LMSO: A Curry-Howard Approach to Church’s Synthesis via Linear Logic
Cécilia Pradic, Colin Riba

To cite this version:
Cécilia Pradic, Colin Riba. LMSO: A Curry-Howard Approach to Church’s Synthesis via Linear Logic. LICS’18, Jul 2018, Oxford, United Kingdom. hal-01698648v2

HAL Id: hal-01698648
https://hal.science/hal-01698648v2
Submitted on 27 Apr 2018

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

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
LMSO: A Curry-Howard Approach to Church’s Synthesis via Linear Logic

Pierre Pradic  
ENS de Lyon, Université de Lyon, LIP  
Lyon, France  
pierre.pradic@ens-lyon.fr  
University of Warsaw, Faculty of Mathematics, Informatics and Mechanics  
Warsaw, Poland

Colin Riba  
ENS de Lyon, Université de Lyon, LIP  
Lyon, France  
colin.riba@ens-lyon.fr

Abstract

We propose LMSO, a proof system inspired from Linear Logic, as a proof-theoretical framework to extract finite-state stream transducers from linear-constructive proofs of omega-regular specifications. We advocate LMSO as a stepping stone toward semi-automatic approaches to Church’s synthesis combining computer assisted proofs with automatic decisions procedures. LMSO is correct in the sense that it comes with an automata-based realizability model in which proofs are interpreted as finite-state stream transducers. It is moreover complete, in the sense that every solvable instance of Church’s synthesis problem leads to a linear-constructive proof of the formula specifying the synthesis problem.

Keywords  Categorical Logic, Game Semantics, Realizability, Linear Logic, MSO on Infinite Words

1 Introduction

Church’s synthesis [5] consists in the automatic extraction of stream transducers (or Mealy machines) from input-output specifications. Ideally, these specifications would be written in Monadic Second-Order Logic (MSO) on ω-words [29, 30]. MSO on ω-words is a decidable logic thanks to Büchi’s Theorem [3], whose proof is originally based on an effective translation of MSO formulae to non-deterministic Büchi automata (NBA’s). It subsumes non-trivial logics used in verification such as LTL (see e.g. [1, 28]). Church’s synthesis for (subsystems of) LTL has also been substantially studied (see e.g. [2, 7, 16]).

Traditional theoretical solutions to Church’s synthesis start from an ω-word automaton recognizing the specification (typically an NBA), and apply McNaughton’s Theorem [18] to obtain an equivalent deterministic (say parity) automaton on ω-words. There are then essentially two methods (see e.g. [29, 30]). The first one turns the deterministic automaton into a game graph, in which the Opponent O (Védelard) plays input characters to which the Proponent P (Eloïse) replies with output characters. Solutions to Church’s synthesis are then given by the Büchi-Landweber Theorem [4], which says that in such games, either P or O has finite-state winning strategy. The second one goes via infinite trees [23], noting that a causal function (say) from Σ to Γ can be represented by an infinite Γ-labeled Σ-ary tree.

However, the translation of MSO-formulae to NBA’s is non-elementary [10], ruling out any tractable implementation. Moreover, even when restricting to LTL (which has an exponential translation to NBA’s, see e.g. [1]), the use of McNaughton’s Theorem has long been a major obstacle to Church’s synthesis.1

In this paper, extending [22], we advocate an approach to Church’s synthesis in the framework of program extraction from proofs (in the sense of e.g. [27]). We propose a constructive deduction system for (an expressively equivalent variant of) MSO, based on a complete axiomatization of MSO on ω-words as a subsystem of second-order Peano arithmetic [26] (see also [24]). The formal proofs in this deduction system are interpreted in an automata-based realizability semantics, along the lines of the Curry-Howard proofs-as-programs correspondence. Our system is correct, in the sense that from a proof of a ∀∃-specification one can extract a Mealy machine implementing the specification. It is moreover complete, in the sense that it proves all ∀∃-specifications which are realizable by Mealy machines.

The crux of our approach is that on the one hand the correctness proof of our realizability interpretation relies on McNaughton’s Theorem, while on the other hand the extraction of realizers from formal proofs does not invoke it.

In the context of MSO, using a deduction system may avoid the systematic translation of formulae to automata, and may allow for human intervention and compositional reasoning. In a typical usage scenario, the user interactively performs some proofs steps and delegate the generated subgoals to automatized synthesis procedures. The partial proof tree built by the user is then translated to a combinator able to compose the transducers synthesized by the algorithms.

The deduction system LMSO proposed in [22] was based on intuitionistic logic. While SMSO is correct and complete for Church’s synthesis, it suffers from a very limited set of primitive connectives (∧, ¬, ∃) so that formal proofs may be cumbersome without resorting to a negative translation from the complete axiomatization of MSO in classical logic. In this paper, we propose a deduction system LMSO inspired from (intuitionistic) Linear Logic [9] (see also [19]). LMSO has a rich set of connectives (with primitive ⊕, ⊗, →, ?!, ?, ℓ, ∃, ∀), with a straightforward interpretation as usual automata constructions.2 The system LMSO is moreover based on an extension

1Interesting workarounds are the Safraless approaches of [7, 16].
2The usual additive connectives ⊕, ⊗ of Linear Logic have also natural interpretations in automata.
MSO+ of MSO with primitive function symbols for Mealy machines, allowing for a much more efficient extraction of realizers from proofs.

Organization of the paper. We begin in §2 by presenting Church’s synthesis problem and our extension MSO+ of MSO. We also briefly discuss there the intuitionistic system SµSO. We then present §3 our linear system LMSO, and show its completeness w.r.t. MSO+ and Church’s synthesis. The realizability interpretation is then split into two parts: §4 recapitulates known material on games and automata from [25], and §5 presents the realizability interpretation of LMSO and states its correctness.

2 Church's Synthesis and MSO+

Notations. Alphabets (denoted Σ, Γ, etc) are sets of the form 2^p for some p ∈ N. We see alphabets as being built by following grammar:

Σ, Γ ::= 1 | 2 | Σ × Γ | Σ → Γ

Concatenation of words u, v is denoted either u.v or u · v, and ε is the empty word. We use the vectorial notation both for words and finite sequences, so that e.g. B denotes a finite sequence B_1, ..., B_n and π denotes a word a_1, ..., a_n ∈ Σ^*. Given an ω-word (or stream) B ∈ Σ^ω and n ∈ N we write B[n] for the finite word B(0), ..., B(n − 1) ∈ Σ^∗.

Specifications. Specifications for stream functions Σ^ω → Γ^ω will be given by formulae ψ(Υ, Z) where, assuming Σ = 2^p and Γ = 2^q, Υ = Y_1, ..., Y_p and Z = Z_1, ..., Z_q are tuples of (monadic) set variables. For instance, the formula

(∃k k(Y(k)) ≡ (∃k k(Z(k)))

specifies functions f : 2^ω → 2^ω such that f(B) ∈ 2^ω ∼ P(N) is infinite whenever B ∈ 2^ω is infinite.

Causal Functions and Mealy Machines. We shall actually require our specifications to be realized by stream functions implementable by finite state stream transducers, a.k.a. Mealy machines.

Definition 2.1. A Mealy machine M with input alphabet Σ and output alphabet Γ (notation M : Σ → Γ) is given by an alphabet of states Q with a distinguished initial state q^0 ∈ Q, and a transition function δ : Q × Σ → Q × Γ.

We write δ^i for π_2 ◦ δ^i : Q × Σ → Γ and δ^ω for the map Σ^ω → Q obtained by iterating δ from the initial state: δ^ω(ε) := q^0 and δ^ω(π(a)) := π_i(δ(δ^ω(π(a)), a)).

A Mealy machine M : Σ → Γ induces a function F_M : Σ^ω → Γ^ω defined as F_M(B)(n) = δ^ω(δ^ω(B)(n), B(n)). Hence F_M can produce a length-n prefix of its output from a length-n prefix of its input. These functions are called causal.

Definition 2.2. A function F : Σ^ω → Γ^ω is causal if for all n ∈ N and all B, C ∈ Σ^ω we have F(B)[n] = F(C)[n] whenever B[n] = C[n]. We say that a causal function F is finite-state (f.s.) if it is induced by a Mealy machine.

Example 2.3. (a) The identity function Σ^ω → Σ^ω is induced by the Mealy machine with state set 1 = {●} and identity transition function δ : {●} → {●}.

(b) Causal functions are obviously continuous (taking the product topology on Σ^ω and Γ^ω, with Σ, Γ discrete), but there are continuous functions which are not causal, e.g. F : 2^ω → 2^ω such that F(A)(n) = 1 if A(n + 1) = 1.

In the context of this paper, it is useful to note that finite-state causal functions form a category with finite products.

Definition 2.4. Let S be the category whose objects are alphabets and whose maps from Σ to Γ are causal functions F : Σ^ω → Γ^ω. Let M be the wide subcategory of S whose maps are finite-state causal functions.

Note that ω-words B ∈ Σ^ω correspond exactly to causal functions from {●}^ω to Σ^ω. We thus identify Σ^ω and S[{●}, Σ]. Also, functions f : Σ → Γ induce M-maps [f] : Σ →_M Γ.

Proposition 2.5. The categories S, M have finite products. The product of Σ_1, ..., Σ_n (for n ≥ 0) is given by the product of sets Σ_1 × · · · × Σ_n (so that {●} is terminal).

The Logic MSO+. We now introduce our specification language, the logic MSO+. It is an extension of (the one-sorted version of) MSO with one function symbol F_M of arity p for each Mealy machine M : 2^ω → 2^ω. The terms of MSO+, ranged over by t, u, etc, are built with these function symbols from (monadic) predicate variables X, Y, Z, etc of arity 0. The formulae of MSO+ are given in Fig. 1.

MSO+-formulae are interpreted in the standard model M of ω-words. Variables range over sets of natural numbers B, C, ... ∈ P(N) ∼ 2^ω. A term t together with a valuation X_i := B_i of its variables X_1, ..., X_n is interpreted as F(B_1, ..., B_n) where F : 2^ω → 2 is the f.s. causal function induced by t. The atomic predicates are interpreted as follows: ⊨ is equality, ⊨≤ is set inclusion, E holds on B iff B is empty, N (resp. 0) holds on B iff B is a singleton {n} (resp. the singleton {0}), and S(B, C) (resp. B ≤ C) holds iff B = {n} and C = {n + 1} for some n ∈ N (resp. B = {n}) and C = {m} for some n ≤ m.

