi automaton* $\mathcal{A}$ *outputs a Büchi automaton* $\mathcal{B}$ *such that for every infinite word* α*,* $\mathcal{B}$ *accepts* α *exactly if* $\mathcal{A}$ *does not accept* α*,*
4. *the decidability of the depth-*n *fragment of the* MSO *theory of* $(\mathbb{N}, \leq)$ *(where* $n \geq 5$ *is a natural number).*

Furthermore, each of 1.–4. implies:

5. *determinisation of Büchi automata: there exists an algorithm which for each nondeterministic Büchi automaton* $\mathcal{A}$ *outputs a deterministic Rabin automaton* $\mathcal{B}$ *such that for every infinite word* α*,* $\mathcal{B}$ *accepts* α *exactly if* $\mathcal{A}$ *accepts* α*.*

We also give a precise statement of the bounded-width form of König's Lemma often used in proofs of Item 5., and show that it is implied by each of 1.–4. Interestingly, it is not clear if 5. implies 1.–4. over RCA_0: standard arguments used to complement deterministic automata with acceptance conditions other than Büchi seem to involve Σ^0_2-IND.

It follows from our results that Büchi's theorem is unprovable in RCA_0, but only barely: it is true in computable mathematics, in the sense that the theorem remains valid if all the set quantifiers are restricted to range over (exactly) the decidable subsets of $\mathbb{N}$. This is in stark contrast to the behaviour of Rabin's theorem on the decidability of MSO on the infinite binary tree, which is known to require the existence of extremely complicated noncomputable sets [41]. Also Additive Ramsey's Theorem and Bounded-width König's Lemma are true in computable mathematics—quite unlike more general forms of Ramsey's Theorem for pairs and König's Lemma [37, 43].

To prove the implication $(4 \to 1)$ of Theorem 7.3.7, we come up with a family of MSO sentences for which truth in $(\mathbb{N}, \leq)$ is undecidable if Σ^0_2-IND fails. The other implications are proved by formalising more or less standard arguments from automata theory. In some cases this is routine, but especially the proof of $(1 \to 5)$ is quite delicate: we have to check not only that Σ^0_2-IND implies Bounded-width König's Lemma, but also that constructing the objects to which we apply the lemma is within the means of RCA_0.

Related work As mentioned above, this work may considered as a sequel to the analysis of Rabin's theorem in [41], which assumed that Büchi's theorem was provable in ACA_0. This fact is also used in A. Simpson's analysis of cyclic arithmetic [67] : there it is shown that Peano's arithmetic extended with cyclic proofs is conservative over Peano's arithmetic by exploiting the conservativity of ACA_0 over first-order Peano's arithmetic and the complementation theorem. Das refined this result to subsystems with limited induction thanks to our finer-grained result in [20]. He also extended our work by showing that (5) is not provable in RCA_0. Some care is required in formulating the result as the notion of Rabin acceptance is fragile in absence of Σ^0_2-IND. Furthermore, his result assumes that the determinization algorithm is given externally, i.e. as some concrete code at the meta-level. These hypotheses are rather benign: this decisevely show that our proof of 5 or any similar endeavour in adapting a known proof of soundness for a determinization procedure cannot be carried out in RCA_0.

Another study of the strength of Büchi's theorem with respect to constructive logic was also carried out in [45]. This paper is accompanied by a mechanization in the Coq proof assistant whose metatheory is an extension of Martin-Löf type theory enjoying a strong extraction property. In particular, it means that the standard interpretation of $\mathsf{MSO}(\omega)$ therein has no reason to be the same as the classical theory of $\mathsf{MSO}(\omega)$ without requiring additional axioms, such as excluded middle. One of the major contribution of [45] is establishing the equivalence between excluded middle for $\mathsf{MSO}(\omega)$, the Additive Ramsey theorem and the complementation theorem for Büchi automata in Coq. This results complements ours as the restriction on the metatheory of Coq and RCA_0 are somewhat orthgonal to one another: RCA_0 admits all instances of excluded middle while Coq rejects a Σ^0_1 instance. On the other hand, Coq admits induction for all formulas, while RCA_0 is limited to Σ^0_1-IND.

Finally, S. Simpson and Yokoyama [69] have independently studied various weak forms of Weak König's Lemma, including principles they call WKL(w-bd) and WKL(ext-bd) that can be seen to be equivalent to Bounded-width König's Lemma over RCA_0. They also prove that Σ^0_2-IND implies these principles, and have some results on circumstances under which the implication reverses (it cannot reverse in general due to the incomparability of Σ^0_2-IND and WKL_0).

9.1 Σ^0_2-IND implies Additive Ramsey

The aim of this section is to prove the following proposition, which is implication $1 \to 2$ of Theorem 7.3.7.

Proposition 9.1.1. *Over* RCA_0, Σ^0_2-IND *implies Additive Ramsey's Theorem.*

The proof of Proposition 9.1.1 consists of two steps. First, we prove another weakening of Ramsey's Theorem.

Definition 9.1.2. Ordered Ramsey's Theorem *for pairs states that if* $(P, \preceq)$ *is a finite partial order and* $C\colon [\mathbb{N}]^2 \to P$ *is a colouring such that for every* $i<j<k$ *we have* $C(i,j) \succeq C(i,k)$*, then there exists an infinite homogeneous set* $I \subseteq \mathbb{N}$*, i.e.* $C(i,j) = C(i',j')$ *for all* $(i,j),(i',j') \in [I]^2$.

It will follow from Lemma 9.1.3 below and the proof of Proposition 9.6.1 in Section 9.6 that Ordered Ramsey's Theorem is equivalent to its restriction to linear orders, and thus to the case where P is $\{0,\dots,n\}$ for some $n \in \mathbb{N}$ and $\preceq$ is the usual ordering. Note also that the theorem follows immediately from the so-called *Stable Ramsey's Theorem* $\mathsf{SRT}^2_{<\infty}$ (cf. [29, Sections 6.4 and 6.8]), where the requirement on C is only that $C(i,\cdot)$ should stabilise for each i.

Lemma 9.1.3. *Over* RCA_0, Σ^0_2-IND *proves Ordered Ramsey's Theorem.*

Proof. We call a colour $p \in P$ *recurring* if $\forall i\, \exists k > j > i.\ C(j,k) = p$. Notice that for each non-recurring colour p there exists i_p such that there is no occurrence of p to the right of i_p (i.e. no $k > j > i_p$ such that $C(j,k) = p$). By an application of strong Σ^0_2-collection we obtain some i_0 such that for every non-recurring colour p and every $k > j > i_0$ we have $C(j,k) \neq p$. In particular, there is a recurring colour. Moreover, being a recurring colour is a Π^0_2 property, so by Σ^0_2-IND we can find a $\preceq$-minimal recurring colour p_0.

We now define a sequence $(u_i, v_i)_{i\in\mathbb{N}}$ by primitive recursion on i. Let (u_0, v_0) be some pair such that $i_0 < u_0 < v_0$ and $c(u_0, v_0) = p_0$. Now assume that $u_0 < v_0 \leq u_1 < v_1 \dots \leq u_i < v_i$ have been defined, $\{u_0,\dots,u_i\}$ is homogeneous with colour p_0, and $C(u_i, v_i) = p_0$. Let (u_{i+1}, v_{i+1}) be the smallest pair such $v_i \leq u_{i+1} < v_{i+1}$ and $C(u_{i+1}, v_{i+1}) = p_0$. Such a pair exists because p_0 is recurring. We know that $C(u_i, u_{i+1}) = p_0$, since on the one hand $C(u_i, u_{i+1}) \preceq C(u_i, v_i) = p_0$, and on the other hand $u_i > i_0$ and thus $C(u_i, u_{i+1})$ is a recurring colour, so it cannot be $\preceq$-strictly

smaller than p_0. Similarly, for $j < i$ we know that $C(u_j, u_{i+1}) = p_0$ because $C(u_j, u_{i+1}) \preceq p_0$ and $u_j > i_0$. Therefore, the set $\{u_i \mid i \in \mathbb{N}\}$ is homogeneous for C. □

Before proceeding to prove the additive version of Ramsey's Theorem, we recall a few basic facts about finite semigroups we shall use in our proof. The facts are proved by elementary combinatorial arguments which readily formalise in RCA_0. The proofs can be found for instance in [54].

Definition 9.1.4. *Green preorders over a semigroup S are defined as follows*

- *$s \leq_{\mathcal{R}} t$ if and only if $s = t$ or $s \in t * S = \{t * a \mid a \in S\}$,*
- *$s \leq_{\mathcal{L}} t$ if and only if $s = t$ or $s \in S * t = \{a * t \mid a \in S\}$,*
- *$s \leq_{\mathcal{H}} t$ if and only if $s \leq_{\mathcal{R}} t$ and $s \leq_{\mathcal{L}} t$,*
- *$\leq_{\mathcal{J}}$ is the transitive closure of the union of $\leq_{\mathcal{R}}$ and $\leq_{\mathcal{L}}$.*

The associated equivalence relations are written $\mathcal{R}$, $\mathcal{L}$, $\mathcal{H}$, $\mathcal{J}$; their equivalence classes are called respectively $\mathcal{R}$, $\mathcal{L}$, $\mathcal{H}$, and $\mathcal{J}$-classes.

Lemma 9.1.5. *For every finite semigroup S and $s, t \in S$, $s \leq_{\mathcal{L}} t$ and $s\ \mathcal{R}\ t$ implies $s\ \mathcal{H}\ t$.*

Lemma 9.1.6 ([54, Proposition 2.4])**.** *If $(S, *)$ is a finite semigroup, $H \subseteq S$ an $\mathcal{H}$-class, and some $a, b \in H$ satisfy $a * b \in H$ then for some $e \in H$ we know that $(H, *, e)$ is a group.*

Now we can prove the main result of the section.

Proof of Proposition 9.1.1. Let a colouring C take values in the finite semigroup $(S, *)$ and satisfy the additivity condition of Definition 8.1.3. For every position i and every $k \geq j > i$, let us observe that $C(i, k) \leq_{\mathcal{R}} C(i, j)$. Let r be the function mapping every element of S to its $\mathcal{R}$-class. The function $r \circ C$ is an ordered colouring with respect to $\leq_{\mathcal{R}}$; let us use Lemma 9.1.3 to obtain a homogeneous sequence $(u_i)_{i \in \mathbb{N}}$ for $r \circ C$.

Since S is finite, we can use Σ^0_2-collection to prove that there is some colour a such that $C(u_0, u_i) = a$ for infinitely many i. This allows us to take a subsequence $(v_i)_{i \geq 0}$ of $(u_i)_{i \geq 0}$ such that $C(v_0, v_i) = a$ for each i.

We now know that $a = a * C(v_i, v_j)$ for every $0 < i < j$. In particular, $a \leq_{\mathcal{L}} C(v_i, v_j)$ by the definition of $\leq_{\mathcal{L}}$. Since a and $C(v_i, v_j)$ are $\mathcal{R}$-equivalent, Lemma 9.1.5 implies that $C(v_i, v_j)\ \mathcal{H}\ a$. Let H be the $\mathcal{H}$-class of a. Since $a * C(v_i, v_j) = a \in H$, we know by Lemma 9.1.6 that $(H, *, e)$ is a group for some $e \in H$. Using this group structure and the equation $a = a * C(v_i, v_j)$ we obtain that $C(v_i, v_j) = e$. Hence, $\{v_{i+1} \mid i \in \mathbb{N}\}$ is a homogeneous set for C with the colour e. □

9.2 Additive Ramsey implies complementation

In this section, we sketch a proof of the following result, which is implication $2 \to 3$ of Theorem 7.3.7.

Proposition 9.2.1. *Over RCA_0, Additive Ramsey's Theorem proves the correctness of the standard complementation procedure for Büchi automata: given a Büchi automaton $\mathcal{A}$ over an alphabet Σ, the procedure outputs a Büchi automaton $\mathcal{B}$ over the same alphabet such that for every $\alpha \in \Sigma^{\mathbb{N}}$ we have that $\mathcal{A}$ accepts α if and only if $\mathcal{B}$ does not accept α.*

The proof of this result follows the usual construction of the automaton $\mathcal{B}$ [12]. The possible transitions of a Büchi automaton over a particular letter $a \in \Sigma$ can be encoded as a *transition matrix* $M_a \colon Q \times Q \to \{0, 1, \star\}$, where $M_a(q, q') = 0$ if $(q, a, q') \notin \delta$, otherwise $M_a(q, q') = \star$ if $q \in F$, and otherwise $M_a(q, q') = 1$. Let $[Q]$ be the set of all such functions $M \colon Q \times Q \to \{0, 1, \star\}$. The states of $\mathcal{B}$ are based on transition matrices of $\mathcal{A}$. The automaton $\mathcal{B}$ guesses a Ramseyan decomposition of the given infinite word α with respect to a certain homomorphism into $[Q]$; and then verifies that the decomposition witnesses that there cannot be any accepting run of $\mathcal{A}$ over α.

Let us fix a Büchi automaton $\mathcal{A} = \langle Q, \Sigma, q^\iota, \delta, F \rangle$. We will introduce a semigroup structure on the set of all transition matrices of $\mathcal{A}$. Let us define the natural operations of addition and multiplication over $\{0, 1, \star\}$ as depicted on Figure 9.1. The addition makes it possible to choose a preferred run (i.e. an accepting transition is better than a non-accepting one) and the multiplication corresponds to concatenation of runs.

+	0	1	$\star$
0	0	1	$\star$
1	1	1	$\star$
$\star$	$\star$	$\star$	$\star$

$*$	0	1	$\star$
0	0	0	0
1	0	1	$\star$
$\star$	0	$\star$	$\star$

Figure 9.1: Two operations on $\{0, 1, \star\}$ used to define multiplication on $[Q]$.

Now, given two transition matrices $M, N \in [Q]$ we can naturally define the matrix $M * N$ that is obtained by the standard matrix multiplication formula. Notice that the mapping $\Sigma \ni a \mapsto M_a \in [Q]$ can be extended to a homomorphism $h\colon \Sigma^* \to [Q]$. Clearly, for a finite word $u \in \Sigma^*$ the matrix $h(u)$ represents possible runs of $\mathcal{A}$ over u, in analogy to the way in which M_a represents possible transitions over a.

We will say that a pair $(N, M) \in [Q] \times [Q]$ is *rejecting* if:

- $N * M = N$,
- $M * M = M$,
- but there is no $q \in Q$ such that $N(q^\iota, q) \in \{1, \star\}$ and $M(q, q) = \star$.

The structure of the automaton $\mathcal{B}$ is as follows: its set of states is $([Q])^3 \cup ([Q])^2 \cup [Q] \cup \{q^\iota\}$. Intuitively, the automaton needs to guess that a given infinite word admits a homogeneous decomposition where the initial fragment has type N and the homogeneous colour is M, for a rejecting pair (N, M). The initial state of the automaton is q^ι. The accepting states are those in $[Q]$. The automaton has the following transitions (we write $K \xrightarrow{a} K'$ for a transition $(K, a, K') \in \delta$):

- $q^\iota \xrightarrow{a} (N, M, M_a)$ for all rejecting pairs (N, M),
- $(N, M, K) \xrightarrow{a} (N, M, K * M_a)$,
- $(N, M, K) \xrightarrow{a} M$, if $K * M_a = N$,
- $M \xrightarrow{a} (M, M_a)$,
- $M \xrightarrow{a} M$ if $M_a = M$,
- $(M, K) \xrightarrow{a} (M, K * M_a)$,
- $(M, K) \xrightarrow{a} M$, if $K * M_a = M$.

To complete the proof of Proposition 9.2.1, it remains to show the following.

Lemma 9.2.2. *Over* RCA_0*, Additive Ramsey's Theorem implies that for every infinite word* α *the automaton* $\mathcal{B}$ *described above accepts* α *if and only if the automaton* $\mathcal{A}$ *does not accept* α*.*

Proof. First assume that both $\mathcal{A}$ and $\mathcal{B}$ accept an infinite word α. Let ρ be an accepting run of $\mathcal{A}$ and let τ be an accepting run of $\mathcal{B}$. Let the state $\tau(1)$ be (N, M, K). Since τ is accepting, we know that τ visits a state from $[Q]$ infinitely many times.

The only possible such state is M. Taking $k_0 < k_1 < \dots$ such that $\tau(k_i) = M$ for each i, we can decompose α as $\alpha = u_0 u_1 \dots$ where the length of $u_0 u_1 ... u_i$ is k_i. Then $h(u_0) = N$ and $h(u_i) = M$ for all $i > 0$. Our aim is to find a state q such that for some $j > i > 0$ we have $\rho(k_i) = \rho(k_j) = q$ and there is some ℓ such that $k_i \leq \ell < k_j$ and $\rho(\ell) \in F$. We can find such q using the pigeonhole principle: first define $\ell_0 = 1$ and then let ℓ_{i+1} be the smallest number such that there is an accepting state in ρ between k_{ℓ_i} and $k_{\ell_{i+1}}$. The sequence $(\ell_i)_{i \in \mathbb{N}}$ is defined by primitive recursion, therefore it can be constructed in RCA_0. By the (finite) pigeonhole principle, there exist $0 \leq i < j \leq |Q| + 1$ such that $\rho(k_{\ell_i}) = \rho(k_{\ell_j}) = q$. Since $M * M = M$ and ρ has an accepting state between k_{ℓ_i} and k_{ℓ_j} we know that $M(q, q) = \star$. Similarly, since $N * M = N$, we know that $N(q^\iota, q) \in \{1, \star\}$. It means that the pair (N, M) is not rejecting, which contradicts the definition of the transitions of $\mathcal{B}$.

Now assume that the automaton $\mathcal{B}$ rejects a given infinite word α. Consider a colouring C such that for $i < j$ we have $C(i, j) = h\big(\alpha(i)\alpha(i+1)\cdots\alpha(j-1)\big)$. Since h is a homomorphism, we know that C is additive. By Additive Ramsey's Theorem, we can find $k_0 < k_1 < \dots$ forming a homogeneous set for C. Decomposing $\alpha = u_0 u_1 \dots$ with k_i the length of $u_0 u_1 \dots u_i$ as previously, we have some $N, M \in [Q]$ such that $M * M = M$, $h(u_0) = N$ and $h(u_i) = M$ for all $i > 0$. by

skipping the first element of the homogeneous set. If the pair (N, M) was rejecting, the automaton $\mathcal{B}$ would accept α—we would be able to define using Δ^0_1-comprehension an accepting run τ of $\mathcal{B}$ over α such that $\tau(k_i) = M$ for all $i > 1$. Therefore, there exists a state q of the kind disallowed by the definition of a rejecting pair. This state can be used to construct an accepting run ρ of $\mathcal{A}$ over α, such that for every $i > 0$ we have $\rho(k_i) = q$. As above, such a run can be defined by Δ^0_1-comprehension. □

9.3 Effective complementation implies decidability

The following gives implication $3 \to 4$ of Theorem 7.3.7.

Proposition 9.3.1. *For each $n \in \omega$, RCA_0 proves: if there exists an algorithm for complementing Büchi automata, then there exists an algorithm which, given an* MSO *formula φ of depth at most n, outputs an automaton $\mathcal{A}_\varphi$ such that for every word α, the formula φ is satisfied by α if and only if $\mathcal{A}_\varphi$ accepts α. As a consequence, the depth-n fragment of $\mathsf{MSO}(\mathbb{N}, \leq)$ is decidable.*

Remark. *In fact, the algorithm producing $\mathcal{A}_\varphi$ on input φ is the same for each n. This is because there is a standard procedure (in the terminology of computability theory, a* Turing functional*) for converting algorithms for complementing Büchi automata into algorithms deciding $\mathsf{MSO}(\mathbb{N}, \leq)$. The proof of Proposition 9.3.1 verifies that the algorithm obtained by this procedure is, provably in RCA_0, correct on depth-n sentences for each $n \in \omega$.*

The proof of Proposition 9.3.1 is based on the usual idea: given φ, inductively construct automata $\mathcal{A}_\psi$ corresponding to increasingly complicated subformulae ψ of φ. However, the formula "$\mathcal{A}_\psi$ is equivalent to ψ" as written is not Σ^0_1 (not even arithmetical, as it quantifies over infinite words), so induction for it is not available in RCA_0. To deal with that, we make sure that for φ of depth n the algorithm only makes $O(n)$ *big steps*, with a single *big step* corresponding to an entire block of quantifiers/connectives at a given depth within φ. In that way, we can reason by induction of fixed length n, which is available in RCA_0 for formulae of arbitrary complexity.

Proof. We first note that w.l.o.g. we can restrict attention to depth-n MSO formulae of the form ψ or ξ given by the following grammar:

$$\begin{array}{lcl} \psi & := & \forall \bar{X}.\, \bigwedge_{i=1}^{k} \xi_i \mid A \mid \neg A \\ \xi & := & \exists \bar{X}.\, \bigvee_{i=1}^{k} \psi_i \mid A \mid \neg A \\ A & := & \mathtt{Sing}(X) \mid \min X \leq \min Y \mid X \subseteq Y \end{array}$$

where $\mathtt{Sing}(X)$ means "X is a singleton" and $\min(X) \leq \min(Y)$ means "either Y is empty or there is an element of X less than or equal to the smallest element of Y". The reason is that provably in RCA_0, it is possible to perform the following operations on an MSO formula:

- replace each first-order variable x by a corresponding second-order variable X; translate $x \leq y$ to $\min(X) \leq \min(Y)$ and relativise quantifiers over X to $\mathtt{Sing}$,
- push negations downwards to the level of atomic formulae,
- rearrange $\vee$'s and $\exists$'s (respectively, $\wedge$'s and $\forall$'s) lying at the same depth,

and obtain a formula of the same depth which is equivalent to the original one modulo the obvious identification of x with $\{x\}$. The benefit of doing so is that we obtain formulae containing solely second-order variables. We can then treat an assignment to the variables $X_1, \ldots, X_k$ as an infinite word over the alphabet $\{0,1\}^k$.

We also note that given an automaton $\mathcal{A}$ over $\{0,1\}^k$, it is easy to construct an automaton over $\{0,1\}^{k+\ell}$ which behaves just like $\mathcal{A}$ and ignores the additional ℓ coordinates. For this reason, when describing the automaton $\mathcal{A}_\psi$ assigned to a formula ψ, we can safely assume that the alphabet of $\mathcal{A}_\psi$ has exactly as many coordinates as there are free variables in ψ; in the later steps of the construction, extra coordinates can be added as needed.

The algorithm assigning automata to subformulae of φ works inductively as follows:

1. The base case is for atomic subformulae of the form $\mathtt{Sing}(X)$, $\min(X) \leq \min(Y)$, and $X \subseteq Y$. To these, the algorithm assigns the automata $\mathcal{A}_{\mathtt{Sing}}$, $\mathcal{A}_{\min}$, and $\mathcal{A}_{\subseteq}$, respectively, pictured in Figure 9.2. It is straightforward to verify in RCA_0 that the only situation in which $\mathcal{A}_{\mathtt{Sing}}$ accepts a word over $\{0,1\}$ is if it encounters a single position labelled 1, switches to the accepting state, and remains in that state by reading an infinite string of 0's. This happens

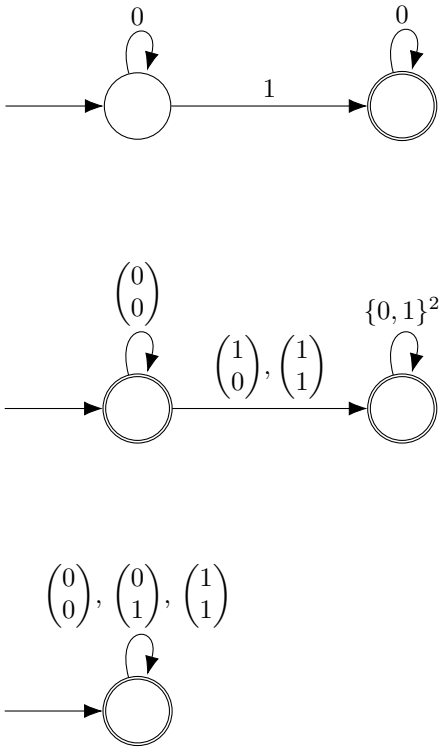


Figure 9.2: The automata $\mathcal{A}_{\texttt{Sing}}$, $\mathcal{A}_{\min}$, and $\mathcal{A}_{\subseteq}$. The initial states of the automata are indicated by incoming arrows. The accepting states are marked by double circles. The transitions are represented by arrows, labelled by the respective letters.

exactly if the word represents a singleton set X. Similarly, it is straightforward to verify that a word over $\{0,1\}^2$ representing two sets X, Y is accepted by $\mathcal{A}_{\min}$ (resp. $\mathcal{A}_{\subseteq}$) exactly if it is not the case that 1 appears on the second coordinate before it appears on the first coordinate (resp. that 1 appears on the first coordinate with 0 on the second). This is just what is needed to recognise the property $Y{=}\emptyset \vee \min(X){\leq}\min(Y)$ (resp. the property $X \subseteq Y$).

2. Automata corresponding to $\neg\texttt{Sing}(X)$, $\neg\min(X) \leq \min(Y)$, and $\neg X \subseteq Y$ are constructed using the algorithm for complementation.

3. Given formulae ψ_i, $1 \leq i \leq k$, and corresponding automata $\mathcal{A}_i = \langle Q_i, \{0,1\}^\ell, q_{q_i^\iota}, \delta_i, F_i\rangle$, the automaton corresponding to $\bigvee_{1\leq i\leq k} \psi_i$ is $\bigvee_i \mathcal{A}_i := \langle \{q_0\} \sqcup \bigsqcup_i Q_i, \{0,1\}^\ell, q_0, \delta' \sqcup \bigsqcup_i \delta_i, \bigsqcup F_i\rangle$ where the set δ' is $\{(q_0, a, q) \mid \exists i \leq k.\ (q_{q_i^\iota}, a, q) \in Q_i\}$. If a word α is accepted by some $\mathcal{A}_i$ due to a run ρ then ρ' defined as $\rho'(0) = q_0$ and as ρ everywhere else is an accepting run of $\bigvee_i \mathcal{A}_i$ over α. Conversely, if $\rho \in (\{q_0\} \sqcup \bigsqcup_i Q_i)^{\mathbb{N}}$ is an accepting run of $\bigvee_i \mathcal{A}_i$ over α, then $\rho(1)$ belongs to Q_i for some i. Then for $j > 0$ each $\rho(j)$ also belongs to Q_i and all corresponding transitions agree with δ_i. Defining ρ' by $\rho'(0) = q_{q_i^\iota}$ and as ρ everywhere else yields an accepting run of $\mathcal{A}_i$ over α.

4. If the automaton $\mathcal{A} = \langle Q, \{0,1\}^{k+\ell}, q_q^\iota, \delta, F\rangle$ corresponding to $\psi(\bar{X}, \bar{Y})$, then the automaton corresponding to $\exists\bar{Y}\psi$ is $\exists\mathcal{A} := \langle Q, \{0,1\}^k, q_q^\iota, \delta_\exists, F\rangle$ with $\delta_\exists := \{(q, (a_1, \ldots, a_k), q') \mid \exists\bar{b}.\, (q, (a_1, \ldots, a_k, b_1, \ldots, b_\ell), q') \in \delta\}$. We argue that $\exists\mathcal{A}$ accepts a word α if and only if there exists some $\beta \in (\{0,1\}^\ell)^{\mathbb{N}}$ such that $\mathcal{A}$ accepts $\alpha \otimes \beta$, where $\otimes$ stands for (coordinate-wise) concatenation of finite sequences. Indeed, suppose that α is accepted by $\exists\mathcal{A}$ using an accepting run $\rho \in Q^{\mathbb{N}}$. By the definition, this means that for every j there exists $\bar{b} \in \{0,1\}^\ell$ such that $(\rho(j), \alpha(j) \otimes \bar{b}, \rho(j+1)) \in \delta$. Use Δ^0_1-comprehension to define an infinite word β by picking a minimal such $\bar{b}$ as $\beta(j)$ for every j. Then ρ is an accepting run of $\mathcal{A}$ over $\alpha \otimes \beta$. Conversely, it is clear that an accepting run ρ of $\mathcal{A}$ over $\alpha \otimes \beta$ is an accepting run of $\exists\mathcal{A}$ over α.

5. Finally, the formula $\forall\bar{X}.\ \bigwedge_{i=1}^k \xi_i$ is equivalent to $\neg\exists\bar{X}.\ \bigvee_{i=1}^k \neg\varphi_i$. The automaton corresponding to it is built by means of constructions 3 and 4 and two rounds of complementations

Clearly, we can argue by induction on $m \leq n$ that for all subformulae ψ of φ at depth m, the automaton $\mathcal{A}_\psi$ is equivalent to ψ. In particular, $\mathcal{A}_\varphi$ is equivalent to φ.

It remains to deduce decidability of the depth-n fragment of $\mathsf{MSO}(\mathbb{N}, \leq)$. Given an algorithm transforming a depth-n MSO formula to an equivalent automaton, it suffices to show decidability of the emptiness problem for Büchi automata: "given a nondeterministic Büchi automaton $\mathcal{A}$, does there exist an infinite word accepted by $\mathcal{A}$?" As is well known, the answer is positive exactly if $\mathcal{A}$ contains a state q which is reachable from the initial state q_I and has the property that q can be reached from q via a path containing an accepting state. The standard argument proving this formalises in RCA_0 in an unproblematic way. □

9.4 Decidability implies Σ^0_2-IND

In this section we prove the following result.

Proposition 9.4.1. *Over RCA_0, the decidability of the depth-5 fragment of the theory $\mathsf{MSO}(\mathbb{N}, \leq)$ implies Σ^0_2-IND.*

This is, of course, implication $4 \to 1$ of Theorem 7.3.7. The proof of the implication is based on two observations which deserve to be stated as separate lemmas.

The first lemma explains one way in which the decidability of the MSO theory of some structure can be used to derive some nontrivial principles. Basically, properties corresponding to families of MSO sentences are decidable (in particular, Σ^0_1), and therefore mathematical induction can be applied to them.

Lemma 9.4.2. *For every $n \in \omega$, the following is provable in RCA_0. Let $(\psi_i)_{i\in\mathbb{N}}$ be a sequence of depth-n MSO sentences and let $\mathbb{A}$ be a structure such that the depth-n fragment of the theory $\mathsf{MSO}(\mathbb{A})$ is decidable. If $\psi_0 \in \mathsf{MSO}(\mathbb{A})$ and if $\psi_i \in \mathsf{MSO}(\mathbb{A})$ implies $\psi_{i+1} \in \mathsf{MSO}(\mathbb{A})$ for each $i \in \mathbb{N}$, then $\psi_i \in \mathsf{MSO}(\mathbb{A})$ for each $i \in \mathbb{N}$.*

Proof. It is enough to note that the property "$\psi_i \in \mathsf{MSO}(\mathbb{A})$" can be expressed by a Σ^0_1 L_2-formula $\varphi(i)$ (and, in fact, by a Π^0_1 formula too), and Σ^0_1-IND is available. □

The second lemma will provide us with a concrete MSO-expressible property to which the first lemma can be applied.

Lemma 9.4.3. *Let $\pi(i)$ be the Π^0_2 formula $\forall x\, \exists y.\, \delta(i, x, y)$, where $\delta(i, x, y)$ is Δ^0_0, possibly with parameters. Then RCA_0 proves that for every $k \in \mathbb{N}$, there exists a word α over the alphabet $\{0, \ldots, k+1\}$ such that for each $i \leq k$ and $v \in \mathbb{N}$ the letter $i+1$ appears in α at least v times if and only if $\forall x < v\, \exists y.\, \delta(i, x, y)$. In particular, $i+1$ appears in α infinitely many times if and only if $\pi(i)$ holds.*

Proof. We reason in RCA_0. Given some $k \in \mathbb{N}$, we define a function C with domain $\{0, \ldots, k\} \times \mathbb{N}$ by letting $C(i, w) = \max\{v \leq w \mid \forall x < v\, \exists y < w.\, \delta(i, x, y)\}$ for $i \leq k$ and $w \in \mathbb{N}$. Clearly the function C is computable and so exists by Δ^0_1-comprehension.

Given some computable enumeration[1] of pairs $\langle \cdot, \cdot \rangle \colon \mathbb{N}^2 \to \mathbb{N}$ that is monotone with respect to the coordinatewise order on $\mathbb{N}^2$, define the infinite word α by:

$$\alpha(j) = \begin{cases} i+1 & \text{if } j = \langle i, w \rangle,\ i \leq k, \\ & \quad \text{and } C(i, w) > \big|\{w' < w \mid \alpha(\langle i, w' \rangle) = i+1\}\big|, \\ 0 & \text{otherwise.} \end{cases}$$

Again, $\alpha(j)$ is computable so α can be obtained by Δ^0_1-comprehension. Note that $\alpha\langle i', w \rangle = i+1$ implies $i' = i$ for any i, i'. We now verify that α satisfies the requirements of the lemma.

First assume that $\forall x < v\, \exists y.\, \delta(i, x, y)$ holds for some $i \leq k$ and $v \in \mathbb{N}$. By Σ^0_1-collection, there exists some w such that $\forall x < v\, \exists y < w.\, \delta(i, x, y)$. Let $\ell = \big|\{w' < w \mid \alpha(\langle i, w' \rangle) = i+1\}\big|$. If $\ell \geq v$ then we are done. Assume the contrary and notice that $C(i, w) \geq v$. This means that for $w' = w, w+1, \ldots, w+v-\ell-1$ we have $\alpha(\langle i, w' \rangle) = i+1$ (we use Σ^0_1-IND to prove this). In total this gives us v positions of α that are labelled by $i+1$.

Now assume that there are at least v positions of α labelled by $i+1$. Let w_0 be the minimal position such that $\big|\{w' \leq w_0 \mid \alpha(\langle i, w' \rangle) = i+1\}\big| = v$. We know that $\alpha(\langle i, w_0 \rangle) = i+1$ and that the set $\{w' < w_0 \mid \alpha(\langle i, w' \rangle) = i+1\}$ has $v-1$ elements. This means that $C(i, w_0) \geq v$. By the definition of $C(i, w)$, it follows that $\forall x < v\, \exists y.\, \delta(i, x, y)$ holds. □

[1] $(n, k) \mapsto \frac{(n+k+1)(n+k)}{2} + k$ is a simple enough example.

To complete the proof of Proposition 9.4.1, we will use Lemma 9.4.3 to show that if the depth$\bar{}$/5 fragment of $\mathsf{MSO}(\mathbb{N},\leq)$ is decidable, then Lemma 9.4.2 can be applied to a sequence of MSO sentences $(\psi_k)_{k\in\mathbb{N}}$ where ψ_k basically says "Π^0_2 induction holds up to k".

Proof of Proposition 9.4.1. For $k\in\mathbb{N}$, let ψ_k be the MSO sentence "for every infinite word over the alphabet $\{0,\dots,k\}$ there is a maximal letter $i\in\{0,\dots,k\}$ occurring infinitely often". More formally, ψ_k is defined to be the depth$\bar{}$/5 sentence

$$\forall X_0\,\forall X_1\,\dots\forall X_k\left[\forall x\left(\bigvee_{i\leq k} x\in X_i\wedge\bigwedge_{i<j\leq k}\neg\big(x\in X_i\wedge x\in X_j\big)\right)\Longrightarrow \bigvee_{i\leq k}\left((\forall x\,\exists y{\geq}x.\,y\in X_i)\wedge\bigwedge_{i<j\leq k}(\exists x\,\forall y{\geq}x.\,y\notin X_j)\right)\right].$$

Clearly, RCA_0 proves that $\psi_0\in\mathsf{MSO}(\mathbb{N},\leq)$ and for every $k\in\mathbb{N}$, if $\psi_k\in\mathsf{MSO}(\mathbb{N},\leq)$, then $\psi_{k+1}\in\mathsf{MSO}(\mathbb{N},\leq)$. So, by Lemma 9.4.2 and the assumption on decidability of depth$\bar{}$/5 $\mathsf{MSO}(\mathbb{N},\leq)$, each sentence ψ_k is true in $(\mathbb{N},\leq)$.