We use the following notational conventions. Lowercase roman letters x, y, z, etc denote variables relativized to N. In particular, ∃x.ϕ and ∀x.ϕ stand respectively for

∃x(N(x) ∧ ϕ) and ∀x(N(x) → ϕ)

Moreover x ∈ t stands for x ⊑ t, so that

M |= X ⊑ Y ↔ ∀x(x ∈ X → x ∈ Y)

We often write X(x) for x ∈ X. Finally ∃ω.n.ϕ stands for ∀m.∃n ≥ m.ϕ and ∀ω.n.ϕ for ∀m.∀n ≥ m.ϕ.

The logic MSO is MSO+ with terms restricted to monadic variables X, Y, Z, etc. MSO+ is an extension by definition of MSO (and thus conservative over MSO) thanks to the following well-known fact:

Proposition 2.6. For each Mealy machine M : 2^ω → 2^ω, one can build an MSO-formula δ_M(X, x) such that for all n ∈ N and all ω ∈ (2^ω)^ω, we have F_M(ω)(n) = 1 iff M |= δ_M({n}, ω).
Example 2.7. MSO directly expresses the specification (1), as well as other typical properties used in software verification, such as the following safety and liveness properties:

\[ \forall x \left( A[Y(x)] \rightarrow G[Z(x)] \right) \] (safety)

\[ \forall x \left( A[Y(x)] \rightarrow \exists y > x. G[Z(y)] \right) \] (liveness)

Here, A (resp. G) is a propositional formula with say \( p \) (resp. \( q \)) variables, representing a subset of \( 2^p \) (resp. \( 2^q \)).

**B"uchi Automata.** The logic MSO (and thus MSO\(^+\)) over \( \forall t \) is decidable thanks to B"uchi's Theorem [3].

**Theorem 2.8 (B"uchi [3]).** MSO over \( \forall t \) is decidable.

In our context, it is pertinent to look at Thm. 2.8 through its original proof method, which consists in translating formulæ to B"uchi automata. A non-deterministic B"uchi automaton (NBA) is an NFA, but which accepts an \( \omega \)-word if there exists an infinite run with infinitely many finite states. It is known that deterministic B"uchi automata are strictly less expressive than NBA's.

The crux of B"uchi's Theorem 2.8 is the effective closure of B"uchi automata under complement. Let us recall a few known algorithmic facts (see e.g. [10, 28]). First, the translation of MSO-formulæ to automata is non-elementary. Second, it is known that complementation of NBA's is algorithmically hard: there is a family of languages \( (L_n)_{n \geq 0} \) such that each \( L_n \) can be recognized by an NBA with \( O(n) \) states, but such that the complement of \( L_n \) can not be recognized by an NBA with less than \( n! \) states. Known constructions for complementation produce NBA's with \( O(2^{\omega \log(n)}) \) states from NBA's with \( n \) states.

**Church's Synthesis.** Church's synthesis problem for MSO\(^+\) is the following. Given as input an MSO\(^+\) formula \( \varphi(Y; Z) \) (where \( Y = Y_1, \ldots, Y_p \) and \( Z = Z_1, \ldots, Z_q \)), (1) decide whether there exist f.s. causal \( \overline{F} = F_1, \ldots, F_p : 2^p \rightarrow \mathbb{M} 2 \) such that \( \exists t \models \varphi(\overline{F}; \overline{F}(\overline{T})) \) for all \( \overline{T} \in (2^x)^p \), and (2), construct \( \overline{F} \) whenever they exist.

**Example 2.9.** The following specification \( \varphi(Y; Z) \) from [29]

\[ \forall n (\neg Y \rightarrow \neg Z_n) \land \forall n, m (S(n, m) \rightarrow Z_n \rightarrow \neg Z_m) \land (\exists \omega n. Y_n \rightarrow \exists \omega n. Z_n) \]

asks \( n \in Z \) whenever \( n \in Y \). \( Z \) not to contain two consecutive positions, and \( Z \) to be infinite whenever \( Y \) is infinite. It is realized by the following Mealy machine, where a transition \( a/b \) outputs \( b \) from input \( a \):

![Diagram](image_url)

We now briefly sketch general solutions to Church’s synthesis. To this end, it is convenient to start from B"uchi automata rather than MSO\(^+\) formulæ. Given an automaton \( A : \Sigma \times \Gamma \) we say that a Mealy machine \( M : \Sigma \rightarrow \Gamma \) realizes \( A \) if \( A \) accepts \((B, F_M(B)) \) for every \( B \in \Sigma^\omega \).

Starting from a B"uchi automaton \( B : \Sigma \times \Gamma \), traditional solutions to Church’s synthesis (see e.g. [29, 30]) begin by translating \( B \) to an equivalent deterministic automaton \( D \) (say equipped with a parity condition\(^6\)). Determinization of automata on \( \omega \)-words is originally due to McNaughton [18].

**Theorem 2.10 (McNaughton [18]).** Each NBA is equivalent to a deterministic parity automaton.

There are two historical solutions to Church’s synthesis. The first one, due to B"uchi & Landweber [4], is to turn the automaton \( D : \Sigma \times \Gamma \) into a two-player sequential game, in which the **Opponent** \( O \) plays inputs characters in \( \Sigma \) while the **Proponent** \( P \) replies with outputs characters in \( \Gamma \). The game is equipped with the parity condition of \( D \). The solution is then provided by B"uchi-Landweber’s Theorem [4], which states that \( \omega \)-regular games on finite graphs are effectively determined, and that the winner has a f.s. winning strategy\(^6\).

A second possibility, due to Rabin [23] (see also [16]), uses tree automata. The idea is that causal functions \( \Sigma^\omega \rightarrow \Gamma^\omega \) can be represented as \( \Gamma \)-labeled \( \Sigma \)-ary trees. The solution is then to build from \( D \) a tree automaton accepting exactly the \( \Gamma \)-labeled \( \Sigma \)-ary trees which represent realizers of \( D : \Sigma \times \Gamma \).

However, neither of these solutions directly lead to applicable algorithms. The best known (and possible) constructions for McNaughton’s Theorem (such as Safra’s trees, see e.g. [10]) give deterministic Muller automata with \( 2^{O(n \log(n))} \) states from NBA’s with \( n \) states. This may seem no worse than NBA’s complementation, but while the latter is amenable to tractable implementations (see e.g. [8]), this is not the case for McNaughton’s Theorem (see e.g. [2, 7, 16]). Also, the states of automata obtained from Thm. 2.10 have a complex structure, making difficult implementations of subsequent algorithms (e.g. game solving).

**Curry-Howard Approaches.** In this paper, extending [22], we advocate semi-automatic approaches in the framework of program extraction from proofs (in the sense of e.g. [27]).

We start with a complete axiomatization of MSO\(^+\), based on a known axiomatization of MSO on infinite words [26] (see also [24]). The theory of MSO\(^+\) is given by deduction for first-order classical logic (with the terms of MSO\(^+\) as

---

\[ ^6 \] There are different expressively equivalent conditions for deterministic automata (parity, Muller, Rabin, Streett, see e.g. [10, 28]). All can specify which states an infinite run must not see infinitely often.

\[ ^6 \] This implies that in the setting of this paper, causal realizers can always be assumed to be finite-state.

\[ ^7 \] Actually, emptiness of tree automata is reduced to solving parity games on finite graphs, so this solution also goes via [4].
The rules of Fig. 2 are given in a two-sided sequent calculus format (see e.g. [27]) in order to ease the later presentation of Theorem 2.12.

One feature of SMSO is that extraction of realizers from formal proofs does not involve McNaughton’s Theorem (nor complementation of NBA’s) even if the correctness proof of the realizability model does invoke it.

The system SMSO has however some limitations. First of all, its set of connectives is very limited, so that proofs in the system SMSO itself may be cumbersome without appealing to a negative translation from the complete axiomatization of MSO in classical logic. Second, the extraction process can itself be quite costly: Mealy machines were represented as usual MSO-formulae (according to Prop. 2.6) so that witness extraction from proofs must pay the price of the translation of these formulae back to automata.

Linear Variants of SMSO. In this paper, we introduce LMSO of SMSO, inspired from Intuitionistic Linear Logic [9] (see also [19]). First, linearity allows to have more primitive connectives: implications and disjunction in addition to conjunction, and primitive universal quantifications in addition to existentials.

The logical system LMSO is built on the model of [25], which relies on a variant of alternating automata [20, 21] called uniform automata (UA’s). UA’s are equipped with a monoidal closed structure and with primitive existential and universal quantifications in the categorical sense [25]. Alternating automata allows in some cases better translations of formulae since they are easier to complement. However, it is well-known that existential (resp. universal) quantifications are only correct on non-det. (resp. universal) automata, so that the full translation of MSO to alternating automata involves the simulation of alternating automata by non-det. ones. This operation, known as the Simulation Theorem [21] in the case of infinite trees, actually amounts on ω-words to McNaughton’s Theorem (see e.g. [21]).

Similarly as with SMSO, we devise for LMSO a realizability model which involves McNaughton’s Theorem in its correctness proof; but not for the extraction of realizers from formal proofs. Theorem 2.12 extends to LMSO (for a suitable translation (−)k), so that if ϕ(Y; Z) is realized by M, then LMSO ⊢ ∀Y.ϕk(Y; tM(Y))

The rules of Fig. 2 are given in a two-sided sequent calculus format (see e.g. [27]) in order to ease the later presentation of LMSO.
Moreover, the system LMSO is equipped with polarities thanks to which the exponential connectives of Linear Logic exactly indicate the applications McNaughton’s Thm. in translations to UA’s. This reflects the fact that the following positive (noted $\varphi^+$) and negative (noted $\varphi^-$) fragments of MSO\(^+\) have exponential translations to automata:\(^9\) $\varphi^+, \psi^+ ::= T \mid \bot \mid \alpha \mid \exists X.\varphi^+ \mid \varphi^- \rightarrow \varphi^+$ $\varphi^-, \psi^- ::= T \mid \bot \mid \alpha \mid \forall X.\varphi^- \mid \varphi^- \rightarrow \varphi^-$

3 LMSO: A Linear Variant of MSO

We introduce here the formal system LMSO, inspired from the multiplicative-exponential fragment of Linear Logic [9]. LMSO has two layers. The first layer, PLMSO, is a polarized logic whose polarities respect the polarities of automata alluded to in §2. The second layer LMSO allows unrestricted polarities but for the exponential connectives !(−) and ?(−). The logic LMSO is only inspired from Linear Logic, since both its polarities and linearity are induced by our automata-based realizability model (to be detailed in §4 and §5) rather than by proof-theory (as in e.g. [17]).