Now consider a Π^0_2 formula $\pi(i)$, possibly with parameters. Let $k\in\mathbb{N}$ and assume that $\pi(0)$ but $\neg\pi(k)$. Let α be the word corresponding to π and k provided by Lemma 9.4.3. Since the MSO sentence ψ_{k+1} is true in $(\mathbb{N},\leq)$, there is a maximal letter i appearing in α infinitely often. Clearly $0<i<k+1$ and $\pi(i-1)$ but $\neg\pi(i)$.

Since $\pi(i)$ was an arbitrary Π^0_2 formula, we have proved Π^0_2-IND and thus also Σ^0_2-IND. □

9.5 Making complementation ineffective

The work of Sections 9.1–9.4 proves the equivalence of items 1, 2, 3 and 4 of Theorem 7.3.7. However, 3, concerning complementation of Büchi automata, contains an effectivity condition, namely that there exists an algorithm that produces an automaton complementing any given input automaton $\mathcal{A}$. It is natural to ask whether this effectivity condition can be dropped without compromising the logical strength of the statement.

Below, we prove that the answer is positive, and therefore also item 4' of Theorem 7.3.7 is equivalent to the others. Our argument relies on the ideas of Section 9.4 and is similar in spirit to the one used in the proof of [41, Theorem 3.1, (2) → (3)], though somewhat simpler. Clearly 3 implies 4'. Hence, it is enough to show for instance that 4' implies 1:

Proposition 9.5.1. *Provably in RCA_0, if for every nondeterministic Büchi automaton $\mathcal{A}$ there exists a Büchi automaton $\mathcal{B}$ such that for every infinite word α, $\mathcal{B}$ accepts α exactly if $\mathcal{A}$ does not accept α, then Σ^0_2-IND holds.*

Proof. Assume Σ^0_2-IND fails and let $\pi(i)$ be a Π^0_2 formula such that $\pi(0)$ and $\pi(i)\to\pi(i+1)$ for each i, but $\neg\pi(k)$ for some k. By Lemma 9.4.3 this means that there is a word α over the alphabet $\{0,\dots,k+1\}$ such that there is no maximal letter $i\leq k+1$ appearing infinitely often in α.

Consider the following Büchi automaton $\mathcal{A}$ working over $\{0,\dots,k+1\}$: at some point, $\mathcal{A}$ nondeterministically chooses a letter i and verifies that from that point onwards, i appears infinitely many times but no $j>i$ appears at all. Apply complementation to obtain an automaton $\mathcal{B}$ which accepts exactly if $\mathcal{A}$ rejects.

Note that $\mathcal{A}$ rejects the word α, because no matter when it makes its nondeterministic choice and what letter i it chooses, either i will appear only finitely many times or some $j>i$ will appear after the choice is made. Therefore, $\mathcal{B}$ has an accepting run on some word, namely on α. By a standard application of the (finite) pigeonhole principle $\ell+p$, it chooses the maximal letter occurring as one of $\beta(\ell),\dots,\beta(\ell+p-1)$. This contradicts the assumption that $\mathcal{B}$ accepts exactly if $\mathcal{A}$ rejects. □

9.6 Additive Ramsey and Ordered Ramsey imply Σ^0_2-IND

In this section, we give a direct proof showing that both Additive Ramsey's Theorem and Ordered Ramsey's Theorem imply Σ^0_2-IND. The implication from Additive Ramsey already follows from Theorem 7.3.7. However, the argument below is very simple and establishes a direct link between our Ramsey-theoretic statements and the induction scheme, without the detour through automata and MSO; thus, we feel it is worth including.

Proposition 9.6.1. *Over* RCA_0*, both Additive Ramsey's Theorem and Ordered Ramsey's Theorem imply* Σ^0_2-IND.

Proof. By Lemma 9.4.3, to derive Σ^0_2-IND it is enough to show that for every $k \in \mathbb{N}$ and every infinite word $\alpha \in \{0, \dots, k\}^{\mathbb{N}}$, there is a maximal letter i appearing infinitely many times in α. Fix k and α and consider the colouring C with values in $\{0, \dots, k\}$ defined for $i < j$ as follows:

$$C(i, j) = \max\{\alpha(\ell) \mid i \leq \ell < j\}.$$

The colouring C can be viewed both as an additive colouring of $[\mathbb{N}]^2$ by elements of the semigroup $(\{0, \dots, k\}, \max)$, or as an ordered colouring w.r.t. the inverse of the usual order on $\{0, \dots, k\}$. Thus, we can use either Additive Ramsey's Theorem or Ordered Ramsey's Theorem to obtain an infinite homoneous set I for C. Let $i \in \{0, \dots, k\}$ be the colour of I. By the definition of C, i is the largest colour that appears infinitely many times in α. □

9.7 Σ^0_2-IND implies Bounded-width König

Theorem 9.7.1. *Over* RCA_0*,* Σ^0_2-IND *implies Bounded-width König's Lemma (see Definition 8.3.1).*

Proof of Theorem 9.7.1. Let us fix a graph G with vertices contained in $Q \times \mathbb{N}$ for some finite set Q. The usual way of proving König's Lemma would start by defining the subset G' of those vertices v of G for which the subgraph under v is infinite. Having defined G', we could inductively pick any infinite path in G' and—assuming G does in fact contain arbitrarily long finite paths starting in $Q \times \{0\}$—we are guaranteed not to get stuck. The issue is whether we can obtain G' by Δ^0_1-comprehension.

A Π^0_1-definition of G' is provided by a standard trick used in the context of WKL_0. Notice that for every fixed k there can be at most $|Q|$ vertices of G of the form (q, k). Thus a vertex (q, k) is in G' if and only if it has the Π^0_1 property that for every $\ell \geq k$ there exists a vertex (q', ℓ) reachable from (q, k) by a path in G; here the existential quantifier over (q', ℓ) is bounded in terms of ℓ and $|Q|$.

What remains is to give a Σ^0_1-definition of G'.

Consider two numbers $k < \ell$ and a vertex $v = (q, k)$ of G. We will say that v *dies before* ℓ if there is no path in G from v that reaches a vertex of the form (q', ℓ). For $i = 0, 1, \dots, |Q|$ we will say that *i vertices die infinitely many times* if

$$\forall j\, \exists k > j\, \exists \ell > k.\ \text{there are at least } i \text{ vertices of the form } (q, k) \text{ that die before } \ell.$$

Notice that the property of i that *i vertices die infinitely many times* is Π^0_2. Clearly if $i \leq i'$ and *i' vertices die infinitely many times* then *i vertices die infinitely many times*. By Σ^0_2-IND we can fix i_0 as the maximal i such that *i vertices die infinitely many times*. By the definition, if $i > i_0$ then there exists $j(i)$ such that for every $\ell > k > j(i)$ there are fewer than i vertices of the form (q, k) that die before ℓ. Notice that we can assume $j_0 := j(i_0 + 1)$ to be an upper bound for all $j(i)$ where $i > i_0$. This means that for $\ell > k > j_0$ we have at most i_0 vertices of the form (q, k) that die before ℓ. Additionally, for infinitely many k there is $\ell > k$ such that exactly i_0 vertices of the form (q, k) die before ℓ. The following claim shows how one can find a witness that the subgraph under a vertex v is infinite.

Claim. *Assume that we are given $\ell > k > j_0$ and a vertex $v = (q, k)$ such that exactly i_0 vertices of the form (q', k) with $q' \neq q$ die before ℓ. Then the subgraph under v is infinite.*

Proof. Assume to the contrary that for some $\ell' > \ell$ there is no vertex of the form (q', ℓ') that can be reached from (q, k) by a path in G. This means that (q, k) dies before ℓ'. Therefore, there are at least $i_0 + 1$ vertices of the form (q', k) that die before ℓ'. This contradicts the way j_0 was chosen. □

Clearly, if for some $\ell > k$ and a vertex $v = (q, k)$ we know that v dies before ℓ then the subgraph of G under v is finite.

We shall now use Claim 9.7 to give a Σ^0_1-definition of G'. We will say that $v = (q, k)$ belongs to G' if there exist $\ell > k' > \max(k, j_0)$ and i_0 vertices of the form (q', k') such that all of them die before ℓ and some other vertex of the form (q'', k') is reachable in G by a path from v. Clearly this is a Σ^0_1-definition. It remains to prove that it defines G'. First assume that v satisfies the above

property and fix ℓ, k', and (q'', k') as in the definition. By Claim 9.7 we know that the subgraph under (q'', k') is infinite. Since (q'', k') is reachable from v in G, this implies that also the subgraph under v is infinite and thus $v \in G'$. Now assume that $v = (q, k) \in G'$. By the choice of i_0 we know that there exist $\ell > k' > \max(k, j_0)$ and exactly i_0 vertices of the form (q', k') that die before ℓ. Since the subgraph under v is infinite, we know that some vertex of the form (p, ℓ) is reachable from v in G. Notice that any path connecting v and (p, ℓ) needs to contain a vertex of the form (q'', k'). Clearly (q'', k') cannot be among the i_0 vertices that die before ℓ. Thus v satisfies the above condition.

We have thus shown that the graph G' is indeed Δ^0_1-definable, so we can use it to complete the proof. Let the vertex $(q, 0)$ of G satisfy the hypothesis of Bounded-width König's Lemma. Clearly, $(q, 0) \in G'$. Just as clearly, each $v = (q, k) \in G'$ is connected by an edge to some $(q', k + 1) \in G'$. This lets us define an infinite path in G' by primitive recursion. Let $\pi(0)$ be $(q, 0)$. If $\pi(k)$ is defined let $\pi(k + 1) = (q', k + 1)$ for the minimal $q' \in Q$ such that $(q', k + 1) \in G'$ and there is an edge in G between $\pi(k)$ and $(q', k + 1)$. By the construction π is an infinite path in G', and hence in G, starting in $(q, 0)$. □

9.8 Σ^0_2-IND implies determinisation

The entirety of this section is devoted to a proof of the following theorem, which coincides with implication $1 \to 4'$ of Theorem 7.3.7.

Theorem 9.8.1. *Over* RCA_0, Σ^0_2-IND *implies the existence of an algorithm which, given a nondeterministic Büchi automaton* $\mathcal{B}$ *over an alphabet* Σ*, outputs an equivalent deterministic Rabin automaton* $\mathcal{A}$ *over the same alphabet such that for every* $\alpha \in \Sigma^{\mathbb{N}}$ *we have*

$$\mathcal{A} \text{ accepts } \alpha \quad \iff \quad \mathcal{B} \text{ accepts } \alpha.$$

The proof scheme presented here is based on a determinisation procedure proposed in [52] (see [2, 38] for similar arguments and a comparison of this determinisation method to the method of Safra). Our exposition follows lecture notes of Bojańczyk [9]. Although the general structure of the argument is standard, we need to take additional care to ensure that the reasoning can be conducted in RCA_0 using only Σ^0_2-IND.

9.8.1 Transducers

The proof of Theorem 9.8.1 will be split into separate steps that will allow us to successively simplify the objects under consideration. The steps typically take the form of lemmas stating the existence of automata with certain properties. All the lemmas in the remainder of the section are asserted to hold provably in $\mathsf{RCA}_0 + \Sigma^0_2$-IND. Moreover, all automata whose existence is claimed can be obtained effectively given a nondeterministic Büchi automaton $\mathcal{B}$ over the alphabet Σ and possibly other automata mentioned in the hypothesis of each particular lemma.

To merge the steps we will use the notion of a deterministic transducer that transforms one infinite word into another[2].

Definition 9.8.2. *A transducer is a deterministic finite automaton, without accepting states, where each transition is additionally labelled by a letter from some* output alphabet*. More formally, a transducer with an input alphabet* Σ *and an output alphabet* Γ *is a tuple* $\mathcal{T} = \langle Q, q_0, \delta \rangle$ *where* $q_0 \in Q$ *is an initial state and* $\delta \colon Q \times \Sigma \to \Gamma \times Q$*.*

A transducer naturally defines a function $\mathcal{T} \colon \Sigma^{\mathbb{N}} \to \Gamma^{\mathbb{N}}$. Formally, such a function is a third-order object and thus not available in second-order arithmetic. However, given a word α, we can use Δ^0_1-comprehension to obtain the unique infinite word produced by $\mathcal{T}$ on the input α. Whenever we write $\mathcal{T}(\alpha)$, we have this word in mind.

It is easy to see that a transducer can be used to reduce the question of acceptance from one deterministic automaton to another, as stated by the following lemma.

Lemma 9.8.3. *For every deterministic Rabin automaton* $\mathcal{A}$ *with input alphabet* Γ *and every transducer* $\mathcal{T} \colon \Sigma^{\mathbb{N}} \to \Gamma^{\mathbb{N}}$*, there exists a deterministic Rabin automaton* $\mathcal{A} \circ \mathcal{T}$ *which accepts an infinite word* $\alpha \in \Sigma^{\mathbb{N}}$ *if and only if* $\mathcal{A}$ *accepts* $\mathcal{T}(\alpha)$*.*

[2]This is exactly the notion of Mealy machines given in Definition 1.3.2 of Part I. In order to keep Part II self-contained, all necessary information is recalled here.

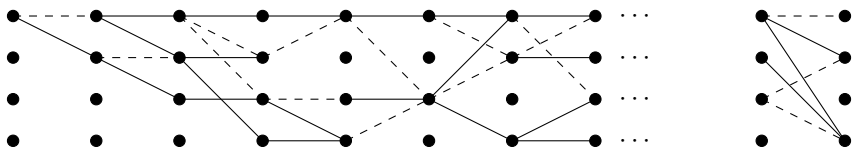


Figure 9.3: A Q-dag and a single letter from the alphabet $[Q]$. The accepting edges are represented by solid lines, and non-accepting edges are dashed lines.

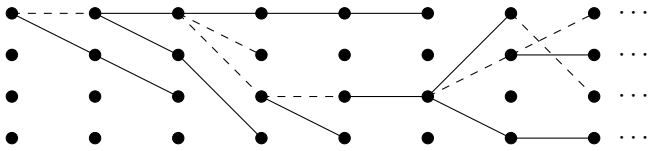


Figure 9.4: A tree-shaped Q-dag.

Proof. Let the set of states of $\mathcal{A} \circ \mathcal{T}$ be the product of the states of $\mathcal{A}$ and the states of $\mathcal{T}$. The transition function of $\mathcal{A} \circ \mathcal{T}$ follows both the transitions of $\mathcal{T}$ and the transitions of $\mathcal{A}$ over letters output by $\mathcal{T}$:

$$\delta^{\mathcal{A}\circ\mathcal{T}}\big((q^{\mathcal{A}}, q^{\mathcal{T}}), a\big) = (\delta^{\mathcal{A}}(q^{\mathcal{A}}, b), q') \quad \text{where } \delta^{\mathcal{T}}(q^{\mathcal{T}}, a) = (b, q').$$

The Rabin acceptance condition of $\mathcal{A} \circ \mathcal{T}$ is taken to be the acceptance of $\mathcal{A}$, skipping the second coordinate of the states. Clearly the first coordinate of the run of $\mathcal{A} \circ \mathcal{T}$ over an infinite word α equals the run of $\mathcal{A}$ over $\mathcal{T}(\alpha)$, so $\mathcal{A} \circ \mathcal{T}$ accepts α if and only if $\mathcal{A}$ accepts $\mathcal{T}(\alpha)$. □

9.8.2 Q-dags

In the exposition below we will work with infinite words representing the set of all possible runs of a nondeterministic automaton over a fixed infinite word. Let us define a Q-dag to be a directed acyclic graph where the set of nodes is $Q \times \mathbb{N}$ and every edge is of the form

$$((q, k), (p, k+1)) \qquad \text{for some } p, q \in Q \text{ and } k \in \mathbb{N}.$$

Furthermore, every edge is coloured by one of the two colours: "accepting" or "non-accepting". We assume that there are no parallel edges. A path in a Q-dag is a finite or infinite sequence of nodes connected by edges (either accepting or non-accepting). As we will see, we can assume that every Q-dag is rooted—there is a distinguished element $q_0 \in Q$ such that all the edges of the Q-dag lie on a path that starts in the vertex $(q_0, 0)$. We call a vertex (q, k) *reachable* if there is a path from $(q_0, 0)$ to (q, k) in α. We say that an infinite path in a Q-dag is *accepting* if it starts in $(q_0, 0)$ and contains infinitely many accepting edges.

Every Q-dag can be naturally represented as an infinite word, where the k-th letter encodes the set of edges of the form $((q, k), (q', k+1))$. The alphabet used for this purpose will be the set of transition matrices $[Q] : Q \times Q \to \{0, 1, \star\}$. An example of a Q-dag and a letter in $[Q]$ are depicted on Figure 9.3.

We will be particularly interested in Q-dags that are *tree-shaped*. A Q-dag is *tree-shaped* if every node (q, k) has at most one incoming edge (i.e. an edge from a node of the form $(p, k-1)$). Notice that it makes sense to say that a letter $M \in [Q]$ is tree-shaped and a Q-dag is tree-shaped if and only if all of its letters are tree-shaped. Figure 9.4 depicts a tree-shaped Q-dag.

A Q-dag is *infinite* if for every k there exists a path connecting the root $(q_0, 0)$ with a vertex of the form (q', k). Similarly, a Q-dag is *infinite under* (q, k) if for every $k' \geq k$ there exists a path connecting the vertex (q, k) with a vertex of the form (q', k').

Lemma 9.8.4. *Given a nondeterministic Büchi automaton $\mathcal{B}$ over an alphabet Σ, there exists a transducer $\mathcal{T}_1$ that takes as input an infinite word $\alpha \in \Sigma^{\mathbb{N}}$ and outputs a Q-dag $\mathcal{T}_1(\alpha)$ such that $\mathcal{B}$ accepts α if and only if $\mathcal{T}_1(\alpha)$ contains an accepting path.*

Proof. The transducer $\mathcal{T}_1$, after reading a finite word $w \in \Sigma^*$, stores in its state the set of states of $\mathcal{B}$ reachable from $q_0^{\mathcal{B}}$ over w. The initial state of $\mathcal{T}_1$ is $\{q_0\}$. Given a state $R \subseteq Q$ of $\mathcal{T}_1$ and a letter a, the transducer moves to the state

$$R' = \{q' \mid (q, a, q') \in \delta^{\mathcal{B}}, q \in R\}$$

and outputs a letter $M \in [Q]$ such that $M(q,q') = M_a(q,q')$ if $q \in R$ and $M(q,q') = 0$ if $q \notin R$. Clearly there is a computable bijection between the accepting runs of $\mathcal{B}$ over α and accepting paths in the Q-dag $\mathcal{T}_1(\alpha)$. □

9.8.3 Reduction to tree-shaped Q-dags

The next lemma shows that one can use a transducer to reduce general Q-dags to tree-shaped Q-dags.

Lemma 9.8.5. *There exists a transducer $\mathcal{T}_2$ that takes as input a Q-dag α' and outputs a tree-shaped Q-dag $\mathcal{T}_2(\alpha')$ such that α' contains an accepting path if and only if $\mathcal{T}_2(\alpha')$ contains an accepting path.*

To prove this lemma we will use a lexicographic order on paths in a given Q-dag. A crucial ingredient here is Bounded-width König's Lemma from Section 9.7. Additionally, we need to make sure that the graph to which Bounded-width König's Lemma is applied can be obtained using Δ^0_1-comprehension. For this purpose we use Σ^0_2-IND once again.

In the proof we will use the following definition.

Definition 9.8.6 (Profiles)**.** *For a finite path w in a Q-dag, define its profile to be the word over the alphabet $\{1,\star\} \times Q^2$ which is obtained by replacing each edge $((q,k),(q',k+1))$ in w by (x,q,q') where $x \in \{1,\star\}$ is the type of the edge ($\star$ for accepting and 1 for non-accepting). Let us fix any linear order $\preceq$ on $\{1,\star\} \times Q^2$ such that $(\star,q,q') \prec (1,p,p')$. Let $\preceq$ be the lexicographic order on paths induced by the order $\preceq$ on their profiles. We call a path w* optimal *if it is lexicographically minimal among all paths with the same source and target.*

Lemma 9.8.5 follows from Claims 9.8.3 and 9.8.3.

Claim. *There is a transducer $\mathcal{T}\colon [Q]^{\mathbb{N}} \to [Q]^{\mathbb{N}}$ such that if the input is α then $\mathcal{T}(\alpha)$ is tree-shaped with the same reachable vertices as in α, and such that every finite path from the root in $\mathcal{T}(\alpha)$ is an optimal path in α.*

Proof. We start with the following observation about the order $\preceq$. Let w, w', u, u' be paths in a Q-dag α such that the target of w (resp. u) is the source of w' (resp. u'); and w, u are of equal length. Then $ww' \preceq uu'$ if and only if $w \prec u$ or $w = u$ and $w' \preceq u'$.

Now let us define $\mathcal{T}(\alpha)$ by choosing, for every vertex reachable in α, an ingoing edge that belongs to some optimal path. Putting all of these edges together will yield a tree-shaped Q-dag as in the statement of the claim. To produce such edges, after reading the first k letters, the automaton keeps in its state a linear order on Q that corresponds to the lexicographic ordering on the optimal paths leading from the root to the nodes at depth k. Updating the order on Q upon reading a new letter from $[Q]$ is possible thanks to the observation above—thus, only finitely many states that keep the current order on Q are enough. □

Notice that the above proof is purely constructive and the statement of Claim 9.8.3 involves only finite combinatorics, therefore it can be performed in RCA_0.

Claim. *Let $\mathcal{T}$ be the transducer from Claim 9.8.3. If the input α to $\mathcal{T}$ contains an accepting path then so does the output $\mathcal{T}(\alpha)$.*

The rest of this subsection is devoted to a proof of Claim 9.8.3. Let α be an input to $\mathcal{T}$. Assume that $\pi \in (Q \times \mathbb{N})^{\mathbb{N}}$ is a path that contains infinitely many accepting edges in α. A node v in the Q-dag α is said to be π-*merging* if there exists a finite path in $\mathcal{T}(\alpha)$ that leads from v to a vertex on π. Our aim is to define the following set of vertices in $Q \times \mathbb{N}$:

$$t = \{v \in Q \times \mathbb{N} \mid v \text{ is } \pi\text{-merging}\}.$$

The above definition is clearly a Σ^0_1-definition of t.

Subclaim 9.8.7. *There exists a Π^0_1 predicate over vertices v equivalent to "v is π-merging". As a consequence, t is definable by Δ^0_1-comprehension.*

The proof of this subclaim makes essential use of Σ^0_2-IND and is similar to the proof of Theorem 9.7.1.

Proof. For $i = 0, 1, \ldots, |Q|$ we will say that i is *π-merging infinitely often* if

$$\forall j\, \exists k{>}j.\ \text{there are at least } i\ \pi\text{-merging vertices of the form } (q,k) \text{ in } \mathcal{T}(\alpha).$$

The above property of i is clearly a Π^0_2 property. Let i_0 be the maximal $i \leq |Q|$ that is π-merging infinitely often. Such i_0 exists by Σ^0_2-IND. Clearly if $i \leq i'$ and i' is π-merging infinitely often then i is also π-merging infinitely often. By the definition, if $i > i_0$ then there exists $j(i)$ such that for all $k > j(i)$ there are fewer than i π-merging vertices of the form (q,k) in $\mathcal{T}(\alpha)$. Notice that we can assume $j_0 := j(i_0 + 1)$ to be an upper bound for all $j(i)$ where $i_0 < i \leq |Q|$. This means that if $k > j_0$ then there are at most i_0 π-merging vertices of the form (q,k) in $\mathcal{T}(\alpha)$.

We can now provide a Π^0_1-definition of t (actually a Σ^0_1-definition of the vertices outside t). A vertex $v = (q,k)$ does not belong to t if ($\star$): there exists $k' > \max(k, j_0)$ and i_0 vertices of the form $v_0 = (q_0, k')$, $v_1 = (q_1, k')$, $\ldots$, $v_{i_0} = (q_{i_0}, k')$ such that:

- all the vertices $v_0, \ldots, v_{i_0}$ are π-merging in $\mathcal{T}(\alpha)$,
- no path from v to any of v_i for $i = 0, 1, \ldots, i_0$ exists,
- there is no path in $\mathcal{T}(\alpha)$ from v to a vertex of the form (q', ℓ) that lies on π with $\ell \leq k'$.

The latter two conditions are decidable, while the first one is Σ^0_1. In total, the condition ($\star$) is Σ^0_1.

We will now prove that the negation of ($\star$) in fact defines t. First assume that $v = (q,k) \notin t$. Recall that there are infinitely many k' such that there are exactly i_0 π-merging vertices of the form (q', k') in $\mathcal{T}(\alpha)$. In particular, there exists $k' > \max(k, j_0)$ and i_0 vertices of the form $v_0 = (q_0, k')$, $v_1 = (q_1, k')$, $\ldots$, $v_{i_0} = (q_{i_0}, k')$ such that all of them are π-merging. Since v is not π-merging, there cannot be a path from v to any of the vertices v_i for $i = 1, 2, \ldots, i_0$. Similarly, there cannot be a path from v to π. Therefore, v satisfies ($\star$).

On the other hand, assume that v has the property ($\star$) as witnessed by some k' and vertices $v_0, \ldots, v_{i_0}$. Assume to the contrary that v is π-merging. Let this be witnessed by a path w from v to a vertex $v'' = (q'', k'')$ on π. By the last item of ($\star$), we must have $k'' > k'$. Let $p \in Q$ be the state such that (p, k') lies on the path w. Clearly (p, k') is π-merging so it needs to be one of the vertices $v_1, \ldots, v_{i_0}$. But in that case this vertex can be reached from v by a path in $\mathcal{T}(\alpha)$, a contradiction. □

We can now apply Bounded-width König's Lemma (see Definition 8.3.1) to the graph with set of vertices t and with edges inherited from $\mathcal{T}(\alpha)$. This graph has arbitrarily long finite paths starting in $(q_0, 0)$, because each vertex on π belongs to t and is reachable from $(q_0, 0)$ by a path in $\mathcal{T}(\alpha)$ contained within t. We obtain an infinite path π' in $\mathcal{T}(\alpha)$ contained within t. Our aim is to prove that π' contains infinitely many accepting edges. Assume to the contrary that for some $k \in \mathbb{N}$ there is no accepting edge of the form $((p,\ell),(p',\ell+1))$ for $\ell > k$ on π'. Let (p,k) be a vertex that belongs to $\pi' \cap Q \times \{k\}$. Since π' is a path in t, we know that (p,k) is π-merging. Let w be a path witnessing this fact and let (p', k') be its final vertex, which lies on π. Since π is accepting, we know that it contains an accepting edge of the form $((r,\ell),(r',\ell+1))$ with $k < \ell$. Let $(q, \ell+1)$ be a vertex that belongs to $\pi' \cap Q \times \{\ell+1\}$. As in the case of (p,k), we have a path w' witnessing that $(q, \ell+1)$ is π-merging, which reaches π in a vertex (q', ℓ').

This means that in α there are two paths between (p,k) and (q', ℓ') (see Figure 9.5): the first one follows w and π, the second one follows π' and w'. Notice that the latter path is contained in t. This means that the profile of the path through π' and w' is smaller than the profile of the path through w and π. By the definition of the order on profiles, since there is an accepting edge on the respective fragment of π, the corresponding fragment of the path π' needs to contain an accepting edge. This contradicts the assumption that there is no accepting edge of the form $((p,k''),(p',k''+1))$ for $k'' > k$ on π'.

This concludes the proof of Claim 9.8.3 and thus of Lemma 9.8.5.

9.8.4 Recognising accepting tree-shaped Q-dags

The proof of Theorem 9.8.1 is concluded by the following lemma and an application of Lemma 9.8.3.

Lemma 9.8.8. *There exists a deterministic Rabin automaton $\mathcal{A}$ over the alphabet $[Q]$ that for every tree-shaped Q-dag $\alpha'' \in [Q]^{\mathbb{N}}$ accepts it if and only if α'' contains an accepting path.*

We will start by defining the states and transitions of the constructed Rabin automaton. Then we will prove that it in fact verifies if a given infinite word that is a tree-shaped Q-dag contains an accepting path.

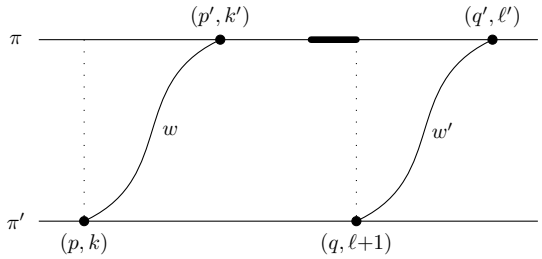


Figure 9.5: An illustration to the proof of Claim 9.8.3. The upper horizontal line is the path π in α that may not be a path in $\mathcal{T}(\alpha)$. The paths w and w' witness that (p, k) and $(q, \ell{+}1)$ are both π-merging. The boldfaced part of π is the chosen accepting edge that appears on π. Among the two paths from (p, k) to (q', ℓ'): one through w and the other through w'; the latter belongs to $\mathcal{T}(\alpha)$. Therefore, it has to have smaller profile than the former, in particular it has to contain an accepting edge in between the vertices (p, k) and $(q, \ell + 1)$.

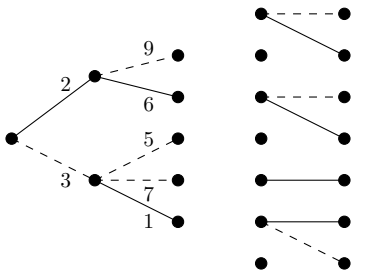


Figure 9.6: A Q-scheme τ (a state of $\mathcal{A}$) and a tree-shaped letter $M \in [Q]$ encountered by $\mathcal{A}$. The "non-accepting" edges in τ are dashed. The leaves of τ are arranged according to some fixed order on Q in such a way as to match the layout of $M \in [Q]$. To simplify the picture we do not include the states in Q labeling the nodes of τ, using dots instead.

In general, the size of the constructed Rabin automaton is one of the crucial parameters of the construction, as it influences the running time of the algorithms for verification and synthesis of reactive systems. However, in this work we are mainly focused on the fact that an equivalent deterministic automaton exists. Therefore, the relatively simple construction presented here will be far from optimal. For a discussion on optimality of the constructions involved, see [19]. We conjecture that soundness of more optimal determinization procedures, such as *Safra's construction* [62], may be proven in Σ^0_2-IND.

Definition 9.8.9. *Fix a finite nonempty set Q. We will say that τ is a* Q-scheme *if τ is a finite tree with:*

- *internal nodes labelled by Q,*
- *leaves uniquely labelled by Q,*
- *edges uniquely labelled by $\{0, 1, \ldots, 2 \cdot |Q|\}$, these labels are called* identifiers*,*
- *each edge additionally marked as either "accepting" or "non-accepting".*

Additionally, the root cannot be a leaf and every node of τ that is neither the root nor a leaf has to have at least two children.

Notice that we are not requiring a Q-scheme to be balanced as a tree. It is easy to see that since the leaves of τ are uniquely labelled by Q, τ has at most $2 \cdot |Q|$ nodes. Therefore, the requirement that the edge labels from $\{0, \ldots, 2 \cdot |Q|\}$ need to be pairwise distinct is not restrictive. Clearly the number of Q-schemes is finite (in fact exponential in $|Q|$). Let the set of states of $\mathcal{A}$ be the set of all Q-schemes. Let the initial state of $\mathcal{A}$ be the Q-scheme consisting of two nodes: the root and its only child, both labelled by q_0. Let the edge between the root and the unique leaf be labelled by the identifier 0 and be "non-accepting".

We will now proceed to the definition of the transitions of $\mathcal{A}$. Assume that the automaton is in a state τ and reads a tree-shaped letter $M \in [Q]$, see Figure 9.6.

The resulting state τ' is constructed by performing the following four steps depicted on Figure 9.7.

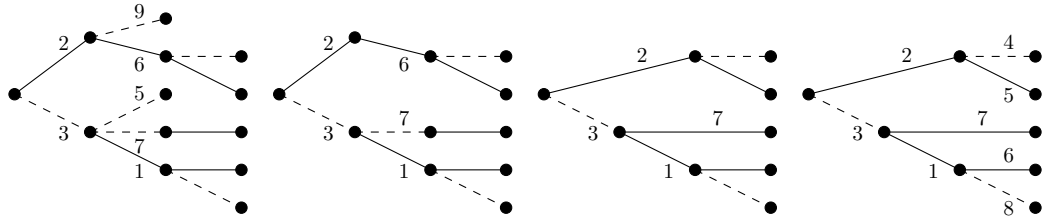


Figure 9.7: The successive transformations of the scheme τ when performing steps 1 to 4 of a transition of $\mathcal{A}$.

Step 1. We append the new letter M to the Q-scheme τ obtaining a new tree. The identifiers on the newly created edges are undefined and some nodes may have exactly one child. However, all the nodes are labelled by states in Q, either coming from τ or from M.

Step 2. We eliminate paths that die out before reaching the target states of M. In the running example, this means eliminating edges with identifiers 9 and 5.

Step 3. We eliminate unary nodes, thus joining several edges into a single edge. This means that a path which only passes through nodes of degree one gets collapsed into a single edge, the identifier for such an edge is inherited from the first (i.e. leftmost) edge on the path. The newly created edge is "accepting" if and only if any of the collapsed edges were "accepting". In the running example, this means eliminating the unary nodes that are the targets of edges with identifiers 2 and 7.

Step 4. Finally, if there are edges that do not have identifiers, these edges get assigned arbitrary identifiers that are not currently used. In the running example we add identifiers 4, 5, 6, and 8.

This completes the definition of the state update function. We now define the acceptance condition.

The acceptance condition. When executing a transition, the automaton described above goes from one Q-scheme to another Q-scheme. For each identifier, a transition can have three possible effects, described below:

Delete An edge can be deleted in Step 2 (it dies out) or in Step 3 (it is merged with a path to the left). The identifier of such an edge is said to be *deleted* in the transition. The deleted identifiers in the running example are 9, 5, and 6. Since we reuse identifiers, an identifier can still be present after a transition that deletes it, because it has been added again in Step 4. This happens to identifiers 5 and 6 in the running example.

Refresh In Step 3, an entire path with edges identified by $e_1, e_2, \cdots, e_k$ is folded into its first edge identified by e_1. If any of the edges identified by $e_2, \cdots, e_n$ was "accepting" then we say that the identifier e_1 is *refreshed*. In the running example the refreshed identifiers are 2 and 7 (the edge identified by 2 was already "accepting" while the edge identified by 7 become "accepting" because of the merging).

Nothing An identifier might be neither *deleted* nor *refreshed*. In the running example, this is the case for identifiers 1 and 3.

The following lemma describes the key property of the above data structure.

Lemma 9.8.10. *For every tree-shaped Q-dag $\alpha \in [Q]^{\mathbb{N}}$, the following are equivalent:*

1. *α contains an accepting path,*
2. *some identifier is deleted only finitely often but refreshed infinitely often.*

Before proving the above lemma, we show how it completes the proof of Lemma 9.8.8. Clearly, the second condition above can be expressed as a Rabin condition on transitions of $\mathcal{A}$—the Rabin pairs (E_i, F_i) range over the set of identifiers $i = 1, \ldots, 2 \cdot |Q|$, a transition is in E_i if an edge with the identifier i is deleted and is in F_i if the edge is refreshed.