3.1 The Language of LMSO

The formulae of PLMSO are divided into the positive formulae (written $\varphi^+$), the negative formulae (written $\varphi^-$) and the deterministic ones (written $\varphi^\text{det}$). They are defined on Fig. 3.

The formulae of LMSO are built from the polarized MSO formulae by using with unrestricted polarities all the connectives of PLMSO but for the exponentials !(−), ?(−). The formulae of LMSO are formally defined as follows:

$$\varphi, \psi ::= \varphi^\text{det} \mid \varphi \rightarrow \psi \mid \varphi \otimes \psi \mid \varphi \oplus \psi \mid \exists X.\varphi \mid \forall X.\varphi$$

In contrast with MSO\(^+\), the formulae of LMSO are not intended to be directly interpreted in the standard model $\mathcal{N}$ of ω-words. We will instead interpret them in an automaton-based realizability model in the vein of [22, 25]. As such, the connectives of LMSO directly reflect usual operations on alternating ω-word automata:

- LMSO-formulae are to be thought about as representing alternating automata. Positive, negative and deterministic formulae represent resp. non-deterministic, universal and deterministic automata.
- $\otimes$ and $\oplus$ are conjunctions and disjunctions based on a direct product of automata\(^10\). The linear implication $\rightarrow$ has been introduced in [25].
- The quantifiers $\exists$ and $\forall$ correspond to the usual operations of projection and co-projection (see e.g. [25]).
- The exponentials $?$ and $!$ correspond to determinization operations.

As usual with alternating automata, projections only correctly implement existential quantifications on non-det. automata. Dually, co-projections completely implement universal quantifications on universal automata. However, both operations can always be defined on alternating automata, and moreover with their intended categorical semantics [25]. This implies that they can be used in a deduction system.

In PLMSO, since existential (resp. universal) quantifications can only be used on positive (resp. negative) formulae, all connectives will indeed have their usual (standard) meaning. This in particular permits the following simple translation from MSO\(^+\)-formulae to PLMSO-formulae.

**Definition 3.1 (Simple Translation).** The translation $(−)^L$ is defined by induction on MSO\(^+\)-formulae as follows:

$$
\begin{align*}
T^L & ::= T & (\varphi \land \psi)^L & ::= \varphi^L \otimes \psi^L \\
\bot^L & ::= \bot & (\varphi \lor \psi)^L & ::= \varphi^L \lor \psi^L \\
\alpha^L & ::= \alpha & (\varphi \rightarrow \psi)^L & ::= \varphi^L \rightarrow \psi^L \\
(\exists X.\varphi)^L & ::= ?\exists X.\varphi^L & (\forall X.\varphi)^L & ::= !\forall X.\varphi^L
\end{align*}
$$

Note that $\varphi^L$ is always a deterministic formula of PLMSO.

Let us stress a couple of important points.

(a) It would have been natural to also allow the usual (additive) non-deterministic disjunction $\oplus$ and its corresponding conjunction $\&$. But this would have required additional structure in our realizability model, while have chosen to keep it as simple as possible in this paper.

(b) Thanks to the Simulation Theorem [21]\(^11\), it would have been possible to have exponentials $?\varphi$ and $!\varphi$ for all LMSO-formulae. In this case, $!\varphi$ would represent an ND automaton simulating the alternating automaton representing $\varphi$. The general exponential $!$ has been investigated in a Curry-Howard setting [25]. We forbid these operations here because they impose realizers to concretely depend on applications of McNaughton’s Thm. 2.10.

3.2 The Deduction System of LMSO

Deduction in LMSO is performed using the rules of Fig. 4, the Arithmetic Rules of Fig. 2 and following axiom schemes:

- **Induction.** For each negative $\varphi^-$, the following rule (where $y, z$ are fresh, $\varphi^+$ are positive and $\psi^-$ negative):

  $\begin{align*}
  \varphi^+, 0(z) \vdash \varphi^+[z/x, \overline{\psi}]
  \end{align*}
  \center
  \begin{align*}
  \varphi^+, S(y, z), !((\varphi^-)[y/x, x], \overline{\psi}) \vdash \varphi^+[z/x, \overline{\psi}]
  \end{align*}
  \center
  \begin{align*}
  \exists X.\varphi, \overline{\psi} \vdash \forall X.\varphi^+, \overline{\psi}
  \end{align*}

- **Deterministic Comprehension.** For each deterministic $\varphi^\pm$ with $X$ not free in $\varphi^\pm$, the axiom

  $\vdash ?\exists X!\forall x (X x \rightarrow \varphi^\pm)$

- **Definition of Mealy machines.** For each function symbol $t_M$ representing the machine $\mathcal{M} : 2^n \rightarrow 2$, the axiom

  $\vdash \forall X \forall x (x \in t_M(X) \rightarrow \delta_M(x, \overline{X} x)^L)$

  where $\delta_M$ is the formula of Prop. 2.6.

- **Polarized Double Negation Elimination.** For each PLMSO-formula $\varphi$, the axiom

  $\vdash \varphi^\pm \vdash \varphi$

  where $\psi^\pm := \psi \rightarrow \bot$ (note that $\varphi^\pm$ is a PLMSO-formula of the same polarity as $\varphi$).

\(^9\)An interesting consequence of [7] is that the negative fragment of MSO\(^+\) is expressively complete.

\(^10\)As such, $\forall$ does not exist on tree automata.

\(^11\)Which is not required to deal with ω-regular properties.
\( \varphi^\pm, \psi^\pm := \top \mid \bot \mid \alpha \mid \lnot (\varphi^-) \mid ?(\varphi^+) \mid \varphi^\pm \otimes \psi^\pm \mid \varphi^\pm \uplus \psi^\pm \mid \varphi^\pm \rightarrow \psi^\pm \)

\( \varphi^+, \psi^+ := \varphi^\pm \mid \exists X. \varphi^+ \mid \varphi^+ \otimes \psi^+ \mid \varphi^+ \uplus \psi^+ \mid \varphi^- \rightarrow \psi^+ \)

\( \varphi^-, \psi^- := \varphi^\pm \mid \forall X. \varphi^- \mid \varphi^- \otimes \psi^- \mid \varphi^- \uplus \psi^- \mid \varphi^+ \rightarrow \psi^- \)

- **Deterministic Exponentials.** For each deterministic formula \( \varphi^\pm \), the axioms
  \( \varphi^\pm \vdash \lnot (\varphi^\pm) \) and \( ?(\varphi^\pm) \vdash \varphi^\pm \)

Even if LMSO has a multiplicative disjunction \( \otimes \), which naturally leads to sequents with multiple formulae on the right of \( \rightarrow \), the proof-system is actually constructive, as witnessed by the right rules for \( \forall \) and \( \rightarrow \), and by the polarity condition in the right contraction rule. Similarly, double negation elimination is only assumed for polarized formulae, so that \( \varphi \rightarrow \psi \) is not isomorphic to \( \varphi^- \otimes \psi \). In Ex. 5.11 we will see that double negation elimination is realizable for all formulae, but is not an isomorphism.

Our first (expected) result on LMSO is that the translation \((\rightarrow)^{\text{L}}\) correctly interprets MSO\(^+\) in LMSO.

**Theorem 3.2.** Given an MSO\(^+\) formula \( \varphi \), if MSO\(^+\) \( \vdash \varphi \) then LMSO \( \vdash \varphi \).

Thanks to the completeness of MSO\(^+\) (Thm. 2.11), Thm. 3.2 implies that LMSO is complete w.r.t. Church’s synthesis.

**Corollary 3.3.** If an MSO\(^+\)-formula \( \varphi(\bar{Y}, \bar{Z}) \) admits a (f.s.) causal realizer, then LMSO \( \vdash \forall \bar{Y}. \exists \bar{Z}. \varphi^L(\bar{Y}, \bar{Z}) \).

### 4 Games and Automata

We present here our games and automata model. It is a simplification to \( \omega \)-words of the model presented in [25] for infinite trees. All statements of this Section (excepted those relative to the \( \forall \)-completeness) are proved in [25].

This model targets two indexed categories: The categories \( \text{Aut}_\Sigma \) of automata over alphabet \( \Sigma \) are indexed over \( \mathbf{M} \), while the categories \( \text{DA}_\Sigma \) of (substituted) automata over \( \Sigma \) are indexed over \( \mathbf{S} \). Moreover, the categories \( \text{Aut}_{\Sigma (-)} \) are equipped with the required categorical structure to interpret the linear part of LMSO.

All the structure we use on \( \text{DA}_{(-)} \) and \( \text{Aut}_{(-)} \) is ultimately induced by the symmetric monoidal closed structure of a category \( \text{DZ} \) of zig-zag games, that we detail first.

#### 4.1 Simple Zig-Zag Games

We present here the category \( \text{DZ} \) of zig-zag games, and discuss some structure relevant to us: symmetric monoidal closure and a construction of indexed categories inspired from [13] and generalizing simple fibrations (see e.g. [14]).

**Definition 4.1.** A game \( A \) has the form \( A \equiv (A_P, A_O) \) where \( A_P \) and \( A_O \) are alphabets of resp. P and O-moves.

We are interested in a very specific form of strategies.

**Definition 4.2.** Given games \( A \) and \( B \), a (total zig-zag) strategy \( \sigma : A \rightarrow_\text{DZ} B \) is a pair of functions \( \sigma = (f, F) \) where

\[
\begin{align*}
  f & : \bigcup_{n \in \mathbb{N}} (A_P^{n+1} \times B_O^n) \rightarrow B_P \\
  F & : \bigcup_{n \in \mathbb{N}} (A_P^{n+1} \times B_O^{n+1}) \rightarrow A_O
\end{align*}
\]

Intuitively, a total zig-zag strategy \( \sigma : A \rightarrow_\text{DZ} B \) amounts to a strategy for \( P \) in an infinite game which consists in \( \mathbb{N} \)-indexed sequences of rounds. In a single round \( n \in \mathbb{N} \), four moves occur in succession:

1. \( O \) plays a move \( a_P^n \in A_P \),
2. \( P \) plays a move \( b_O^n \in B_O \),
3. \( O \) answers with a move \( b_O^n \in B_O \),
4. \( P \) concludes with a move \( a_O^n \in A_O \).