Proof of Lemma 9.8.10. First assume that α contains an accepting path π. Let ρ be the sequence of states of $\mathcal{A}$ when reading α. Notice that for every k, the path π induces a path in the Q-scheme $\rho(k)$ that connects the root with a leaf labelled by a state $q(k)$ such that $\pi(k) = (q(k), k)$. Let $e_0^{(k)}, \ldots, e_{j(k)}^{(k)}$ be the identifiers of the edges on this path. Notice that $j(k) \leq |Q|$ because each internal node of a Q-scheme has at least two children and leaves of Q-schemes are uniquely labelled by the states in Q. We will say that a position $j = 0, 1, \ldots, |Q|$ is *unstable* if for infinitely many k either $j(k) < j$ or some identifier $e_{j'}^{(k)}$ for $j' \leq j$ is *deleted* in the k-th transition in ρ. Notice that 0 is *stable* because we never delete the first edge of a Q-scheme. Let j_0 be the greatest *stable* number; such a number exists by Σ_2^0-IND.

By Σ_2^0-collection we can find a number k_0 such that for $k \geq k_0$ we have $j(k) \geq j_0$ and no identifier $e_{j'}^{(k)}$ with $j' \leq j_0$ is *deleted* in the k-th transition in ρ. Therefore, for every $j' \leq j_0$ and $k \geq k_0$ we have

$$e_{j'}^{(k)} = e_{j'}^{(k_0)}.$$

Let $i = e_{j_0}^{(k)}$. Clearly by the definition of j_0 we know that the identifier i is not deleted for $k \geq k_0$. It remains to prove that i is refreshed infinitely many times. Assume to the contrary that for some $k_1 \geq k_0$ and every $k \geq k_1$ the identifier i is never refreshed in the k-th transition in ρ. First notice that π contains an accepting edge of the form $((q, k_2 - 1), (q', k_2))$ for some $k_2 \geq k_1$. The edge identified by $e_{j(k_2)}^{(k_2)}$ is accepting in $\rho(k_2)$—this is the last edge on the path corresponding to π in the Q-scheme obtained after reading the k_2-th letter of α. There are two cases. If $j(k_2) = j_0$, then i is refreshed in the k_2-th transition, contradicting our assumption that i is not refreshed beyond k_1. Otherwise, $j(k_2) \geq j_0 + 1$ and, by the definition of j_0 we know that for some $k_3 \geq k_2$ the identifier $e_{j_0+1}^{(k_3)}$ is deleted in the k_3-th transition in ρ. Notice that since π is an infinite path, this identifier cannot be deleted in Step 2 as it never dies out. Therefore, it must be the case that $e_{j_0+1}^{(k_3)}$ is deleted in Step 3 and that $j(k_3 + 1) = j_0$. Let us prove by Σ_1^0-IND on $k = k_2, k_2 + 1, \ldots, k_3$ that either:

- the identifier i is refreshed in the k'-th transition of ρ for some k' such that $k_2 \leq k' \leq k$, or
- there exists an accepting edge in the Q-scheme $\rho(k)$ that is identified by $e_{j'}^{(k)}$ for some j' such that $j_0 < j' \leq j(k)$.

For $k = k_2$ the second possibility holds. The inductive step follows directly from the definition of the transitions of $\mathcal{A}$—an accepting edge propagates to the left, firing successive refreshes for the merged identifiers. For $k = k_3$ we know that there is no j' such that $j_0 < j' \leq j(n)$ thus the first possibility needs to hold. This contradicts our assumption that there was no refresh on i after the k_1-th letter of α was read. This concludes the proof of the first implication in Lemma 9.8.10.

Now assume that α is a tree-shaped Q-dag accepted by the automaton $\mathcal{A}$. Let us fix the run ρ of $\mathcal{A}$ over α and assume that i_0 is an identifier that is deleted only finitely many times but refreshed infinitely many times. Let k_0 be such that the identifier i_0 is never deleted after the k_0-th transition of $\mathcal{A}$. Our aim is to prove that the Q-dag α contains an accepting path.

We start by noticing that for every $k \geq 0$ and an edge identified by e in the Q-scheme $\rho(k)$, this edge corresponds to a finite path $w_{k,e}$ in the Q-dag α. For the newly created edges that are assigned new identifiers in Step 4, the corresponding path is an edge $(q, k), (q', k')$ from the letter M. For edges that were assigned an identifier earlier, the path is defined inductively, by merging the paths whenever we merge edges in Step 3. Using Σ_1^0-IND we easily prove that a corresponding edge is marked "accepting" if and only if the path contains an accepting edge in α. If an identifier i is refreshed then the path gets longer and contains at least one new accepting transition.

In this way, we can track the path corresponding to the edges identified by i_0 for $k \geq k_0$. Since the identifier i_0 is refreshed infinitely many times, the path corresponding to it is prolonged infinitely many times. Notice that the source of the paths corresponding to i_0 is fixed and of the form $(q(k_0), k_0)$—the identifier i_0 is never merged to the left. Clearly, to every $k \geq k_0$ we can effectively assign a state $q(k)$ such that for some $k' > k_0$ the path w_{k',i_0} passes through $(q(k), k)$—such k' exists because i is refreshed infinitely many times. This gives us a Δ_1^0-definition of an infinite path π that starts in $(q(k_0), k_0)$. We can append it to a path from $(q_0, 0)$ to $(q(k_0), k_0)$ and obtain a path π' starting in $(q_0, 0)$. Notice that each refresh of i_0 corresponds to a new accepting edge on π, which means that π' is accepting. □

Chapter 10

MSO over countable orders

10.1 Ramseyan principles over $\mathbb{Q}$

In [63], one of the critical combinatorial lemmas in the proof of decidability of MSO over $\mathbb{Q}$ is an additive Ramsey Theorem over $\mathbb{Q}$. In [14], that theorem does not make an appearance, but a principle which we call the *Shuffle Lemma* takes its place.

Definition 10.1.1. *The* additive Ramsey Theorem over $\mathbb{Q}$ *is the following statement (originally proved in [63]): "for any finite semigroup S and any additive colouring $\alpha : [\mathbb{Q}]^2 \to S$, there exists a homogeneous set H which is dense in $]x, y[$ for some $x < y \in \mathbb{Q}$".*

Given a linear order $(P, \leq_P)$ and a function $\alpha : P \to \Sigma$, we say that a value $a \in \Sigma$ *occurs densely* in α if for every $x, y \in P$ there exists $z \in]x, y[$ such that $\alpha(z) = a$. We call α a *shuffle* if and only if for every $a \in \Sigma$, either a is not in the image of α or a occurs densely in α. If the image of α is some set X, we say that α is an *X-shuffle*. We say that α *contains a shuffle* if there exist $x, y \in P$ with $x < y$ such that $\alpha\big|_{]x,y[}$ is a shuffle.

Definition 10.1.2. *The* Shuffle Lemma *is the following statement: "for every $\alpha : \mathbb{Q} \to \Sigma$ with Σ finite, α contains a shuffle."*

Below we prove:

Theorem 10.1.3. *The following statements are equivalent over* RCA_0*:*

1. *the additive Ramsey Theorem over $\mathbb{Q}$,*
2. *for any finite semigroup S and any additive colouring $\alpha : [\mathbb{Q}]^2 \to S$, there exist $x, y \in \mathbb{Q}$ such that $]x, y[$ is partitioned into finitely many dense homogeneous subsets,*
3. *the Shuffle Lemma,*
4. Σ^0_2-IND*.*

We establish Theorem 10.1.3 in the following manner:

- we prove the Shuffle Lemma in $\mathsf{RCA}_0 + \Sigma^0_2$-IND (Lemma 10.1.4),
- we prove in RCA_0 that the Shuffle Lemma implies the strong form of the additive Ramsey Theorem over $\mathbb{Q}$ formulated as item 2. (Lemma 10.1.7),
- we then prove in RCA_0 that the usual form of the additive Ramsey Theorem over $\mathbb{Q}$ implies Σ^0_2-induction (Lemma 10.1.9).

Lemma 10.1.4. $\mathsf{RCA}_0 + \Sigma^0_2$-IND *proves the Shuffle Lemma.*

Proof. Let $\alpha : \mathbb{Q} \to \Sigma$ be a function with Σ finite. For any natural number n, consider the following Σ^0_2 formula $\varphi(n)$: "there exists a finite set $L \subset \Sigma$ of cardinality n and there exist $u, v \in \mathbb{Q}$ with $u < v$ such that $\alpha(w) \in L$ for every $w \in]u, v[$".

Since $\varphi(|\Sigma|)$ is true, it follows from the Σ^0_2 minimization principle that there exists a minimal n such that $\varphi(n)$ holds. Consider $u, v \in \mathbb{Q}$ and the set of colours L corresponding to this minimal n.

Claim. $\alpha\big|_{]u,v[}$ *is a shuffle.*

Proof of Claim. Let $a = \alpha(x)$ for some $x \in]u, v[$. We need to prove that a occurs densely in $]u, v[$. Consider arbitrary $x, y \in]u, v[$ with $x < y$. We are done if we show that there exists some $w \in]x, y[$ with $\alpha(w) = a$.

Suppose that there is no such w. By bounded Σ^0_1-comprehension, there exists a finite set $L' \subset \Sigma$ consisting of exactly those $b \in \Sigma$ which occur as values of $\alpha\big|_{]x,y[}$. Clearly, $\varphi(|L'|)$ holds. However, $L' \subseteq L$, and by assumption $a \notin L'$, so $|L'| < n$, contradicting the choice of n as the minimal number such that $\varphi(n)$. □

□

A fact that we need later on is that X-shuffles exist for arbitrary non-empty X.

Lemma 10.1.5. *Over* RCA_0*, for any non-empty* $X \subseteq \mathbb{N}$ *there is an* X*-shuffle with domain* $]0, 1[\cap \mathbb{Q}$.

Proof. Without loss of generality, it suffices to show the result for $X = \mathbb{N}$. Define $\alpha :]0, 1[\mapsto \mathbb{N}$ by $\alpha(\frac{a}{b}) = b$ where $\frac{a}{b}$ is written as an irreducible fraction. □

We now turn to the proof of the additive Ramsey theorem for pairs in $\mathbb{Q}$. Much like the proof for $\mathbb{N}$, we use some basic resuts in Green theory to streamline the proof. In addition to 9.1.6, we use the following elementary algebraic statement.

Lemma 10.1.6. *For any pair of elements* $x, y \in S$ *a finite semigroup, if we have* $x \leq_{\mathcal{R}} y$ *and* x, y $\mathcal{J}$*-equivalent, then* x *and* y *are also* $\mathcal{R}$*-equivalent.*

Lemma 10.1.7. *Provably in* RCA_0*, the Shuffle Lemma implies that for any finite semigroup* S *and any additive colouring* $\alpha : [\mathbb{Q}]^2 \to S$*, there exist* $x, y \in \mathbb{Q}$ *such that* $]x, y[$ *is partitioned into finitely many dense homogeneous subsets.*

Proof. Fix a finite semigroup $(S, \cdot)$ and an additive colouring $\alpha : [\mathbb{Q}]^2 \to S$. We say that a colour c occurs in $X \subseteq \mathbb{Q}$ if there exists $\{x, y\} \in [X]^2$ such that $\alpha(x, y) = c$.

We proceed in two stages: first, we find an interval $]u, v[$ such that all colours occurring in $]u, v[$ are $\mathcal{J}$-equivalent to one another. Then we find a subinterval of $]u, v[$ partitioned into finitely many dense homogeneous sets.

Claim. *There exists* $\{u, v\} \in [\mathbb{Q}]^2$ *such that all colours of* $\alpha\big|_{]u,v[}$ *are* $\mathcal{J}$*-equivalent to one another.*

Proof of Claim. Fix an enumeration $(q_n)_{n\in\mathbb{N}}$ of the rationals. Consider the colouring $\beta : \mathbb{Q} \to S$ given by:

$$q_n \mapsto \alpha\left(q_n, q_n + \frac{1}{n+1}\right).$$

By the Shuffle Lemma, there exists some interval I_0 in which every value of β occurs either densely or not at all. There exists some k high enough such that, additionally, $I_1 :=]q_k, q_k + \frac{1}{k+1}[\subseteq I_0$. Set $c_1 = \alpha(q_k, q_k + \frac{1}{k+1})$.

Subclaim 10.1.8. *For every* $\{x, y\} \in [I_1]^2$ *it holds that* $\beta(x, y)$ $\mathcal{J}$ c_1.

Proof of Subclaim. Take $\{x, y\} \in [I_1]^2$ and $c = \alpha(x, y)$. We have $c_1 \leq_{\mathcal{J}} c$ since $c_1 = \alpha(q_k, x) \cdot c \cdot \alpha(y, q_k + \frac{1}{k+1})$. But, since c_1 occurs densely in $]x, \frac{x+y}{2}[$, there are infinitely many ℓ such that $x < q_\ell < \frac{x+y}{2}$ and $\beta(q_\ell) = \alpha(q_\ell, q_\ell + \frac{1}{\ell+1}) = c_1$. We can choose such ℓ high enough that $]q_\ell, q_\ell + \frac{1}{\ell+1}[\subseteq]x, y[$, which gives $c \leq_{\mathcal{J}} c_1$ and so c $\mathcal{J}$ c_1. □

□

Moving on to stage two of the proof, we want to look for a subinterval of $I_1 =]u, v[$ from the Claim partitioned into finitely many dense homogeneous sets. To this end, define the following colouring $\gamma : I_1 \to S^2$:

$$z \mapsto (\alpha(u, z), \alpha(z, v)).$$

By the Shuffle Lemma, there exist $x, y \in I_1$ with $x < y$ such that every value of γ either occurs densely in $]x, y[$ or not at all. For $l, r \in S$, define $H_{l,r} := \gamma^{-1}(\{(l, r)\}) \subseteq]x, y[$; note that this is a set by bounded Σ^0_1-comprehension. Clearly, all $H_{l,r}$ are either empty or dense in $]x, y[$, with $]x, y[= \bigcup_{l,r} H_{l,r}$. Since there are finitely many pairs (l, r), all we have to prove is:

Claim. *Each non-empty* $H_{l,r}$ *is homogeneous for* α.

Proof of Claim. Let $c = \alpha(x, y)$ such that $x, y \in H_{l,r}$ with $x < y$. By additivity of α and the definition of $H_{l,r}$,

$$cr = \alpha(x, y)\alpha(y, v) = \alpha(x, v) = r. \tag{10.1}$$

In particular $r \leq_{\mathcal{R}} c$. But we also have $r \mathcal{J} c$, which gives $r \mathcal{R} c$ by Lemma 10.1.6. This shows that all the colours occurring in $H_{l,r}$ are $\mathcal{R}$-equivalent to one another. A dual argument shows that they are all $\mathcal{L}$-equivalent, so they are all $\mathcal{H}$-equivalent. Clearly, the assumptions of Lemma 9.1.6 are satisfied, so their $\mathcal{H}$-class is actually a group.

All that remains to be proved is that any colour c occurring in $H_{l,r}$ is actually the (necessarily unique) idempotent of this $\mathcal{H}$-class. Since $r \mathcal{R} c$, there exists a such that $c = ra$. But then by (10.1), $cc = cra = ra = c$, so c is necessarily the idempotent.

Thus, $H_{l,r}$ is homogeneous. □

□

Remark. *The above method of proof is a Green relation-based take of Shelah's proof in [63].*

This proof follows the same pattern as the proof of the additive Ramsey over ω: first we isolate the $\mathcal{J}$-classes using an "ordered colouring", and then one deals with the semigroup structure in a similar way, using the Shuffle Lemma instead of the infinite pigeonhole principle.

We have a loose correspondence of the following three principles in the proofs of additive Ramsey over $\mathbb{N}$, arbitrary ordinals and $\mathbb{Q}$: the infinite pigeonhole principle, the unboundedness principle and the Shuffle Lemma.

Lemma 10.1.9. *Provably in* RCA_0*, the additive Ramsey Theorem implies* Σ^0_2-IND.

Proof. We work in RCA_0 and assume the Additive Ramsey principle. It is enough to prove that given a Π^0_2 formula $\varphi(j)$ and a number ℓ, if there is any $j \leq \ell$ such that $\varphi(j)$, then there is a maximal such j. By a standard normal form for Π^0_2 formulas, we may assume w.l.o.g. that $\varphi(j)$ has the form

$$\exists^\infty n\, \delta(j, n) := \forall m\, \exists n \geq m\, \delta(j, n),$$

where δ is Δ^0_0. Moreover, modulo some simple manipulation, we may also assume that for each n there is exactly one $j \leq \ell$ such that $\delta(j, n)$.

We will use φ to define a colouring over the dense linear order $(D, \leq)$ of *dyadic numbers*, the suborder of $\mathbb{Q}$ defined by $D = \{\frac{m}{2^k} \mid m \in \mathbb{Z}, k \in \mathbb{N}\}$. Since RCA_0 knows that any two (countable) dense linear orders without endpoints are isomorphic, the additive Ramsey Theorem holds over D as well.

For $x \in D$, let the *rank* of x, $\mathrm{rk}(x)$, be the least $k \in \mathbb{N}$ such that $x = \frac{m}{2^k}$ for some $m \in \mathbb{Z}$. There are two simple but important facts to note about ranks. Firstly, for any interval $]x, y[\subseteq D$ and any $k \in \mathbb{N}$, there are only finitely many elements of $]x, y[$ with rank $< k$, so there exists a subinterval $]x', y'[\subseteq]x, y[$ which contains only elements of rank $\geq k$. Secondly, for any $]x, y[\subseteq D$, all but finitely many ranks occur in $]x, y[$.

Define $\alpha : D \to \{0, \dots \ell\}$ by:

$$\alpha(x) = j \text{ iff } \delta(j, \mathrm{rk}(x)).$$

This is correctly defined by our assumptions on δ. Moreover, by properties of rank, for any $]x, y[\subseteq D$, the colour j occurs densely in $]x, y[\subseteq D$ exactly if $\varphi(j)$ holds.

Now define $\beta : [D]^2 \to \{0, \dots \ell\}$ by:

$$\beta(x, y) = \max(\{\alpha(z) : x < z < y, \mathrm{rk}(z) \leq \max(\mathrm{rk}(x), \mathrm{rk}(y))\}).$$

Since we are maximizing α over a finite set of z's, the colouring β is computable and therefore available in RCA_0.

Apply the additive Ramsey Theorem to β, obtaining a homogeneous set H dense in some interval $]x, y[\subseteq D$. Let j be the colour of H. It remains to prove that j is the maximal number below ℓ satisfying $\varphi(j)$.

On the one hand, j has to occur densely in $]x, y[$ as a value of α, which means that $\varphi(j)$ holds. On the other hand, assume that $j < j' \leq \ell$ and that $\varphi(j')$ holds. Let $u \in H$. Since all but finitely many ranks occur in $]x, y[$, there is some $z \in]x, y[$ such that $\delta(j', \mathrm{rk}(z))$. W.l.o.g., $u < z$. Now, find an interval $I \subseteq]z, y[$ with no elements of rank $< \mathrm{rk}(z)$ and let $v \in I \cap H$. Then, since $u, v \in H$, we have $\beta(u, v) = j$. However, since $u < z < v$ and $\mathrm{rk}(z) \leq \mathrm{rk}(v)$ but $\alpha(z) = j'$, we also have $\beta(u, v) \geq j'$, which is a contradiction. □

10.2 Consequences of decidability of MSO($\mathbb{Q}$)

In this section we establish so-called "reversals", namely implications from the decidability of MSO($\mathbb{Q}$) to principles axiomatizing strong fragments of second-order arithmetic. These implications can be viewed as proof-theoretical lower bounds for the decidability theorem. We prove two kind such lower bounds:

- Firstly, much like in Proposition 9.4.1, we derive induction schemes from decidability of MSO. The hypothesis here is that we suppose that there exists some algorithm deciding the MSO theory.
- Second, we give examples of statements which are expressible in MSO which are equivalent to comprehension schemes. While this does not show that decidability of MSO requires necessarily those axioms in the absolute, it shows that the soundness of the *usual* algorithm, which can be shown to be correct in, say, ZF.

10.2.1 Preliminaries on linear orders

Before embarking in the proof of the reversals, we first make a few generalities on MSO and linear orders. The syntax of MSO formulas over linear orders is given by:

- First-order logic with an atomic predicate for the underlying order $<$.
- Quantification over sets of elements, together with a set membership relation.

$$\varphi, \psi ::= x < y \mid x \in X \mid \varphi \wedge \psi \mid \neg\varphi \mid \exists x\ \varphi \mid \exists X\ \varphi$$

Given an arbitrary (countable) order $(X, <)$, the formulas are interpreted in the expected way. Recall however that the satisfaction for MSO formulas is only defined up to an externally fixed number of quantifier alternation at a time. Given a predicate variable X, one may define the relativization $(\varphi \restriction X)$ of a formula φ with respect to the set X by recursion over φ

$$\begin{array}{lcl}
(x < y \restriction X) & = & x < y \\
((x \in Y) \restriction X) & = & x \in Y \\
((\varphi \wedge \psi) \restriction X) & = & (\varphi \restriction X) \wedge (\psi \restriction X) \\
((\neg\varphi) \restriction X) & = & \neg(\varphi \restriction X) \\
((\exists x\ \varphi) \restriction X) & = & \exists x\ (x \in X \wedge (\varphi \restriction X)) \\
((\exists Y\ \varphi) \restriction X) & = & \exists Y\ (Y \subseteq X \wedge (\varphi \restriction X))
\end{array}$$

where $Y \subseteq X$ is a shorthand for $\forall x. x \in Y \Rightarrow x \in X$. With respect to truth, for an arbitrary order $(P, <)$, if given a subset $Q \subseteq P$, a MSO formula φ and a valuation $\rho : \mathsf{FV}(\varphi) \to P \cap \mathcal{P}(P)$, we have $(P, <) \models_\rho \varphi$ if and only $(Q, <) \models_{\rho, X \leftarrow Q} (\varphi \restriction X)$.

A first remark concerning $\mathbb{Q}$ is that it is universal among countable linear orders in the following sense.

Lemma 10.2.1. *We work in* RCA_0. *For every countable linear order* $(X, <_X)$, *there exists an order homomorphism* $i : (X, <) \to (\mathbb{Q}, <)$.

Proof sketch. The basic idea is to recall that elements of X may be seen as natural numbers build i by recursion as follow:

- If $n \notin X$, then n is not in the domain of i.
- Otherwise, consider the set $I_n = \mathrm{dom}(i) \cap [\![0, n-1]\!]$. We then have three alternatives:
  - Either $n <_X k$ for every $k \in I_n$, in which case we set $i(k)$ to be strictly less than all elements of I_n according to the order over $\mathbb{Q}$.
  - We proceed similarly if $k <_X n$ for every $k \in I_n$.
  - Otherwise, there is a maximal $k \in I_n$ and minimal $k' \in I_n$ such that $k <_X n <_X k'$. We then set $i(n)$ to be strictly between $i(k)$ and $i(k')$.

It is possible to write an algorithm computing i and to show it sound with respect to the above specification within RCA_0. Then it is easily seen to be an order-homomorphism. □

In [27], Hausdorff studied inductive decomposition of linear orders as lexicographic sums. A crucial notion in this analysis is the notion of *scattered* and *dense* orders.

Definition 10.2.2. *Let $(L, <_L)$ be a linear order. $X \subseteq L$ is* dense in itself *if and only if, for every $x, y \in L$, there exists $z \in X$ such that $z \in]x, y[$ and X is non-empty. A linear order $(L, <_L)$ is* scattered *if and only if no $X \subseteq L$ is dense in itself.*

Remark. *Note that, up to isomorphism, there are only four dense in themselves countable linear orders: $\mathbb{Q}$ and the variants of $\mathbb{Q}$ with endpoints ($\mathbb{Q} \cup \{+\infty\}$, $\mathbb{Q} \cup \{-\infty\}$ and $\mathbb{Q} \cup \{-\infty, +\infty\}$). This is provable by back-and-forth within* RCA_0.

Hausdorff's theorems give decomposition result for scattered and non-scattered linear orders using the notion of lexicographic sum.

Definition 10.2.3. *Let $(I, <)$ be a linear order and $(P_i, <_i)_{i \in I}$ a family of countable linear orders indexed over I. The lexicographic sum is the order $(\sum_{i \in I} P_i, <_{lex})$ has for underlying set the set of pairs (i, j) such that $i \in I$ and $j \in P_i$ and for order the lexicographic order: we have $(i, j) <_{lex} (i', j')$ if either $i < i'$ or $i = i'$ and $j < j'$.*

Lexicographic product of orders $(I, <)$ and $(J, <)$ are particular cases of lexicographic sum where the family $(P_i, <_i)_{i \in I}$ is constat equal to $(J, <)$. In the context of reverse mathematics where all orders are countable and have for carrier a subset of $\mathbb{N}$, RCA_0 shows that the lexicographic sum of linear orders exist and are indeed linear orders.

Hausdorff's analysis, suitably restricted to countable orders, was studied from the point of view of Reverse Mathematics in [17] and [23]. Two theorems are of importance: the inductive characterization of countable scattered orders and the decomposition of arbitrary countable orders as a sum of scattered orders. As far as Reverse Mathematics are concerned, the following result of Clote is going to be used to show that MSO over $\mathbb{Q}$ can express Π^1_1-CA_0.

Theorem 10.2.4 ([17])**.** *Over ACA_0, the following are equivalent:*

- Π^1_1-CA_0
- *every linear order P is either scattered, or $P \simeq \sum_{d \in D} P_d$ where D is dense in itself and P_d are all scattered and non-empty.*

10.2.2 Induction from decidability

We rely on a trick similar to the one employed in Theorem 9.4.1. There, we used the fact that MSO over the naturals can express a Σ^0_2-complete property to show that its decidability implies Σ^0_2-IND. Here, we notice that MSO over $\mathbb{Q}$ can express a Π^1_1-complete property: well-foundedness.

Theorem 10.2.5. *Provably in ACA_0, if there exists an algorithm deciding the depth-7 fragment of the MSO theory of $(\mathbb{Q}, \leq)$, then Π^1_1-IND holds.*

Proof. Here, we use the fact that MSO over the rationals can express a Π^1_1-complete property to show that its decidability implies Π^1_1-IND. For $k \in \mathbb{N}$, let ψ_k be the MSO sentence

$$\forall X_0 \, \forall X_1 \, \ldots \forall X_k \left[\bigvee_{-1 \leq i \leq k+1} \left(X_i \text{ is well-ordered } \wedge \bigwedge_{i < j \leq k} (\neg X_j \text{ is well-ordered }) \right) \right],$$

where "X is well-ordered" is an MSO formula stating in a natural way that each non-empty subset of X has a smallest element (in the ordering of $\mathbb{Q}$). Thus, ψ_k essentially says that if at least one of $k+1$ sets $X_0, \ldots, X_k \subseteq \mathbb{Q}$ is well-ordered, then there is a highest i for which X_i is well-ordered. Intuitively, ψ_k says that Π^1_1-induction holds up to k. Already RCA_0 proves that $\psi_0 \in \mathsf{MSO}(\mathbb{Q})$ and for every $k \in \mathbb{N}$, if $\psi_k \in \mathsf{MSO}(\mathbb{Q})$, then $\psi_{k+1} \in \mathsf{MSO}(\mathbb{Q})$. Moreover, each ψ_k can be written as a depth-7 sentence, so the existence of an algorithm deciding the depth-7 fragment of $\mathsf{MSO}(\mathbb{Q})$ would imply that $\psi_k \in \mathsf{MSO}(\mathbb{Q})$ for all $k \in \mathbb{N}$ (since "$\psi_k \in \mathsf{MSO}(\mathbb{Q})$" would then be a decidable property of k, and RCA_0 has induction for decidable properties).

Now, assume $\psi_k \in \mathsf{MSO}(\mathbb{Q})$ for all k and let $\pi(x)$ be a Π^1_1 property such that $\pi(0)$ but $\neg\pi(\ell)$ holds for some $\ell \in \mathbb{N}$. We have to show that there is a maximal $i \leq \ell$ such that $\pi(i)$. ACA_0 proves that $\pi(i)$ is equivalent to the well-ordering of the *Kleene-Brouwer ordering*$\mathrm{KB}(T_i)$, where $(T_i)_{i \leq \ell}$ is a sequence of trees definable by arithmetical comprehension. Define X_i to be the range of a computable embedding of $\mathrm{KB}(T_i)$ into $\mathbb{Q}$. For each $i \leq \ell$, $\pi(i)$ holds exactly if X_i is well-ordered as a subset of $\mathbb{Q}$. Since ψ_ℓ is in $\mathsf{MSO}(\mathbb{Q})$, there is a maximal $i \leq \ell$ such that X_i is well-ordered, which is also the maximal $i \leq \ell$ such that $\pi(i)$. □

10.2.3 Comprehension as an MSO sentence

Now that we established that the mere decidability of $\mathsf{MSO}(\mathbb{Q})$ implies Π^1_1-IND over ACA_0, we show that $\mathsf{MSO}(\mathbb{Q})$ can express a theorem $\psi_{\Pi^1_1\text{-}\mathsf{CA}_0}$ equivalent to Π^1_1-CA_0 over ACA_0. A fixed algorithm which can be shown to be sound in, say, ZF, deciding $\mathsf{MSO}(\mathbb{Q})$ should output "true" if taking $\psi_{\Pi^1_1\text{-}\mathsf{CA}_0}$ as input. For a fixed algorithm and a fixed sentence, this is witnessed by a concrete computation which can be reflected withing RCA_0; therefore, soundness of such an algorithm readily implies Π^1_1-CA_0.

Lemma 10.2.6. *There exists a sentence φ_{ACA_0} of MSO over $(\mathbb{N}^2, <_{lex})$ equivalent to ACA_0 over RCA_0.*

Proof. The sentence under consideration states that, for every subset $Z \subseteq \mathbb{N}^2$, there exists a set $X \subseteq \mathbb{N}^2$ such that:

- Z is included in X.
$$Z \subseteq X := \forall x\ (x \in Z \Rightarrow x \in X)$$
- X is successor and predecessor-closed: if $\dot{\mathsf{S}}(x, y)$ holds and either $x \in X$ or $y \in X$, then both $x, y \in Z$.
$$C(X) := \forall x\ y.\dot{\mathsf{S}}(x, y) \wedge (x \in X \vee y \in X) \Rightarrow x \in X \wedge y \in X$$
- X is the minimal such set.

Putting everything together, we obtain the following sentence

$$\psi := \forall X\ \exists Z\ \big(Z \subseteq X \wedge C(X) \wedge (\forall Y(Z \subseteq Y \wedge C(Y) \Rightarrow Z \subseteq Y))\big)$$

of quantifier depth less than 5. Now, suppose that $(\mathbb{N}^2, <_{\text{lex}}) \models_5 \psi$ and let $\varphi(n) = \exists m\ \delta(n, m)$ be an arbitrary Σ^0_1 formula (with possibly other parameters beyond n). Since δ is Δ^0_0, there exists $Z \subseteq \mathbb{N}^2$ such that $(n, m) \in Z$ if and only if $\delta(n, m)$ holds. Then, since ψ holds, we have some minimal X closed under successor and predecessor containing Z. Then we show that $\varphi(n) \Leftrightarrow (n, 0) \in X$ which suffices to conclude.

- If $\varphi(n)$ holds, then there exists m such that $(n, m) \in Z \subseteq X$. But since $C(X)$ holds, a Δ^0_0 induction over m shows that $(n, m) \in X \Rightarrow (n, 0) \in X$.
- Conversely, assume that for every m, $(n, m) \notin Z$. Define $\widetilde{X} = X \setminus \{(n, m) \mid m \in \mathbb{N}\}$. It is easy to check that $C(\widetilde{X})$ holds and that $Z \subseteq \widetilde{X}$. Consequently, $X \subseteq \widetilde{X}$ and thus $(n, 0) \notin X$.

□

Theorem 10.2.7. *There exists a true sentence $\psi_{\Pi^1_1\text{-}\mathsf{CA}_0}$ of MSO over $(\mathbb{Q}, \leq)$ which is equivalent to Π^1_1-CA_0 over RCA_0.*

The first step towards proving Theorem 10.2.7 is to first find a sentence of $\mathsf{MSO}(\mathbb{Q})$ which imply ACA_0. Thankfully, we may reuse Lemma 10.2.6 together with Lemma 10.2.1 as follows.

Lemma 10.2.8. *There exists a true sentence ψ_{ACA_0} of MSO over $(\mathbb{Q}, <)$ which is equivalent to ACA_0 over RCA_0.*

Proof. By Lemma 10.2.6, it suffices to find a sentence whose validity in $\mathbb{Q}$ is equivalent to the validity of φ_{ACA_0} in $\mathbb{N}^2$. To define φ_{ACA_0}, we first give a MSO sentence $I_{\mathbb{N}^2}$ which characterize subsets of $\mathbb{Q}$ which are order-isomorphic to $(\mathbb{N}^2, <_{\text{lex}})$. A first step is to give a similar sentence $I_{\mathbb{N}}$ for orders isomorphic to $(\mathbb{N}, <)$.

$$I_{\mathbb{N}} = \exists x\ (\forall y.x \leq y) \wedge \forall X.x \in X \wedge (\forall yz.y \in X \wedge \dot{\mathsf{S}}(y, z) \Rightarrow z \in X) \Rightarrow \forall z\ z \in X$$

$$I_{\mathbb{N}^2} = \exists X.(I_{\mathbb{N}} \restriction X) \wedge \forall Y.\exists x\ y.x \in X \wedge y \in X \wedge (\forall z.z \in Y \Leftrightarrow x \leq z \wedge z < y) \wedge (I_{\mathbb{N}} \restriction Y)$$

The sentence ψ_{ACA_0} is then

$$\forall Y.(I_{\mathbb{N}^2} \restriction Y) \Rightarrow (\varphi_{\mathsf{ACA}_0} \restriction Y)$$

where φ_{ACA_0} is given in Lemma 10.2.6. Note that RCA_0 proves that $(\mathbb{N}^2, <) \models I_{\mathbb{N}^2}$.

As every countable linear order embed into $\mathbb{Q}$ by Lemma 10.2.1, so does $\mathbb{N}^2$; let $Y \subseteq \mathbb{Q}$ be the corresponding subset of $\mathbb{Q}$. If $(\mathbb{Q}, <) \models \psi_{\mathsf{ACA}_0}$, then $(Y, <) \models \varphi_{\mathsf{ACA}_0}$ and thus $(\mathbb{N}^2, <) \models \varphi_{\mathsf{ACA}_0}$ and ACA_0 holds. Conversely, it is not difficult to check that any order $(P, <)$ such that $(P, <) \models I_{\mathbb{N}^2}$ is order-isomorphic to $(\mathbb{N}^2, <_{\text{lex}})$ in ACA_0[1], and that the converse thus holds. □

[1]However, Δ^0_1-comprehension is not enough to show that $\dot{\mathsf{S}}$ is indeed a function encodable as a set.

Then, we can safely reduce Theorem 10.2.7 to the following lemma.

Lemma 10.2.9. *There exists a true sentence $\psi'_{\Pi^1_1\text{-}\mathsf{CA}_0}$ of MSO over $(\mathbb{Q}, \leq)$ equivalent to $\Pi^1_1\text{-}\mathsf{CA}_0$ over ACA_0.*

Proof. The statement $\psi'_{\Pi^1_1\text{-}\mathsf{CA}_0}$ comes from the following mild reformulation of Theorem 10.2.4:

Claim. *Over ACA_0, the following are equivalent:*

- $\Pi^1_1\text{-}\mathsf{CA}_0$
- *every linear order P is either scattered, or there exists $Q \subseteq P$ such that*
  - *Q is dense in itself.*
  - *for every convex $X \subseteq P$ disjoint from Q, X is scattered.*
  - *for every $p \in P$, there exists a convex, scattered $X \subseteq P$ such that $p \in X$ and $X \cap Q \neq \emptyset$.*

Proof. We use Theorem 10.2.4 and show the equivalence with the second alternative. When P is scattered, both direction are trivial, so, without loss of generality, assume that P is not scattered.