**Proposition 4.3.** Games and (total zig-zag) strategies form a category \( \text{DZ} \).

**Proposition 4.4** (Symmetric Monoidal-Closed Structure). The category \( \text{DZ} \) is symmetric monoidal-closed. The monoidal unit is \( I = (\{\ast\}, \{\ast\}) \). Given games \( A \) and \( B \), the monoidal product \( A \otimes B \) and the internal horn \( A \otimes B \rightarrow B \) are given by

\[
\begin{align*}
  A \otimes B & := (A_P \times B_P, A_O \times B_O) \\
  A \otimes B & := (B_P^A \times A_O^B, A_O \times B_O)
\end{align*}
\]

**Monoids and Comonoids.** A commutative monoid in a symmetric monoidal category (SMC) \( (\mathbb{C}, \otimes, I) \) is an object \( M \) equipped with structure maps \( m : M \otimes M \rightarrow M \) and \( u : I \rightarrow M \) subject to coherence conditions (see e.g. [19]). A (commutative) monoid in \( \mathbb{C} \) is a (commutative) monoid in \( \mathbb{C}^{op} \). In this paper, by (co)monoid we always mean commutative (co)monoid. The category of (co)monoids in \( (\mathbb{C}, \otimes, I) \) is the (co)monoids as objects and maps are \( \mathbb{C} \)-maps which commute with the (co)monoid structure. We write \( \text{Comon}(\mathbb{C}) \) for the category of comonoids of \( (\mathbb{C}, \otimes, I) \).

Games \( A \) with \( A_P \backsimeq \{\ast\} \) \( (A_O \backsimeq \{\ast\}) \) induce (co)monoids in \( (\text{DZ}, \otimes, I) \). The following is well-known (see [19, §6.5]).

**Proposition 4.5.** The category of comonoids (resp. monoids) of an SMC \( (\mathbb{C}, \otimes, I) \) has finite products (resp. coproducts) induced by \( (\otimes, I) \).

Given an alphabet \( \Sigma \), we write \( \Sigma \) for the \( \text{DZ} \)-object \( (\Sigma, \{\ast\}) \).

**Proposition 4.6.** \( \mathbb{S} \) is equivalent to the full subcategory of \( \text{Comon}(\text{DZ}) \) whose objects are induced by alphabets.

**Comonoid Indexing.** Given a comonoid \( K \) in an SMC \( (\mathbb{C}, \otimes, I) \), the functor \( A \mapsto K \otimes A \) of comonoid indexing with \( K \) is equipped with a comonad structure whose co-Kleisli category \( \text{KI}(K) \) is an SMC for \( \text{KI}(K) = I \) and (on objects) \( A \otimes_{\text{KI}(K)} B = A \otimes B \) [13, Prop. 5].\(^{13}\) Note that each \( \text{Comon}(\mathbb{C}) \)-map \( f : K \rightarrow \text{KI}(L) \) induces a functor \( f^* : \text{KI}(L) \rightarrow \text{KI}(K) \). This extends to a functor \( (\rightarrow)^* : \text{Comon}(\mathbb{C})^{op} \rightarrow \text{Cat} \)

taking \( K \) to \( \text{KI}(K) \).

We let \( \text{DI}(\Sigma) \) be the co-Kleisli category of comonoid indexing with \( \Sigma \). It has the same objects as \( \text{DZ} \), and its \( \text{DZ} \)-maps are actually total zig-zag strategies in the simple game \( A \rightarrow B \) with \( \rightarrow \) negative and \( A, B \) positive (\cite{11}, see also \cite{19}).

\(^{12}\) See also [25, Prop. 4.4] and [19, §6.5 & 6.6].
The category \( DZ \) is symmetric monoidal-closed for \( A \otimes_{DZ}(\Sigma) B \coloneqq A \otimes B \) (with unit \( I \)) and internal hom \( A \Rightarrow_{DZ}(\Sigma) B \coloneqq (A \Rightarrow B) \).

We write \((-)^\dagger\) for the canonical functor \( DZ(\Sigma) \rightarrow DZ \) taking \( \sigma : A \Rightarrow_{DZ}(\Sigma) B \) to \( \sigma^\dagger : \Sigma \square A \Rightarrow DZ \Sigma \square B \).

### 4.2 Games with Winning

As usual, acceptance will be defined using games equipped with winning conditions.

**Proposition 4.7.** \( DZ(\Sigma) \) is symmetric monoidal-closed for \( A \otimes_{DZ}(\Sigma) B \coloneqq A \otimes B \) (with unit \( I \)) and internal hom \( A \Rightarrow_{DZ}(\Sigma) B \coloneqq (A \Rightarrow B) \).

**Definition 4.8.** A game with winning is a game \( A \) equipped with a winning condition \( W_A \subseteq (A_0 \times A_0)^\omega \).

**Definition 4.9.** Consider games with winning \( (A, W_A) \) and \( (B, W_B) \), and a strategy \( \sigma = (f, F) : A \rightarrow_{DZ} B \).

Given sequences \((a_n^0)^n \in A_0^\omega\) and \((b_n^0)^n \in B_0^\omega\), the strategy \( \sigma \) induces sequences \((b_n^p)^n \in B_p^\omega\) and \((a_n^0)^n \in A_0^\omega\) defined as

\[
\begin{align*}
b_n^p &\coloneqq f(a_0^p, \ldots, a_n^p, b_0^p, \ldots, b_{n-1}^p) \in B_p \\
and 
a_n^0 &\coloneqq F(a_0^p, \ldots, a_n^p, b_0^p, \ldots, b_n^0) \in A_0.
\end{align*}
\]

Then \( \sigma \) is winning if for all \((a_n^0)^n \in A_0^\omega\), the induced sequences \((b_n^0)^n \in B_0^\omega\) and \((b_n^p)^n \in B_p^\omega\), we have \((b_n^0)^n \in W_B\) whenever \((a_n^0)^n \in W_A\).

**Proposition 4.10.** Games and winning strategies form a category \( DZ^W \).

The SMC structure \((\square, I, \square \rightarrow)\) of \( DZ \) lifts to \( DZ^W \), inducing a model of IMLL.

**Proposition 4.11.** (Symmetric Monoidal-Closed Structure) The category \( DZ^W \) is symmetric monoidal-closed. The unit is \( \top \coloneqq (I, (\bullet)^\omega) \). Given \( (A, W_A) \) and \( (B, W_B) \), the tensor product \( (A, W_A) \otimes (B, W_B) \) and the linear arrow \( (A, W_A) \rightarrow_o (B, W_B) \) are given by

\[
\begin{align*}
(A, W_A) \otimes (B, W_B) &\coloneqq (A \otimes B, W_{A \otimes B}) \\
and (A, W_A) \rightarrow_o (B, W_B) &\coloneqq (A \Rightarrow B, W_{A \Rightarrow B}) \\text{where} \quad (a_n^p, b_n^0, a_n^0) \in W_{A \otimes B} \iff ((a_n^p, a_n^0) \in W_A \text{ and } (b_n^0) \in W_B) \\
and (f_n, F_n, a_n^p, b_n^0) \in W_{A \Rightarrow B} \iff (f_n(a_n^p, b_n^0)) \in W_A \Rightarrow (f_n(a_n^p, b_n^0)) \in W_B \\
\text{Winning also induces a disjunctive symmetric monoidal structure on } DZ^W.
\end{align*}
\]

**Proposition 4.12.** (Multiplicative Disjunction). The category \( DZ^W \) is symmetric monoidal with unit \( \top \coloneqq (I, \emptyset) \) and \( (A, W_A) \otimes (B, W_B) \coloneqq (A \otimes B, W_{A \otimes B}) \) where \((a_n^p, b_n^0, a_n^0) \in W_{A \otimes B} \iff \text{either } (a_n^p, a_n^0) \in W_A \text{ or } (b_n^0) \in W_B\).

We write \( A \) for \( (A, W_A) \) when no confusion arises. Note that since sets of moves are assumed to be non-empty, \( DZ^W \) is equipped with (non-canonical) weakening maps \( A \rightarrow_{DZ^W} 1 \) and \( \top \rightarrow_{DZ^W} A \).

### 4.3 Uniform Automata

The adequacy of realizability will be proved using the notion of uniform automata (UA’s), adapted from [25]. UA’s are essentially usual alternating automata, but in which alternation is expressed via an explicitly given set of moves.

**Definition 4.13.** A uniform automaton \( (UA, Q_A) \) over \( \Sigma \) (notation \( A : \Sigma \)) has the form

\[
A = (A_B, Q_A, q_A^0, \partial_A, \Omega_A)
\]

where \( A_B \) (resp. \( A_0 \)) is the alphabet of \( P \) (resp. \( O \)) moves, \( Q_A \) is the alphabet states (with \( q_A^0 \in Q_A \text{ initial} \)), the transition function \( \partial_A \) has the form

\[
\partial_A : Q_A \times \Sigma \rightarrow A_B \times A_0 \rightarrow Q_A
\]

and the acceptance condition \( \Omega_A \) is an \( \alpha \)-regular subset of \( Q_A^\omega \). \( A \) is called positive (or, in accordance with automata-theoretic

---

**Figure 4.** The Deduction Rules of LMSO (where \( Z \) is fresh for \( \phi, \phi' \) in each rule mentioning it).
terminology, non-deterministic) if \( A_0 \simeq 1 \), negative (or, in accordance with automata-theoretic terminology, universal) if \( A_0 \simeq 1 \) and deterministic if it is both positive and negative.

The interpretation of PLMSO formulae will respect polarities.

An automaton \( A : \Sigma \to \Gamma \) together with a causal function \( F \in S[\Sigma, \Gamma] \) induce a substituted acceptance game \( A(F) : \Sigma \) with \( P \)-moves \( \Sigma \times A_0 \) and \( O \)-moves \( A_0 \). We equip \( A(F) \) with the winning condition consisting of the \( \omega \)-sequences \((b_n, q'_n, q''_n) \in ((\Sigma \times A_0) \times A_0)^\omega\) such that \((q_n)_n \in \Omega_A\) where \( q_0 := q'_0 \) and \( q_{n+1} := \partial_A(q_n, F(b_n, \ldots, b_n), a'_n, a''_n) \).

The substituted acceptance game \( A(F) : \Sigma \) is an object of \( DZ^\omega \). Acceptance of \( B \in \Sigma^\omega \simeq S[1, \Sigma] \) by \( A \) is defined via the game \( A(B) : 1 \).