First, if $P \simeq \sum_{d\in D} P_d$ where D is dense in itself and P_d are all scattered and non-empty. We prove the result for $\sum_{d\in D} P_d$, as it is rather straightforward to push through the order isomorphism $P \simeq \sum_{d\in D} P_d$. Since all P_d are non-empty, we may define a computable function $f : D \to \mathbb{N}$ such that for every d, $f(d) \in P_d$ (taking, for instance, the minimal element of P_d when seen as a subset of $\mathbb{N}$). Call Q the graph of f. We now have three things to check:

- Q is order-isomorphic to D, so it is dense in itself.
- Now assume that $X \subseteq \sum_{d\in D} P_d$ is convex and $X \cap Q = \emptyset$. Note that for every elements (d, x) and (d', x') of Q, $d' = d$; otherwise assume without loss of generality that $d < d'$. Since D is dense, we have some d'' such that $d < d'' < d'$, and thus $(d, x) < (d'', f(d'')) < (d', x')$. As X is convex, we should have $(d'', f(d'')) \in X$, which is impossible since $X \cap Q = \emptyset$. Hence, $Q \subseteq P_d$ for some $d \in D$. As a subset of a scattered subset of $\sum_{d\in D} P_d$, Q is thus scattered.
- Finally, for every $(d, x) \in \sum_{d\in D} P_d$, the set P_d is scattered and intersect Q at $f(d)$.

Conversely, assume that we have $Q \subseteq P$ is dense in itself such that every $X \subseteq P$ such that $X \cap Q = \emptyset$ is scattered and that for every $p \in P$, we do have a convex scattered subset Y such that $p \in Y$ and $Y \cap Q \neq \emptyset$. Define the family $(P_q)_{q\in Q}$ of subsets of P by arithmetical comprehension as follows

$$x \in P_q \quad \Leftrightarrow \quad \forall q' \in Q.\ (q' < q \Rightarrow q' < x) \wedge (q < q' \Rightarrow x < q')$$

For every $q \in Q$, $q \in P_q$. Furthermore, P_q is a partition of P into convex subsets:

- Every P_q is convex: suppose that we have $x < y$ with $x, y \in Q$ and $z \in [x, y]$ and an arbitrary $q' \in Q$. Either $q' < q$, in which case $q' < x \leq z$, or $q' > q$ and $z \leq y < q'$; thus $z \in Q$.
- If $q \neq q'$, $P_q \cap P_{q'} = \emptyset$: without loss of generality, assume that $q < q'$ and $x \in P_q \cap P'_q$. Since Q is dense in itself, there exists $q'' \in]q, q'[$. By definition of P_q, we have necessarily $x < q''$. However, by definition of $P_{q'}$, we have $q'' < x$, a contradiction.
- Finally, let us show that every $x \in P$ belongs to some P_q. By assumption, there exists a convex scattered set Y containing x and intersecting Q. Note that $Y \cap Q$ is necessarily a singleton. Otherwise, we would have $q < q' \in Q \cap Y$, and, since Y is convex, $[q, q'] \subseteq Y$, a dense subset of Y. Thus, let q be such that $Y \cap Q = \{q\}$; we show that $x \in P_q$. To this end suppose that we are given an arbitrary $q' \in Q$. Suppose that $q < q'$ (the symmetric case is treated similarly). We then have to show that $x < q'$; by contradiction, suppose that $q' \leq x$. Since Y is convex, we have $q' \in Y$, which contradicts $|Y \cap Q| = 1$.

We thus readily have $P \simeq \sum_{q\in Q} P_q$, with Q dense. It remains to show that every P_q is scattered and non-empty; the latter is immediate since $q \in P_q$ for every $q \in Q$. As for scatteredness, define the sets

$$\begin{aligned} P_q^+ &= \{x \in P_q \mid x > q\} \\ P_q^- &= \{x \in P_q \mid x < q\} \end{aligned}$$

Since the family $(P_q)_{q\in Q}$ is a partition and $q \in P_q$, we have $P_q^+ \cap Q = \emptyset$ and $P_q^- \cap Q = \emptyset$. Therefore, both P_q^+ and P_q^- are scattered. Since $P_q = P_q^- \cup \{q\} \cup P_q^+$ and scattered sets are closed under finite unions, P_q is therefore scattered. □

With this claim, it then suffices to notice that since every countable order embeds into $\mathbb{Q}$, $\mathsf{MSO}(\mathbb{Q})$ allow to quantify over a single countable order and to formalize density and scatteredness in MSO.

$$\begin{aligned}\mathsf{dense} &= (\exists x\ y.x < y) \wedge (\forall x\ y.x < y \Rightarrow \exists z.x < z \wedge z \wedge y)\\ \mathsf{scat} &= \forall X.\neg(\mathsf{dense} \restriction X)\end{aligned}$$

Therefore $\psi'_{\Pi^1_1\text{-}\mathsf{CA}_0} = \forall Z\ ((\mathsf{scat} \vee \exists Y\ \psi'') \restriction Z)$ where ψ'' is the conjunction

$$(\mathsf{dense} \restriction Y) \wedge \big(\forall V.V \cap Y = \emptyset \Rightarrow (\mathsf{scat} \restriction Y)\big) \wedge \forall x\ \exists y V.y \in V \wedge y \in Y \wedge x \in V \wedge (\mathsf{scattered} \restriction V)$$

where $V \cap Y = \emptyset$ formally stands for $\forall x\ \neg(x \in X \wedge x \in Y)$. □

Conclusion

As announced in the introduction, we have studied constructive aspects of MSO theories, and more specifically, MSO(ω) from two complementary perspectives. While Part I gave intuitionistic counterparts to MSO(ω) satisfying a Curry Howard correspondence for (finite-state) causal functions, Part II attempts to determine the metatheoretic assumptions required to make the classical standard MSO theories true within second-order arithmetic.

Part I starts by giving basic properties of Mealy machine in Chapter 2. While Mealy machines are a natural object to consider in automata theory, simply because it is a useful tool for intermediate constructions (see for instance Subsection 9.8.1 of Part II) which is central to the development of Part I as we make the choice to restrict our notion of realizer to only consider causal functions. Most things are left unsaid about the general theory of Mealy machines as one of the main focus is the guarded fixpoint construction, a crucial ingredient for the composition of strategies in zigzag games in Chapter 7. Although this does not serve in the rest of the thesis, a concrete syntax for finite-state causal functions with a sound and complete equational theory is given thanks to this fixpoint construction. Another preliminary move made in Chapter 2 is to show the equivalence between MSO(ω) and a first-order theory of streams FOM. This is rather uncontroversial from a purely technical standpoint and justified by the term language of FOM which includes all finite-state causal functions. As with parametric guarded fixpoints, this might also be seen as preliminary setup for Chapter 7 which would make little sense if we were working with natural base categories for (a fragment of) second-order arithmetic. Then, an intuitionistic subsystem SFOM of FOM is introduced in Chapter 3. After establishing that it is as expressive as FOM thanks to a simplified double-negation translation (amounting to Glivenko's theorem), a proof-relevant model of SFOM is given to justify extraction. The most interesting point, beyond the formal soundness and completeness of SFOM with respect to extraction, is that the model itself is based on a simple refinement of the usual translation of FOM formulas[2] into automata: the formulas are interpreted as automatas and the proof, instead of being mere witnesses of language inclusion with no computational content, are interpreted as simulations. A similar approach is taken in the subsequent Chapter 4 where a richer logic LSFOM based on intuitionistic linear logic is studied. A linear translation from the classical theory FOM is given, and a proof-relevant model for extraction is sketched. Once again, the main aesthetic advantage of the model is that it is based on standard translations into automata at the level of formulas, while the interpretation of proofs does no longer corresponds to inclusions of languages, but rather winning strategies in a simulation game. The proof of soundness of extraction is postponed to later chapters, so while this is not formally mentioned at that point, the guarded fixpoint construction over Mealy machines plays a crucial rule to interpret the cut rule of LSFOM. While the presentation of the models of SFOM and LSFOM as refinements of the usual automata-based interpretation of formulas is appealing and theoretically allow for automatic verification algorithm to be applied to those automatas to check, for instance, for the existence of simulations, it is also rather clear that the interpretation of proofs do *not* require to compute the automata interpretation of the involved formulas. In a sense, this hints at a crucial fact underlying the developments in latter chapters: the automata are not essential part of these models, the simulation and games are. Thus, the latter chapter are dedicated to giving categorical constructions allowing to recover equivalent models for FOM and LSFOM syntactically. The starting point is Chapter 5 which, after giving a few preliminaries on fibrations, recalls the Dialectica construction $\mathfrak{Dial}$ over them. The reason for this development is because the logical structure of $\mathfrak{Dial}$ and LSFOM share some striking similarities. Mentioned in passing is the $\mathfrak{Sum}$ construction, which generalizes the simple fibration, and essentially corresponds to building a syntactic model for SFOM when starting from the syntactical fibration for

[2]It is straightforward to check that the usual translation of formulas into infinite word automata can be carried out in the same way for FOM as for MSO(ω).

the classical theory FOM. Then, after introducing a convenient category for higher-order (and thus, not necessarily finite-state) causal functions $\mathbb{S}$, Chapter 6 gives the explicit construction of a category of simulation games, the zigzag games, and a construction $\mathfrak{Dial}^{\blacktriangleright}$ over fibrations over $\mathbb{S}$. Roughly speaking, $\mathfrak{Dial}^{\blacktriangleright}$ is a higher-order generalization of the model construction for LSFOM. Its formal relationship with $\mathfrak{Dial}$ is clarified and a similar characterization theorem is given. Finally Chapter 7 adapts this material to work with finite-state causal functions and exploits the characterization theorem of the previous chapter to give a reasonably nice complete axiomatization of the proof-relevant model of LSFOM.

Part II is less concerned with structural issues, but rather the foundational strength of MSO theories. Its main contribution lies in Chapter 9 where Büchi's decidability theorem for $\mathsf{MSO}(\omega)$, together with relevant theorems from the theory of infinite word automata, are analyzed from the point of view of Reverse mathematics. It turns out that over the weak base theory RCA_0, the decidability of $\mathsf{MSO}(\omega)$ (presented as a scheme for technical reasons), the existence of complement of Büchi automata, the additive Ramsey theorem over $\mathbb{N}$ and the scheme of Σ^0_2-induction are all equivalent. Furthermore, the Muller-Schupp algorithm determinizing Büchi automata into Rabin automata can be shown to be sound in Σ^0_2-induction. Some of those proofs, such as determinization from Σ^0_2-induction, are obtained by formalizing usual automata-theoretic proofs within second-order arithmetic, although sometimes the argument needs to be substantially changed to fit our weak theories. For instance, the additive Ramsey theorem can not be taken to be consequence of the general Ramsey theorem for pairs which is unprovable in Σ^0_2-IND, but requires a more refined argument based on basic Green theory here. The proofs that these theorems imply Σ^0_2-IND all employ a similar trick based around the idea that Σ^0_2-complete sets may be encoded in $\mathsf{MSO}(\omega)$. Chapter 10 contains preliminary steps towards a similar study for $\mathsf{MSO}(\mathbb{Q})$. It is centered around the idea that it makes for interesting intermediate case lying between $\mathsf{MSO}(\omega)$ and MSO over the infinite tree in terms of axiomatic strength. While we are nowhere close to having a crisp characterization of the strength of $\mathsf{MSO}(\mathbb{Q})$ as for $\mathsf{MSO}(\omega)$, we first establish that the additional additive Ramsey theorem over $\mathbb{Q}$ used in Shelah's proof of decidability is also equivalent to Σ^0_2-IND and is thus rather elementary with respect to the logical complexity of $\mathsf{MSO}(\mathbb{Q})$. Indeed, we then show that $\mathsf{MSO}(\mathbb{Q})$ can express Π^1_1-complete statements, which allow to derive Π^1_1-IND from decidability of $\mathsf{MSO}(\mathbb{Q})$ and Π^1_1-CA_0 from the soundness of the usual algotrithm deciding $\mathsf{MSO}(\mathbb{Q})$ over RCA_0.

All in all, while both parts of the thesis purports to study the constructivity of MSO, and more specifically, $\mathsf{MSO}(\omega)$, there is little overlap between the two. While this might serve as an illustration of the diverging interests of communities in foundational strength and those focussed on Curry-Howard correspondences and intuitionistic logics, one should keep in mind that those two aspects of logic still enjoy tight connexions that fall outside the scope of this thesis.

Further work

We collect below some ideas for further work. For Part I, we give several problems which arise as extension of the development above. For Part II, we focus on the open problems related to $\mathsf{MSO}(\mathbb{Q})$ on which we are still working on at the time of writing.

Part I

Axiomatization of FOM and its constructive counterparts FOM is a theory which is equivalent to $\mathsf{MSO}(\omega)$ from the point of view of expressivity in classical logic and that we found to be more pleasant from an aesthetic point of view when studying constructive aspects of the theory of infinite word automata for various reasons. Classically, because it is essentially the same as $\mathsf{MSO}(\omega)$, Siefkes' axiomatization can be seemlessly lifted to FOM.

However, the appeal of Siefkes' axiomatization of $\mathsf{MSO}(\omega)$ is also largely a matter of aesthetics that gets largely lost in translation: it is the restriction of the usual axiomatization of second-order Peano's arithmetic restricted to the language of $\mathsf{MSO}(\omega)$. When lifted to FOM, the induction and comprehension schemes get buried under cumbersome encodings for natural numbers, and an ad-hoc axiom gets added to relate the translation of $\mathsf{MSO}(\omega)$ formulas to the atomic equalities of FOM.

So a first informal question is the following:

Question. *Does there exist a natural axiomatization of* FOM *based on stream equations rather than encoding of the comprehension/induction axioms and natural numbers?*

It is unclear at the moment if such an axiomatization would be easy to find, but this might be an intersting first step towards finding more convincing axiomatizations of intuitionistic variants of FOM. Indeed, the axiomatizations of SFOM and LSFOM suffer from the same defect as they include negative/linear translation of those cumbersome axioms. This is to be constrasted with the cleaner situation in arithmetic, where, for instance, the axioms of Heyting arithmetic are aesthetically reasonable while still ensuring the soundness of the double-negation translation.

Axiomatization of equality in Mealy, $\mathbb{S}^{\mathrm{fin}}$ and its cartesian-closed extension We have provided a term syntax for finite-state causal functions and a complete axiomatization of its equational theory in Chapter 2. The fact that there exists a semi-recursive axiomatization is obvious, but once again, this particular axiomatization is rather pleasant because it fits neatly the syntactic constructs of the term language we provided. However, during the proof of completeness, multiple naturality conditions reminiscent of those required when defining trace operators in monoidal categories [33] must be proved. This leads to the following question:

Question. *Can the uniqueness axiom in the axiomatization of equalities between Mealy terms be replaced by naturality conditions while retaining completeness?*

If the answer is positive, this might possibly be straightforward to check by inspecting the proof of completeness.

While this axiomatization was not used further in the thesis, this paved the way to the crucial definition of the category $\mathbb{S}^{\mathrm{fin}}$ which serves as a stepping stone in defininingn $\mathsf{DZ}_{\mathrm{fin}}$. We did not attempt to give a complete axiomatization of equalities between terms forming the morphisms $\mathbb{S}^{\mathrm{fin}}$ along the same lines.

Question. *Is there a natural axiomatization of the equality between morphisms of* $\mathbb{S}^{\mathrm{fin}}$*?*

We presume that the answer is positive and rather obvious. The axiomatization itself probably mirrors the one given for Mealy, together with additional axioms pertaining to the pointwise arrow (namely, the counterpart of Lemma 6.1.8 together with some additional axioms arising from the isomorphism $(B^A)^\omega \cong A^\omega \multimap B^\omega$). Presumably, material from Section 7.1 could be leveraged to this end.

A more interesting question is to consider the analogous situation for a term language extending those coming from $\mathbb{S}^{\mathrm{fin}}$ to support general exponentials. This would roughly correspond to a fragment of the guarded λ-calculus where the most complex base type would essentially be streams.

Question. *Is there a recursively enumerable axiomatization (complete) of the term language of* $\mathbb{S}^{\mathrm{fin}}$ *augmented with* ev *and* Λ*?*

Note that this would be equivalent to the decidability of the equivalence of two terms, the set of pairs of unequal terms is recursively enumerable. The question makes sense for any reasonable inductively defined fragment of the topos of trees, so it might make sense to consider both restrictions and generalizations of $\mathbb{S}^{\mathrm{fin}}$ augmented with exponentials. In any case, let us notice that it does not take much to make the problem undecidable as it would be easy to simulate Minsky machines if we further assume that a morphism $3^\omega \to (2^\omega)^{2^\omega}$ simulating a counter is definable in addition to internal homsets and morphisms given by Mealy machines in our fragment of interest.

A complete extension of LSFOM with general exponentials As remarked when introducing LSFOM, while we have refrained from introducing general exponentials in the theory, it is entirely possible to do so while retaining a perfectly consistent theory that allows extraction. While Chapter 6 does so at the cost of introducing realizers which are not necessarily finite-state, it is also possible to adapt the construction of the general exponential found in [61] to our setting. Despite its structural defect, this latter construction ensures that this extension can be made without affecting the soundness theorem with respect to Church's synthesis and by keeping an automata-theoretic interpretation. In particular, it means that there is a decidable complete extension of LSFOM with full exponentials. Thus we may ask the following informal question:

Question. *Is there a natural extension of* LSFOM^+ *completely axiomatizing the model with full exponentials?*

At the time of writing, we have no idea if there is an elegant way to do so. A first idea towards attacking this problem would go as follows: first, note that parity uniform alternating automata $\mathcal{A} : A$ may be encoded as a formula $\varphi_{\mathcal{A}}(a, u, x)$ in a straightforward way, so that $\mathsf{LSFOM}^+ \vdash \mathcal{A} \multimap \exists x.\forall u.\varphi_{\mathcal{A}}(a, u, x)$. Then, one may try to check what basic axioms are required to show that, for instance, $\exists u'.\varphi_{!\mathcal{A}}(a, u', *) \vdash !\exists u.\forall x.\varphi_{\mathcal{A}}(a, u, x)$ in the extension. Having axioms strong enough to show this and the dual statement $?\exists u.\forall x.\varphi_{\mathcal{A}}(a, u, x) \vdash \forall x'.\varphi_{?\mathcal{A}}(a, *, x')$ would be sufficient.

Let us also note that having unrestricted exponential modalities allow for a straightforward translation of $\mathsf{MSO}(\omega)$ extended with game quantifiers in our logic.

Kleene realizability and continuous functions While we have studied extraction for synchronous functions here, nothing was said about the interpretation of the language of FOM[3] in general models for higher-order intuitionistic logic, such as the effective topos corresponding to Kleene realizability or the sheaf topos based on continuous maps considered in [47, VI.9]. There, the questions of axiomatizing and deciding the logics may be also be asked. These are much more challenging as, beyond the myriad of settings to consider, they seem to lead away from the usual basic automata-theoretic tools used to deal with $\mathsf{MSO}(\omega)$. Furthermore, as with the synchronous case, interpreting all the connectives of first-order logic in those interpretation seems to require a notion of higher-order realizers.

However, some modest goals in this direction may be within reach. A first step would be to clarify the situation for simple logics based on SFOM which only feature a limited number of connectives.

Question. *What are the consistent extensions of* SFOM *based on realizability?*

A first case do study would be the interepretation of SFOM formulas in Kleene's realizability. The situation looks quite simple because of the following fact: for any FOM formula if there exists any continuous $f : A^\omega \to B^\omega$ such that $\forall a^{A^\omega}.\varphi(a, f(a))$ holds classically, then there exists $k \in \mathbb{N}$ and a f.s. k-Lipschitz function $g : A^\omega \to B^\omega$ such that $\forall a^{A^\omega}.\varphi(a, f(a))$ holds classically. This can be seen as a consequence of [39] or proven directly by a pumping argument on the underlying automata. This essentially means that settings with continuous realizers coincide for SFOM formulas, and that we obtain a decidable model by a reduction to Büchi-Landweber. It would be interesting to seee if this result can be extended to cases where realizers f are Δ^0_1 and Δ^0_2 functionals; if so, it might mean that there is a formal way of saying that there are essentially three "interesting" proper extensions of SFOM[4].

The other natural extension of the case of continuous functions would be to see what happens with higher-order continuous realizers and the interpretation of all connectives of first-order logic that require them (namely, $\Rightarrow$ and $\forall$). While it is rather clear how to systematically build models as soon as we are given a cartesian closed category in which Mealy admits a (finite-limit preserving) embedding by using $\mathfrak{Sum}$ and change of base, it is unclear if it can be shown that they are all equivalent for FOM formulas or not.

Part II : the proof-theoretic strength of $\mathsf{MSO}(\mathbb{Q})$?

It is likely that one would be able to prove decidability of $\mathsf{MSO}(\mathbb{Q})$ in Π^1_2-comprehension[5] by simply adapting the proof of decidability found in [14]. The crucial property that seems to require a strong comprehension axiom there is Proposition 1, which is proven using Zorn's lemma. This proposition is provable in Π^1_2-CA_0, and it might even be the case that a mild modification makes the proof go through in Δ^1_2-CA_0. One should note that this axiom is strictly less powerful than *Rabin's theorem* in terms of axiomatic strength as [41] establishes that Rabin's theorem is not provable in Δ^1_3 comprehension. However, our investigations thus far hint at the existence of a tighter upper bound. Note for instance that while we are able to derive Π^1_1 induction from the decidability of $\mathsf{MSO}(\mathbb{Q})$ (and that $\mathsf{MSO}(\mathbb{Q})$ is able to express theorems equivalent to Π^1_1-CA_0), it does not seem possible to extend this result to the class of Δ^1_2 formulas. It is more likely that the true theory of $\mathsf{MSO}(\mathbb{Q})$ may be shown to be decidable by a strenghthening of Π^1_1-CA_0 that could be dubbed finite Π^1_1-recursion.

[3] We refrain from speaking about $\mathsf{MSO}(\omega)$, specifically because the absence or presence of primitive integers start being quite significant. For instance, having a bijection between those streams $x \in 2^\omega$ such that $\mathbb{N}_\infty(x) = 0^\omega \wedge x \neq 0^\omega$ (as per Figure 2.4) and the set of natural numbers implicitly relies on Markov's principle!

[4] The "interesting" would cover technical restrictions, such as e.g. requiring that the theories of interest be invariant under relativization over infinite domains...

[5] With the same caveat as in Theorem 9.3.1: Π^1_2-CA_0 would only prove decidability of the depth-n fragment of $\mathsf{MSO}(\mathbb{Q})$ for every fixed external $n \in \omega$.

Definition 10.2.10. *Let* Γ *be a class of formulas. Call the following axiom scheme, where* $\varphi(X, Y) \in \Gamma$ *(possibly with other parameters),* finite Γ-recursion*:*

$$\forall n \in \mathbb{N}\ \exists X\ \big((\forall k < n\ \varphi(X_k, X_{k+1})) \wedge \varphi(\emptyset, X_0)$$

Note that for every standard $n \in \omega$, Γ-recursion up to n can be done using n times Γ-comprehension. In particular, it means that for every model of L_2 with a standard first-order part, finite Γ-recursion holds if and only if Γ-comprehension does. Our current conjecture regarding the decidability of $\mathsf{MSO}(\mathbb{Q})$ is thus the following.

Conjecture 10.2.11. *For every external* $n \in \omega$, Π^1_1*-finite recursion proves that the standard algorithm deciding* $\mathsf{MSO}(\mathbb{Q})$ *is sound for the depth-*n *fragment.*

Proving Conjecture 10.2.11 is more challenging than merely adapting [14], as the impredicative proof does not readily go through. At the time of writing, it is still unclear whether Conjecture 10.2.11 may be solved positively, although we believe that an analogue of Proposition 1 from [14] may be proven in finite Π^1_1-recursion, based however on a more general notion of *evaluation tree*. However, it is much less clear whether the soundness of the projection operation on the underlying algebras is still provable in finite Π^1_1-recursion (Lemma 3 in [14]).

Nevertheless, the mere definability of the (standard) truth value of formulas of $\mathsf{MSO}(\mathbb{Q})$ within finite Π^1_1-recursion would still be interesting in its own right. In particular, finite Π^1_1-recursion seems to be equivalent, over RCA_0, to the determinacy of weak parity games (over infinite arena) of finite index (or equivalently, finite boolean combination of Π^0_2 by adapting [70] which proves (lightface) Δ^0_2 determinacy using transfinite Π^1_1-recursion. Making this connexion would suggest that there might be a reasonable notion of alternating automata for countable words corresponding to $\mathsf{MSO}(\mathbb{Q})$ with a weak parity acceptance condition, although one should remain cautious; to our knowledge, only reasonable automata models for MSO over countable scattered linear orders have appeared in the literature so far [11].

Bibliography

[1] S. Abramsky, P. Malacaria, and R. Jagadeesan. Full abstraction for PCF. In *Theoretical Aspects of Computer Software, International Conference TACS '94, Sendai, Japan, April 19-22, 1994, Proceedings*, pages 1–15, 1994.

[2] C. S. Althoff, W. Thomas, and N. Wallmeier. Observations on determinization of Büchi automata. *Theor. Comput. Sci.*, 363(2):224–233, 2006.

[3] R. M. Amadio and P. Curien. *Domains and lambda-calculi*, volume 46 of *Cambridge tracts in theoretical computer science*. Cambridge University Press, 1998.

[4] J. Avigad and S. Feferman. Gödel's functional ("dialectica") interpretation. *Handbook of proof theory*, 137:337–405, 1998.

[5] P. N. Benton. A mixed linear and non-linear logic: Proofs, terms and models (extended abstract). In *Computer Science Logic, 8th International Workshop, CSL '94, Kazimierz, Poland, September 25-30, 1994, Selected Papers*, pages 121–135, 1994.

[6] B. Biering. Cartesian closed dialectica categories. *Ann. Pure Appl. Logic*, 156(2-3):290–307, 2008.

[7] L. Birkedal, R. E. Møgelberg, J. Schwinghammer, and K. Støvring. First steps in synthetic guarded domain theory: step-indexing in the topos of trees. *Logical Methods in Computer Science*, 8(4), 2012.

[8] M. Bojańczyk. Polyregular functions. 2018.

[9] M. Bojańczyk. Lecture notes on languages, automata and computations, University of Warsaw, `http://www.mimuw.edu.pl/~bojan/20152016-2/jezyki-automaty-i-obliczenia-2/mcnaughtons-theorem`. 2015.

[10] F. Borceux and D. Dejean. Cauchy completion in category theory. *Cahiers de Topologie et Géométrie Différentielle Catégoriques*, 27(2):133–146, 1986.

[11] V. Bruyère and O. Carton. Automata on linear orderings. In *Developments in Language Theory, 6th International Conference, DLT 2002, Kyoto, Japan, September 18-21, 2002, Revised Papers*, pages 103–115, 2002.

[12] J. R. Büchi. On a decision method in restricted second order arithmetic. In *Logic, Methodology and Philosophy of Science. Proceeding of the 1960 International Congress*, pages 1 – 11. 1962.

[13] J. R. Büchi and L. H. Landweber. Solving Sequential Conditions by Finite-State Strategies. *Transation of the American Mathematical Society*, 138:367–378, 1969.

[14] O. Carton, T. Colcombet, and G. Puppis. Regular languages of words over countable linear orderings. In *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part II*, pages 125–136, 2011.

[15] C. Choffrut and S. Grigorieff. Uniformization of rational relations. In *Jewels are Forever, Contributions on Theoretical Computer Science in Honor of Arto Salomaa*, pages 59–71, 1999.

[16] A. Church. Applications of recursive arithmetic to the problem of circuit synthesis. In *Summaries of the SISL*, volume 1, pages 3–50. Cornell Univ., 1957.

[17] P. Clote. The metamathematics of scattered linear orderings. *Arch. Math. Log.*, 29(1):9–20, 1989.

[18] J. R. B. Cockett and R. A. G. Seely. Weakly distributive categories. *Journal of Pure and Applied Algebra*, 114(2):133–173, 1997.

[19] T. Colcombet and K. Zdanowski. A tight lower bound for determinization of transition labeled Büchi automata. In *ICALP (2)*, pages 151–162, 2009.

[20] A. Das. On the logical complexity of cyclic arithmetic. *CoRR*, abs/1807.10248, 2018.

[21] V. de Paiva. The Dialectica categories. Technical Report 213, University of Cambridge Computer Laboratory, January 1991.

[22] E. A. Emerson and C. S. Jutla. Tree Automata, Mu-Calculus and Determinacy (Extended Abstract). In *FOCS*, pages 368–377. IEEE Computer Society, 1991.

[23] E. Frittaion. Reverse mathematics and partial orders, 2014.

[24] E. Frittaion and L. Patey. Coloring the rationals in reverse mathematics. *Computability*, 6(4):319–331, 2017.

[25] K. Gödel. Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. *Dialectica*, 12(3-4):280–287, 1958.

[26] P. Hájek and P. Pudlák. *Metamathematics of first-order arithmetic*. Perspectives in Mathematical Logic. 1993.

[27] F. Hausdorff. Grundzüge einer Theorie der geordneten Mengen. *Math. Ann.*, 65(4), 1908.

[28] T. A. Henzinger and N. Piterman. Solving games without determinization. In *CSL 2006, 15th Annual Conference of the EACSL, Szeged, Hungary, September 25-29, 2006, Proceedings*, pages 395–410, 2006.

[29] D. R. Hirschfeldt. *Slicing the truth*, volume 28 of *Lecture Notes Series. Institute for Mathematical Sciences. National University of Singapore*. World Scientific, 2015.

[30] J. L. Hirst. *Combinatorics in Subsystems of Second Order Arithmetic*. PhD thesis, Pennsylvania State University, 1987.

[31] P. J. W. Hofstra. The dialectica monad and its cousins. In M. Makkai and B. Hart, editors, *Models, Logics, and Higher-dimensional Categories: A Tribute to the Work of Mihály Makkai*, CRM proceedings & lecture notes. American Mathematical Society, 2011.

[32] J. M. E. Hyland and C. L. Ong. On full abstraction for PCF: i, ii, and III. *Inf. Comput.*, 163(2):285–408, 2000.

[33] M. Hyland. Abstract and concrete models for recursion. *NATO security through science series D - information and communication security*, 14:175, 2008.

[34] M. Hyland and V. de Paiva. Full Intuitionistic Linear Logic (Extended Abstract). *Annals of Pure and Applied Logic*, 64(3), 1993.

[35] M. Hyland and A. Schalk. Abstract games for linear logic. *Electr. Notes Theor. Comput. Sci.*, 29:127–150, 1999.

[36] B. Jacobs. *Categorical Logic and Type Theory*. Studies in logic and the foundations of mathematics. Elsevier, 2001.

[37] C. G. Jockusch, Jr. Ramsey's theorem and recursion theory. *J. Symbolic Logic*, 37:268–280, 1972.

[38] D. Kähler and T. Wilke. Complementation, disambiguation, and determinization of Büchi automata unified. In *ICALP*, pages 724–735, 2008.

[39] F. Klein and M. Zimmermann. What are strategies in delay games? borel determinacy for games with lookahead. In *24th EACSL Annual Conference on Computer Science Logic, CSL 2015, September 7-10, 2015, Berlin, Germany*, pages 519–533, 2015.

[40] U. Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer Monographs in Mathematics. Springer, 2008.

[41] L. A. Kołodziejczyk and H. Michalewski. How unprovable is Rabin's decidability theorem? (accepted@LICS 2016). *CoRR*, abs/1508.06780, 2015.

[42] L. A. Kolodziejczyk, H. Michalewski, P. Pradic, and Michał Skrzypczak. The logical strength of Büchi's decidability theorem. In *Proceeding CSL'16*, pages 36:1–36:16, 2016.

[43] G. Kreisel. A variant to Hilbert's theory of the foundations of arithmetic. *British J. Philos. Sci.*, 4:107–129, 1953.

[44] O. Laurent. Classical isomorphisms of types. *Mathematical Structures in Computer Science*, 15(5):969–1004, 2005.

[45] M. Lichter and G. Smolka. Constructive analysis of S1S and Büchi automata. *CoRR*, abs/1804.04967, 2018.

[46] J. Liu. RT^2_2 does not imply WKL_0. *J. Symbolic Logic*, 77(2):609–620, 2012.

[47] S. Mac Lane and I. Moerdijk. *Sheaves in Geometry and Logic*. 1992.

[48] R. McNaughton. Testing and generating infinite sequences by a finite automaton. *Information and Control*, 9(5):521 – 530, 1966.

[49] P.-A. Melliès. Categorical semantics of linear logic. In *Interactive models of computation and program behaviour*, volume 27 of *Panoramas et Synthèses*. SMF, 2009.

[50] J. Moeller and C. Vasilakopoulou. Monoidal grothendieck construction, 2018.

[51] S. K. Moss and T. von Glehn. Dialectica models of type theory. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 739–748, 2018.

[52] D. E. Muller and P. E. Schupp. Simulating alternating tree automata by nondeterministic automata: New results and new proofs of the theorems of rabin, mcnaughton and safra. *Theoretical Computer Science*, 141(1–2):69 – 107, 1995.

[53] H. Nakano. A modality for recursion. In *15th Annual IEEE Symposium on Logic in Computer Science, Santa Barbara, California, USA, June 26-29, 2000*, pages 255–266, 2000.

[54] D. Perrin and J.-E. Pin. *Infinite words : automata, semigroups, logic and games*. Pure and applied mathematics. London, San Diego (Calif.), 2004.

[55] P. Pradic. *A sound and complete axiomatization of the equational theory of Mealy machines*, 2019. `https://hal.archives-ouvertes.fr/hal-02155786`.

[56] P. Pradic and C. Riba. A Curry-Howard Approach to Church's Synthesis. In *Proceedings of FSCD17*.

[57] P. Pradic and C. Riba. A Dialectica-Like Interpretation of a Linear MSO on Infinite Words. In *Proceedings of FOSSACS19*.

[58] P. Pradic and C. Riba. LMSO: A Curry-Howard Approach to Church's Synthesis via Linear Logic. In *Proceedings of LICS18*.

[59] M. O. Rabin. Decidability of second-order theories and automata on infinite trees. *Transactions of American Mathematical Society*, 141:1–35, 1969.

[60] C. Riba. A model theoretic proof of completeness of an axiomatization of monadic second-order logic on infinite words. In *Proceedings of IFIP-TCS'12*, 2012.

[61] C. Riba. Monoidal-Closed Categories of Tree Automata. Submitted. Available on HAL (hal-01261183), `https://hal.archives-ouvertes.fr/hal-01261183`, 2017.

[62] S. Safra. On the complexity of omega-automata. In *FOCS*, pages 319–327, 1988.

[63] S. Shelah. The monadic theory of order. *Ann. of Math. (2)*, 102(3):379–419, 1975.

[64] M. Shulman. Enriched indexed categories. *Theory and Applications of Categories*, 28(21):616–695, 2013.

[65] D. Siefkes. *Decidable Theories I : Büchi's Monadic Second Order Successor Arithmetic*, volume 120 of *LNM*. Springer, 1970.

[66] D. Siefkes. The recursive sets in certain monadic second order fragments of arithmetic. *Arch. Math. Log.*, 17(1-2):71–80, 1975.

[67] A. Simpson. Cyclic arithmetic is equivalent to Peano arithmetic. In *Foundations of Software Science and Computation Structures - 20th International Conference, FOSSACS 2017*, pages 283–300, 2017.

[68] S. G. Simpson. *Subsystems of second order arithmetic*. Perspectives in Mathematical Logic. 1999.

[69] S. G. Simpson and K. Yokoyama. Very weak fragments of weak König's Lemma, 2016. In preparation.

[70] K. Tanaka. Weak axioms of determinacy and subsystems of analysis I: Δ^0_2 games. *Mathematical Logic Quarterly*, 36(6):481–491, 1990.

[71] W. Thomas. Automata on Infinite Objects. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B: Formal Models and Semantics, pages 133–192. Elsevier Science Publishers, 1990.

[72] W. Thomas. Solution of Church's Problem: A tutorial. *New Perspectives on Games and Interaction*, 5:23, 2008.

[73] A. Troelstra. History of constructivism in the 20th century. *Set Theory, Arithmetic, and Foundations of Mathematics*, 1991.