**Definition 4.14.** An automaton \( A : \Sigma \) accepts the \( \omega \)-word \( B \in \Sigma^\omega \) if there is a winning strategy \( \sigma \in DZ^\omega[\Sigma, A(B)] \). We let \( L(A) \) be the set of \( \omega \)-words accepted by \( A \).

### 4.4 Some Structure on Automata

Our goal here is to display some structure on automata that will produce a realizability model of LMSO.

**Definition 4.15.** The category \( DA^\Sigma \) has games of the form \( A(F) : \Sigma \) as objects. Maps from \( A(F) \) to \( B(G) \) are \( DZ^\Sigma \)-maps \( \sigma \) from \( (A_0, A_0) \) to \((B_0, B_0)\), whose lift are winning strategies \( \sigma^\uparrow : A(F) \to DZ^\omega B(G) \).

\( Aut_\Sigma \) is the full subcategory of \( DA^\Sigma \) whose objects are of the form \( A(Id_\Sigma) : \Sigma \) (denoted \( A : \Sigma \)) where \( Id_\Sigma \) is the \( S \)-identity on \( \Sigma \). We let \( Aut^+_\Sigma \) (resp. \( Aut^-_\Sigma \), \( Aut^\pm_\Sigma \)) be the restriction of \( Aut_\Sigma \) to positive (resp. negative, deterministic) automata.

We write \( \sigma : A(F) \to B(G) \) when \( \sigma \) is a \( DA^\Sigma \)-map from \( A(F) \) to \( B(G) \). Note that substituted acceptance games \( A(F) : \Sigma \) are \( DZ^\omega \)-objects with \( P \)-moves \( \Sigma \times A_0 \) and \( O \)-moves \( A_0 \), while a \( DA^\Sigma \)-map from \( A(F) \to B(G) \) is in fact a \( DZ \)-map \( \Sigma \sqsubseteq (A_0, A_0) \to \Sigma \sqsubseteq (B_0, B_0) \).

**Substitution.** The categories \( DA^\Sigma \) are indexed over \( S \), while the categories \( Aut_\Sigma \) are indexed over \( M \). An immediate consequence is that the realizability arrow \( \to \) is correct w.r.t. language inclusion.

**Proposition 4.16.** Given \( A, B : \Sigma \), if there is an \( Aut_\Sigma \)-map \( A \to B \), then \( L(A) \subseteq L(B) \).

Notice that a crucial point in the game \( A \to B \) is that the word \( w \) is progressively given by the plays of \( O \); if it were a data given before the first round, the previous proposition would be an equivalence.

**Monoidal-Closed Structure.** The symmetric monoidal-closed structures of \( DZ[\Sigma] \) and \( DZ^\omega \) lift to each category \( Aut_\Sigma \).

The unit automaton \( \top \) has \( P \)-moves, \( O \)-moves and states \( (\bullet) \) (with thus \( \bullet \) initial) and acceptance condition \((\bullet)^\omega \). Given \( A, B : \Sigma \), the monoidal product \((A \otimes B) : \Sigma \) and the linear arrow \((A \to B) : \Sigma \) both have states sets \( Q_A \times Q_B \) with \((q'_A, q'_B) \) initial. Their moves are given (via Prop. 4.7) by Prop. 4.4:

\[
(A \otimes B)_p := A_0 \times B_0 \\
(A \to B)_p := B_0^p \times A_0^{A_0 \times B_0} \\
(A \otimes B)_0 := A_0 \times B_0 \\
(A \to B)_0 := A_0 \times B_0
\]

For the transition functions, we let

\[
\partial_{A \otimes B}(\langle q_A, q_B \rangle, a, (a^p, b^p), (a^0, b^0)) := (q_0, q_1) \\
\partial_{A \to B}(\langle q_A, q_B \rangle, a, (f, F), (a^p, b^p)) := (q_0, q_1)
\]

where

\[
q_0 := \partial_A(q_A, a, a^p, a^0) \\
q_1 := \partial_B(q_B, b, b^p, b^0)
\]

Finally, we let \((q_n, q'_n)_n \in \Omega_{A \otimes B} \) iff \((q_n)_n \in \Omega_A \) and \((q'_n)_n \in \Omega_B \), and we let \((q_n, q'_n)_n \in \Omega_{A \to B} \) iff \((q_n)_n \in \Omega_A \) implies \((q'_n)_n \in \Omega_B \).

**Proposition 4.17.**

(a) \((Aut_\Sigma, \otimes, \top, \to)\) is a symmetric monoidal closed.

(b) We have \( L(\top : \Sigma) = \Sigma^\omega \) and \( L(A \otimes B) = L(A) \cap L(B) \).

(c) By determinacy of \( \omega \)-regular games, \( B \in L(\Sigma) \) iff \( B \notin L(A) \).

**Multiplicative Disjunction.** The multiplicative disjunction \((\vee, \sqsubseteq) \) of \( DZ^\omega \) induces a symmetric monoidal structure in each \( Aut_\Sigma \). The falsity automaton \( \bot \), as defined as \( \top \) above, with acceptance condition \( \emptyset \subseteq \{a\}^\omega \). Given \( A, B : \Sigma \), the UA \( A \sqsubseteq B \) is defined as \( \bot \) above, but with \((q_n, q'_n)_n \in \Omega_{A \sqsubseteq B} \) iff either \((q_n)_n \in \Omega_A \) or \((q'_n)_n \in \Omega_B \).

**Proposition 4.18.** \( L(\bot) = \emptyset \) and \( L(A \sqsubseteq B) = L(A) \cup L(B) \).

It follows from §4.1 that \((\otimes, \bot)\) induces finite products in \( Aut_\Sigma \) and that \((\vee, \sqsubseteq)\) induces finite co-products in \( Aut_\Sigma \).

**Quantifications.** Quantifications in UA’s can be seen as simple adaptations of quantifications in usual alternating automata. They are actually induced, via the generalization of simple fibrations to comonoid indexing (§4.1), by the categorical quantifiers in simple fibrations (see e.g. [14, Prop. 1.9.3]).

In this paper, we only need the following.

**Definition 4.19.** Given \( A : \Sigma \times \Gamma \to \Gamma \), let

\[
\langle \exists \Gamma, A : \Sigma \rangle := \Gamma \times A_\Gamma : A_0, Q_A, q'_A, \partial_{\exists \Gamma, A} : \Omega_A \) \\
\langle \forall \Gamma, A : \Sigma \rangle := \Gamma \times A_\Gamma : A_0, \Gamma \times Q_A, Q_A, \partial_{\forall \Gamma, A} : \Omega_A
\]

where

\[
\partial_{\exists \Gamma, A}(q, a, (b, a^p), a^0) := \partial_{A}(q, (a, b), a^p, a^0) \\
\partial_{\forall \Gamma, A}(q, a, (b, a^p), a^0) := \partial_{A}(q, (a, b), f(b), a^0)
\]

**Proposition 4.20.** Given \( A : \Sigma \times \Gamma \) and \( B(C) : \Sigma \), we have

\[
DA_{\Sigma}:([\exists \Gamma, A](B(C)), B(C)) \simeq DA_{\Sigma, \Gamma}[A(B \times I_{\Gamma})_1, B(C \circ [\pi_{\Sigma}])] \\
DA_{\Sigma}:([\forall \Gamma, A](B(C)), B(C)) \simeq DA_{\Sigma, \Gamma}[B(B \circ [\pi_{\Sigma}])_1, B(C \times I_{\Gamma})]
\]

Moreover, there are canonical maps \( \langle \forall \Gamma, A \rangle([\pi_{\Sigma}]) \to A \) and \( A \to \langle \exists \Gamma, A \rangle([\pi_{\Sigma}]) \).

**Proposition 4.21.** If \( A : \Sigma \times \Gamma \) is positive then \( B \in L(\exists \Gamma, A) \) iff there exists \( C \in \Gamma^\omega \) such that \((B, C) \in L(A) \).

If \( A : \Sigma \times \Gamma \) is negative then \( B \in L(\forall \Gamma, A) \) iff for all \( C \in \Gamma^\omega \) we have \( \langle B, C \rangle \in L(A) \).

\footnote{Which correspond to quantifications in Dialectica categories [6, 12].}
4.5 Polarities and Duality

Say that \( \mathcal{A} \) is polarized if \( \mathcal{A} \) is positive or negative. Polarized automata are particularly well-behaved. First, they are equipped with a direct complementation operation \((-)^\perp\), which is defined as

\[
\mathcal{A}^\perp := (A_0, A^\perp, Q_\mathcal{A}, q^0, \partial_{A^\perp}, Q^\perp_\mathcal{A} \setminus \Omega_\mathcal{A})
\]

where \( \partial_{A^\perp}(q_a, a^0, a^0) := \partial_a(q_a, a_a, a^0) \). For \( \mathcal{A}, \mathcal{B} : \Sigma \) of opposite polarities, we have the following isomorphism in \( \text{Aut}_\Sigma \):

\[
\mathcal{A} \rightarrow \mathcal{B} \simeq \mathcal{A}^\perp \uplus \mathcal{B}
\]

This in particular implies \( \mathcal{A} \rightarrow \perp \simeq \mathcal{A}^\perp \), which has the following interesting consequence.

Corollary 4.22. If \( \mathcal{A} \) is polarized, then for all \( B \), we have \( B \in \mathcal{L}(\mathcal{A}^\perp) \) iff \( B \notin \mathcal{L}(\mathcal{A}) \).

Second, det. automata are closed under \( \otimes, \uplus, (\_)^\perp \), and positive and negative automata are closed under the following productions (where \( \mathcal{A}^+ \) is positive, \( \mathcal{A}^- \) is negative and \( \mathcal{D} \) is deterministic):

\[
\begin{align*}
\mathcal{A}^+, \mathcal{B}^+ & := \mathcal{D} \mid (\mathcal{A}^+)^\perp \mid \exists X. \mathcal{A}^+ \\
\mathcal{A}^-, \mathcal{B}^- & := \mathcal{D} \mid (\mathcal{A}^-)^\perp \mid \forall X. \mathcal{A}^-
\end{align*}
\]

This, together with the fact that exponentials \(?\) and \(!\) always give det. automata (see Prop. 5.2 below), will imply that the interpretation of PLMSO-formulae preserves polarities.

Third, we have the following isos in \( \text{Aut}_\Sigma \) (where \( \mathcal{A} \) and \( \mathcal{B} \) have opposite polarities):

\[
(\mathcal{A}^+)^\perp \simeq \mathcal{A} \quad (\exists \Sigma \mathcal{A})^\perp \simeq \exists \Sigma \mathcal{A}^+ \\
(\mathcal{A} \otimes \mathcal{B})^\perp \simeq \mathcal{A}^+ \uplus \mathcal{B}^+ \\
(\mathcal{A} \uplus \mathcal{B})^\perp \simeq \mathcal{A}^+ \uplus \mathcal{B}^+
\]

5 The Realizability Model of LMSO

This last Section connects the two previous ones: we show that the categories \( \text{Aut}(\perp) \) provide a realizability model of LMSO. This in particular implies the correctness of LMSO w.r.t. Church’s synthesis.

5.1 The Realizability Interpretation of LMSO

We have seen in §4.4 that uniform automata are equipped with categorical structure for the interpretation of the connectives \( \top, \otimes, \perp, \uplus, \exists, \forall \) of LMSO. In order to devise an interpretation of all LMSO-formulae, it remains to deal with the atoms \( \alpha \in \mathcal{A} \), and with the exponential modalities \( (\_)^\perp \) and \( (?)^\perp \). Atoms are dealt-with as usual (see e.g. [28]), and we rely on McNaughton’s Thm. 2.10 for \( (\_)^\perp \) and \( (?)^\perp \).

Proposition 5.1. For each atom \( \alpha \in \mathcal{A} \) with free variables among \( \mathcal{X} \), there is a deterministic automaton \( \mathcal{A}_\alpha \) such that \( \mathcal{B} \in \mathcal{L}(\mathcal{A}_\alpha) \) iff \( \mathfrak{N} \models (\alpha(\mathcal{B})) \).

Proposition 5.2. Given a positive (resp. negative) automaton \( \mathcal{A} : \Sigma \), there is a deterministic automaton \( \mathcal{A}^\perp : \Sigma \) (resp. \( \mathcal{A} : \Sigma \)) which recognizes the same language as \( \mathcal{A} \).

Note that Prop. 5.2 produces deterministic automata, which therefore only have trivial realizers. Hence, no construction for McNaughton’s Thm. 2.10 is actually required for the extraction of realizers from proofs.

Interpretation of PLMSO-Formuilae. We are now ready to define the interpretation of LMSO-formulae as automata.

Definition 5.3. The automaton \( [\varphi] : 2^n \), for \( \varphi \) an LMSO-formula with free variables among \( \mathcal{X} = X_1, \ldots, X_n \), is defined by induction on \( \varphi \) as follows:

\[
\begin{align*}
[T] & := T \\
[\bot] & := \bot \\
[\alpha] & := \alpha \\
[\exists \Sigma \varphi] & := [\exists \Sigma \varphi] \\
[\forall \Sigma \varphi] & := [\forall \Sigma \varphi] \\
[\varphi^\perp] & := [\varphi^\perp] \\
[\psi^\perp] & := [\psi^\perp] \\
\end{align*}
\]

This definition requires some comments. First, it follows from §4.5 that \([\_]\) respects polarities of LMSO-formulae, so that \([?\varphi^\perp]\) and \([?!\varphi]\) are well-defined. Also, in the cases of \( \otimes, \uplus, \perp \) we assume that both compound formulae have free variables among \( X_1, \ldots, X_n \). For \( \forall X. \varphi \) and \( \exists X. \varphi \), we assume that \( \varphi \) has free variables among \( X, X_1, \ldots, X_n \).

5.2 Correctness of PLMSO w.r.t. \( \mathfrak{N} \)

Since \([\_]\) respects polarities of PLMSO-formulae, it follows from the properties of §4.4 that for PLMSO-formulae, the quantifiers \( \exists \) and \( \forall \) are correctly implemented by the corresponding operations on automata. As a consequence, the interpretation \([\_]\) of PLMSO-formulae is correct w.r.t. the following erasure map.

Definition 5.4. The erasure map \([\_]\) is defined by induction on LMSO-formulae as follows:

\[
\begin{align*}
[T] & := T \\
[\bot] & := \bot \\
[\alpha] & := \alpha \\
[\exists \Sigma \varphi] & := [\exists \Sigma \varphi] \\
[\forall \Sigma \varphi] & := [\forall \Sigma \varphi] \\
[?\varphi] & := [?\varphi] \\
[?!\varphi] & := [?!\varphi] \\
\end{align*}
\]

Proposition 5.5. For a PLMSO-formula \( \varphi, \mathcal{B} \in \mathcal{L}([\varphi]) \) if and only if \( \mathfrak{N} \models [?\varphi](\mathcal{B}) \).

Proposition 5.6. \([?\varphi^\perp]\) is realized if and only if \( \mathfrak{N} \models [?!\varphi^\perp] \).

5.3 Adequacy and Realized Axioms

The central result on \([\_]\) is its adequacy:

Theorem 5.7. Given LMSO-formulae \( \exists \varphi_1, \ldots, \varphi_n \) and \( \psi = \psi_1, \ldots, \psi_m \), from a derivation of \( \varphi_1 \vdash \text{LMSO} \psi \), one can extract a f.s. realizer of \( \varphi_1 \vdash \ldots \vdash \varphi_n \rightarrow \psi_1 \ldots \rightarrow \psi_m \).

In the statement of Thm. 5.7, the interpretation \([\_]\) is taken for \( \mathcal{X} \) containing all the free variables of \( \varphi \) and \( \psi \).

An immediate consequence of Thm. 5.7 is that from a proof of LMSO \( \forall \Sigma \exists \Sigma, \varphi(\mathcal{Y}; \mathcal{Z}) \) one can extract Mealy machines \( \mathcal{M} \) together with f.s. realizer of \( \top \rightarrow [?\varphi(\mathcal{Y}; \mathcal{Z})] \). When \( \varphi \) is a PLMSO formula, by Prop. 5.5 this gives a f.s. causal realizer of \( \varphi^\perp(\mathcal{Y}; \mathcal{Z}) \).

Corollary 5.8. Given a PLMSO-formula \( \varphi(\mathcal{Y}; \mathcal{Z}) \), from a proof of LMSO \( \forall \Sigma \exists \Sigma, \varphi(\mathcal{Y}; \mathcal{Z}) \) one can extract a f.s. causal realizer of \( \varphi^\perp(\mathcal{Y}; \mathcal{Z}) \).

A general feature of realizability models is that they may realize more statements than those provable in the theory they interpret (see e.g. [15]). Here are some examples. Examples 5.9
and 5.10 are counterparts of usual additional axioms for intuitionistic arithmetic (see e.g. [15]).

**Example 5.9.** The following versions of “independence of premises” and Markov’s principle are realizable (where \(\varphi\) is negative, \(\delta, \delta'\) are deterministic and \(X\) is not free in \(\varphi, \delta\)):  
\[
(\varphi \rightarrow \exists X \psi) \rightarrow \exists X (\varphi \rightarrow \psi) \\
([\exists X \delta] \rightarrow \delta') \rightarrow \exists X (\delta \rightarrow \delta')
\]

**Example 5.10.** The following form of causal (functional) choice is realizable, for each negative formula \(\varphi\):  
\[
\forall X.\exists Y. \varphi(X, Y) \rightarrow \exists Z. \forall X. \varphi(X, \text{app}_2^{Z \in \Sigma} (X, Z))
\]

where \(X = X_1, \ldots, X_n\) (representing \(2^n\)), \(Z = Z_1, \ldots, Z_{2^n}\) (representing \((2 \rightarrow 2^n)\)) and \(\text{app}_2^{Z \in \Sigma} (\Gamma)\) stands for the Mealy machine \(\Gamma^{X \times \Sigma} \rightarrow \Gamma\) computing pointwise applicative.

**Example 5.11.** LMSO has an axiom for the elimination of double negation for PLMSO-formulae. One can actually realize \([\langle A \rightarrow \bot \rangle \rightarrow \bot] \rightarrow A\) for any \(A\) by a non-trivial combinatorial argument.\(^{15}\)

### 6 Conclusion

We introduced LMSO, a constructive linear proof system for MSO on \(\omega\)-words. LMSO is complete w.r.t. the translation \((-)^L\) for both MSO and Church’s synthesis. We devised an automata-based realizability semantics for LMSO. This model implies that LMSO is correct for Church’s synthesis. It also validates some extra axioms, counterparts of usual additional axioms to intuitionistic arithmetic.

**Further Works.** LMSO has a polarized subsystem PLMSO which reflects the usual polarities of alternating \(\omega\)-word automata and the corresponding polarized fragments of MSO.

We plan in future work to build on this feature, in particular because it corresponds to the polarities underlying the Safraless approaches of [7, 16]. Actually, universal automata are reminiscent from Gödel’s Functional (Dialectica) interpretation (see e.g. [15]).\(^{16}\) The Dialectica interpretation maps formulae to \(\exists\forall\)-formulae, in such a way that proofs induce witnesses for the prefix existential. This format is very close to the one obtained by reformulating the approach of [7] in MSO\(^\oplus\). We plan to investigate this further works.

### Acknowledgments

This work was partially supported by the ANR-14-CE25-0007-RAPIDO and by the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon.

### References


Figure 5. A Sequent Calculus for MSO\(^+\) (where Z is fresh for \(\overline{v}, \overline{v}'\) in each rule mentioning it).

A Proofs of §2 (Church’s Synthesis and MSO\(^+\))

**Theorem A.1** (Thm. 2.11). For each closed formula \(\varphi\) of MSO\(^+\),

\[\not\models \varphi\quad \text{iff} \quad \text{MSO}^+ \vdash \varphi\]

MSO\(^+\) is defined in §2 as deduction for first-order classical logic augmented with the Arithmetic Rules and Fig. 5, and the axiom schemes of **Induction, Comprehension** and **Definition of Mealy Machines** given in §2.

In order to prove Thm. A.1 we first eliminate the term symbols of MSO\(^+\) and to reduce to MSO.

**Lemma A.2.**

(a) For each term \(t\) of MSO\(^+\), MSO\(^+\) proves that

\[\exists X \forall x (x \in X \leftrightarrow x \in t)\]

(b) MSO\(^+\) proves that

\[\forall x (x \in t \leftrightarrow x \in u) \vdash \varphi[t/X] \leftrightarrow \varphi[u/X]\]

(c) Each MSO\(^+\)-formula is MSO\(^+\)-equivalent to an MSO-formula.

**Proof.**

(a) By induction on the terms of MSO\(^+\), using comprehension.

(b) The assumption \(\forall x (x \in t \leftrightarrow x \in u)\) unfolds to

\[\forall X (N(X) \rightarrow [X \subseteq t \leftrightarrow X \subseteq u])\]

But this implies \(t \subseteq u\) and \(u \subseteq t\), and thus \(t \equiv u\). The result then follows from the axiom:

\[t \equiv u, \ varphi[t/X] \vdash \varphi[u/X]\]

(c) The property is an easy consequence of the two above points.

We shall therefore prove the following version of Thm. A.1, where MSO refers to the axiomatization presented in §2, with deduction made in the system of Fig. 5 restricted to the language of MSO (this amounts to restrict the term \(t\) in the left \(\forall\)-rule and the right \(\exists\)-rule to monadic variables).

**Theorem A.3.** For each closed formula \(\varphi\) of MSO,

\[\not\models \varphi\quad \text{iff} \quad \text{MSO} \vdash \varphi\]

In order to prove Thm. A.3 we reduce to the axiomatization of MSO used in [22], that we call here MSO\(^\prime\). First, since we are in a classical setting, we can restrict to MSO-formulae build on the grammar:

\[\varphi, \psi ::= \alpha \mid T \mid \bot \mid \neg \varphi \mid \varphi \land \psi \mid \exists X \varphi\]

In the system of Fig. 5, this amounts to discard all rules concerning the connectives \(\lor, \rightarrow\) and \(\forall\), and to add the following rules:

\[
\begin{array}{c}
\frac{\varphi, \psi \vdash \bot}{\varphi, \psi \vdash \varphi}
\end{array}
\]
On the other hand, the MSO\(^\star\)-formulae of [22] are based on the following two-sorted language:\(^{17}\)

\[\Phi, \Psi ::= x \doteq y \mid x \leq y \mid S(x, y) \mid 0(x) \mid x \in X \mid T \mid \bot\]

As deduction system for MSO\(^\star\), we take the same system as MSO, augmented with the quantifier rules for individuals:

\[
\frac{\Phi, \Phi \vdash \Phi'}{\Phi, \exists x. \Phi \vdash \Phi'} \quad (x \text{ not free in } \Phi, \Phi') \quad \frac{\Phi \vdash \Phi[x/y], \Phi'}{\Phi \vdash \exists x. \Phi, \Phi'}
\]

We will define two translations:

- A translation taking an MSO-formula \(\varphi\) in the sense of §2 to an MSO\(^\star\)-formula \(\varphi\) in the sense of [22].
- A translation taking an MSO\(^\star\)-formula \(\Phi\) in the sense of [22] to an MSO-formula \(\Phi\) in the sense of §2.

The translations satisfy the following properties:

(a) For each closed formula \(\varphi\) in the sense of §2, we have

\[\mathcal{M} \models \varphi \iff \mathcal{M} \models \varphi\]

(b) For each formula \(\varphi\) in the sense of §2, MSO proves that

\[\varphi \iff \varphi\]

(c) For each closed formula \(\Phi\) in the sense of [22],

\[\text{MSO} \vdash \Phi \implies \text{MSO} \vdash \Phi\]

The above properties then imply Thm. A.3 from [22, Thm. 2.10].

**Definition A.4.** The translation \((-)^\uparrow\) is defined by induction on MSO-formulae in the sense of §2 as follows:

\[
(X \doteq Y)^\uparrow ::= \forall x (x \in X \iff x \in Y)
\]

\[
E(X)^\uparrow ::= \neg \exists x (x \in X)
\]

\[
(X \subseteq Y)^\uparrow ::= \forall x (x \in X \implies x \in Y)
\]

\[
N(X)^\uparrow ::= \exists ! x (x \in X)
\]

\[
0(X)^\uparrow ::= N(X)^\uparrow \land \forall x (x \in X \implies 0(x))
\]

\[
S(X, Y)^\uparrow ::= N(X)^\uparrow \land N(Y)^\uparrow \land \forall x, y (S(x, y) \rightarrow x \in X \rightarrow y \in Y)
\]

\[
(X \leq Y)^\uparrow ::= N(X)^\uparrow \land N(Y)^\uparrow \land \forall x, y (x \in X \rightarrow y \in Y \rightarrow x \leq y)
\]

\[
(\neg \varphi)^\uparrow ::= \neg (\varphi)^\uparrow
\]

\[
(\varphi \land \psi)^\uparrow ::= (\varphi)^\uparrow \land (\psi)^\uparrow
\]

\[
(\exists X. \varphi)^\uparrow ::= \exists X. (\varphi)^\uparrow
\]

Property (a) is obvious from the definition of \((-)^\uparrow\).

**Definition A.5.** The translation \((-)^\circ\) is defined by induction on MSO\(^\star\)-formulae in the sense of [22] as follows:

\[
(x \doteq y)^\circ ::= x \doteq y
\]

\[
(0(x))^\circ ::= 0(x)
\]

\[
(S(x, y))^\circ ::= S(x, y)
\]

\[
(x \leq y)^\circ ::= x \leq y
\]

\[
(x \in X)^\circ ::= x \subseteq X
\]

\[
(\neg \varphi)^\circ ::= \neg (\varphi)^\circ
\]

\[
(\varphi \land \psi)^\circ ::= \varphi \land (\psi)^\circ
\]

\[
(\exists X. \varphi)^\circ ::= \exists X. \varphi^\circ
\]

\[
(\exists x. \varphi)^\circ ::= \exists x. \varphi^\circ
\]

(where we have used the conventions of §2).

**Lemma A.6.** For each MSO-formula \(\varphi\) in the sense of §2, we have

\[\text{MSO} \vdash \varphi \iff \varphi^\circ\]

**Proof.** The proof is by induction on formulae. Since the composite translation \((-)^\circ\) commutes over all connectives, we just have to show the property for the atomic formulae of MSO (in the sense of §2).

\(^{17}\)The formula \(0(x)\) was noted \(Z(t)\) in [22].
• **Case of** \((X \equiv Y)\). We have
\[
(X \equiv Y)^_0 = \forall x \left( N(x) \rightarrow [x \subseteq X \leftrightarrow x \subseteq Y] \right)
\]

We have \(\varphi \vdash_{\textsc{MSO}} \varphi^*_0\) thanks to the axiom scheme:
\[
\frac{t \equiv u, \psi[t/X] \vdash \psi[u/X]}{\vdash t \subseteq u}
\]
The converse implication follows from the axioms
\[
\frac{t \subseteq u, u \subseteq t \vdash t \equiv u}{\text{(X fresh)}}
\]

- **Case of** \(E(X)\). We have
\[
(E(X))^_0 = \neg \exists x \left( N(x) \land x \subseteq X \right)
\]

We first show that \(\varphi \vdash_{\textsc{MSO}} \varphi^*_0\). Assume \(E(X)\) and \(N(x) \land x \subseteq X\). Since \(E(X)\) we have \(x \subseteq X\), so we get \(x \equiv X\). But this implies \(E(X) \land N(X)\), a contradiction.

Conversely, assume \(\neg \exists x \left( N(x) \land x \subseteq X \right)\). In order to show \(E(X)\) we show \(\forall Y. X \subseteq Y\). We apply the axiom
\[
\frac{N(Z), Z \subseteq X \vdash Z \subseteq Y}{\vdash X \subseteq Y} \quad \text{(Z fresh)}
\]
and we are done thanks to our assumption \(\neg \exists Z \left( N(Z) \land Z \subseteq X \right)\).

• **Case of** \((X \subseteq Y)\). We have
\[
(X \subseteq Y)^_0 = \forall x \left( N(x) \rightarrow x \subseteq X \rightarrow x \subseteq Y \right)
\]

If \((X \subseteq Y)\) then by transitivity of \(\subseteq\) we have \(Z \subseteq Y\) for all \(Z \subseteq X\), so that we get \((X \subseteq Y)^_0\).

The converse direction is given by the axiom
\[
\frac{N(Z), Z \subseteq X \vdash Z \subseteq Y}{\vdash X \subseteq Y} \quad \text{(Z fresh)}
\]

• **Case of** \(N(X)\). We have
\[
N(X)^_0 = \exists x \left( N(x) \land x \subseteq X \land \forall y \left[ N(y) \rightarrow y \subseteq X \rightarrow y \equiv X \right] \right)
\]

Assume \(N(X)\). We obviously have \(N(X) \land X \subseteq X\). Moreover, given \(N(Y)\) such that \(Y \subseteq X\), we apply the axiom
\[
\frac{N(X), Y \subseteq X \vdash E(Y), Y \equiv X}{\vdash \top}
\]
and we get \(Y \equiv X\) thanks to the axiom
\[
E(Y), N(Y) \vdash \top
\]

Conversely, assume \(N(X)^_0\), and let \(x\) such that \(N(x)\), \(x \subseteq X\) and
\[
\forall y \left[ N(y) \rightarrow y \subseteq X \rightarrow y \equiv X \right]
\]

In order to show \(N(X)\), we apply the axioms
\[
\frac{Z \subseteq X \vdash E(Z), Z \equiv X}{\vdash N(X), E(X)} \quad \text{and} \quad \frac{N(X), E(X) \vdash \top}{\text{N(X), E(X) \vdash}}
\]
First, note that \(X \subseteq Y\) and \(E(Y)\) imply \(E(X)\), so we have \(\neg E(X)\) since \(x \subseteq X\) with \(N(x)\). Hence we are done if we show
\[
\forall Z \left( Z \subseteq X \rightarrow E(Z) \lor Z \equiv X \right)
\]
So let \(Z \subseteq X\) such that \(\neg E(Z)\). For all \(Y \subseteq Z\) such that \(N(Y)\), we have \(Y \subseteq X\) so that \(Y \equiv X\) and thus \(Y \subseteq X\). It follows that \(Z \subseteq x\). But this implies \(N(Z)\) since \(\neg E(Z)\) and \(N(x)\), and we obtain \(Z \equiv x\) from \(Z \subseteq x\).

Now, given \(N(Y)\) such that \(Y \subseteq X\), we have \(Y \equiv Z\) and thus \(Y \subseteq Z\). Hence \(X \subseteq Z\), and are done since we assumed \(Z \subseteq X\).

• **Case of** \(0(X)\). We have
\[
0(X)^_0 = \left( N(X)^_0 \land \forall x \right) \left( N(x) \rightarrow [x \subseteq X \rightarrow 0(x)] \right)
\]

Assume first \(0(X)\). We have \(N(X)\) and thus \(N(X)^_0\). Let now \(N(x)\) such that \(x \subseteq X\). Since \(N(X)\) and \(N(x)\) we get \(x \equiv X\), so \(0(x)\).

Conversely, assume \(0(X)^_0\). We thus get \(N(X)^_0\) and thus \(N(X)\). So there is some \(x \subseteq X\) with \(N(x)\). But we must have \(x \equiv X\) and this implies \(0(X)\) since \(0(x)\).
• Case of $S(X, Y)$. We have

$$S(X, Y) \overset{\circ}{=} N(X) \wedge N(Y) \wedge \forall x, y \,(N(x) \rightarrow N(y) \rightarrow S(x, y) \rightarrow x \subseteq X \rightarrow y \subseteq Y)$$

Assume $S(X, Y)$. We have $N(X)$ and $N(Y)$, so that $N(X) \overset{\circ}{=} \wedge N(Y) \overset{\circ}{=} \wedge \forall x, y \,(N(x) \rightarrow N(y) \rightarrow x \subseteq X \rightarrow y \subseteq Y \rightarrow x \subseteq y)$.

Conversely, assuming $S(X, Y)$, we obtain $N(X)$ and $N(Y)$. It follows that given $N(x)$ with $x \subseteq X$ we have $x \subseteq X$ (and such an $x$ exists by $N(X) \overset{\circ}{=} \wedge \forall x, y \,(N(x) \rightarrow N(y) \rightarrow x \subseteq X \rightarrow y \subseteq Y)$. But then, there is some $y$ such that $S(X, y)$, and thus $N(y)$. This implies $y \subseteq Y$ and thus $y \subseteq Y$ and we are done.

• Case of $(X \subseteq Y)$. We have

$$(X \subseteq Y) \overset{\circ}{=} N(X) \wedge N(Y) \wedge \forall x, y \,(N(x) \rightarrow N(y) \rightarrow x \subseteq X \rightarrow y \subseteq Y \rightarrow x \subseteq y)$$

Assume $(X \subseteq Y)$. We have $N(X)$ and $N(Y)$, so that $N(X) \overset{\circ}{=} \wedge N(Y) \overset{\circ}{=} \wedge \forall x, y \,(N(x) \rightarrow N(y) \rightarrow x \subseteq X \rightarrow y \subseteq Y, so that $x \subseteq y$.

Conversely, assuming $X \subseteq Y$, since $N(X) \overset{\circ}{=} \wedge N(Y) \overset{\circ}{=} \wedge \forall x, y \,(N(x) \rightarrow N(y) \rightarrow x \subseteq X \rightarrow y \subseteq Y$. It follows that $x \subseteq X$, $y \subseteq Y$ and $x \subseteq y$, so that $X \subseteq Y$.

□

Lemma A.7. Given a closed MSO'-formula $\Phi$ in the sense of [22], we have

$$\text{MSO}' \vdash \Phi \quad \Rightarrow \quad \text{MSO} \vdash \Phi_0$$

Proof. The proof is by induction on derivations. Given formulae $\Phi_1, \ldots, \Phi_n, \Phi$ with free individual variables among $\overline{x} = x_1, \ldots, x_p$, we show that if

$$\Phi_1, \ldots, \Phi_n \vdash_{\text{MSO}'} \Phi$$

is derivable in the system of [22], then

$$\overline{N(x)}, \Phi_1, \ldots, \Phi_n \vdash_{\text{MSO}} \Phi_0 \quad (3)$$

We distinguish the different cases of $\Phi_1, \ldots, \Phi_n \vdash_{\text{MSO}'} \Phi$.

• We first discuss the Arithmetic Rules of MSO', given in [22, Fig 3]. They all directly follow from the corresponding rules of Fig. 2, but for the rules

$$\overline{\Phi} \vdash \exists y.0(y) \quad \text{and} \quad \overline{\Phi} \vdash \exists y.S(x, y)$$

For these rules, one uses the axioms

$$0(x) \vdash N(x) \quad \text{and} \quad S(x, y) \vdash N(y)$$

in addition to the derivable rules

$$\vdash \exists y.0(Y) \quad \text{and} \quad \vdash \exists y.S(x, Y)$$

• The induction rule of [22] directly follows from the induction rule of MSO given in §2.

• As for comprehension, the comprehension rule of [22] is expressed as a right $\exists$ rule:

$$\Phi_1, \ldots, \Phi_n \vdash \Phi[\Psi[x]/X]$$

which is translated to

$$\Phi_1, \ldots, \Phi_n \vdash (\overline{\Phi[\Psi[x]/X]}_0$$

The translation $(\cdot)_0$ is compatible with second-order substitution in the sense that

$$\text{MSO} \vdash \Phi_0[\Psi_0[y]/X] \leftrightarrow (\Phi[\Psi[y]/X])_0$$

where the substitution $\Phi_0[\Psi_0[y]/X]$ is defined by induction as usual but with

$$(x \in X) \circ [\Psi_0[y]/X] \quad := \quad \Psi[y/x]$$

The result then follows as usual (using the substitution lemma) from the comprehension scheme of MSO given in §2.

• Finally, the logical rules are straightforward, but for the right $\exists$ rules on individuals, which uses the supplementary assumptions $\overline{N(x)}$ in (3).

□
B Proofs of §3 (LMSO: A Linear Variant of MSO)

B.1 Proofs of §3.2 (The Deduction System of LMSO)

Theorem B.1 (Thm. 3.2). Given an MSO\(^+\) formula \(\varphi\), if MSO\(^+\) \(\vdash \varphi\) then LMSO \(\vdash \varphi^L\).

Proof. We show by induction on derivations that

\[ \varphi \vdash_{\text{MSO}^+} \varphi' \quad \Rightarrow \quad \varphi^L \vdash_{\text{LMSO}} \varphi'^L \]

In most cases, for each MSO\(^+\)-rule of the shape

\[ \frac{(\gamma_i \vdash \varphi_i)_{i \in I}}{\varphi \vdash} \]

there is an LMSO-rule of the shape

\[ \frac{(\varphi_i^L \vdash \gamma_i^L)_{i \in I}}{\varphi^L \vdash \varphi'^L} \]

which enables to conclude swiftly. We distinguish the different cases of \(\varphi \vdash_{\text{MSO}^+} \varphi'\).

- Arithmetic Rules of Fig. 2. Since \(\alpha^L = \alpha\) for each \(\alpha \in \text{At}\), these rules fall in the scheme described above.
- Among the non-logical rules of Fig. 5, the cases of

\[
\begin{align*}
\varphi, \varphi, \varphi & \vdash \gamma, \gamma, \gamma \\
\varphi, \psi, \psi, \psi & \vdash \gamma, \psi, \gamma, \psi \\
\varphi, \psi, \psi, \psi & \vdash \gamma, \psi, \psi, \gamma \\
\psi, \varphi, \varphi & \vdash \psi, \gamma, \gamma, \gamma \\
\psi, \varphi, \varphi & \vdash \psi, \gamma, \gamma, \gamma \\
\psi, \varphi, \varphi & \vdash \psi, \gamma, \gamma, \gamma \\
\psi, \varphi, \varphi & \vdash \psi, \gamma, \gamma, \gamma \\
\psi, \varphi, \varphi & \vdash \psi, \gamma, \gamma, \gamma
\end{align*}
\]

follow from the corresponding rule in LMSO.

The cases of the rules

\[ \frac{\varphi, \varphi \vdash \varphi}{\varphi^L, \varphi^L \vdash \varphi^L} \quad \text{and} \quad \frac{\varphi \vdash}{\varphi^L \vdash \varphi^L} \]

follow, since \(\varphi^L\) is deterministic, using the LMSO-rules

\[ \frac{\varphi^L, \varphi^L \vdash \varphi^L}{\varphi, \varphi \vdash \varphi^L} \quad \text{and} \quad \frac{\varphi \vdash}{\varphi^L \vdash \varphi^L} \]

- Consider now the logical rules of MSO\(^+\). First, since \(\varphi^L\) is a formula of LMSO, the case of double negation elimination

\[ (\varphi \rightarrow \bot) \rightarrow \bot \vdash \varphi \]

follows from the Polarized Double Negation Elimination axioms of LMSO.

All the other logical rules for propositional logic follow from the corresponding rules of LMSO, replacing \(\land\) by \(\otimes\), \(\lor\) by \(\oplus\) and \(\rightarrow\) by \(\rightarrow\).

It remains to deal with the quantifier rules in which exponential intervene. We use the fact that all formulae \(\varphi^L\) are deterministic, hence, we may introduce and suppress exponentials as needed.

- Suppose that the last rule was a \(\exists\)-left (resp. \(\forall\)-right) rule:

\[ \frac{\varphi, \varphi \vdash \varphi}{\varphi \vdash \exists Z \varphi} \quad \text{resp.} \quad \frac{\varphi \vdash}{\varphi \vdash \forall Z \varphi} \]

By the induction hypothesis and the \(\exists\)-left (resp. \(\forall\)-right) rule of LMSO, we can also derive

\[ \varphi^L, \exists Z \varphi^L \vdash \varphi^L \quad \text{resp.} \quad \varphi^L \vdash \forall Z \varphi^L \]

But \(\varphi^L\) and \(\varphi'^L\) are all deterministic, so we deduce

\[ \varphi^L, \exists Z \varphi^L \vdash \varphi'^L \quad \text{resp.} \quad \varphi^L \vdash \forall Z \varphi^L \]

and we are done since \((\exists Z \varphi)^L = ?\exists Z \varphi^L\) (resp. \((\forall Z \varphi)^L = \forall Z \varphi^L\)).

- Suppose that the last rule was an \(\exists\)-right (resp. \(\forall\)-left) rule

\[ \frac{\varphi \vdash \varphi[t/Z, \varphi^L]}{\varphi \vdash \exists Z \varphi, \varphi^L} \quad \text{resp.} \quad \frac{\varphi, \varphi^L[t/Z]}{\varphi \vdash \forall Z \varphi, \varphi^L} \]

By induction hypothesis (and since \((-)^L\) commutes with substitution) we get

\[ \varphi^L \vdash \varphi^L[t/Z, \varphi^L] \quad \text{resp.} \quad \varphi^L \vdash \varphi^L[t/Z]^L \]

We can now use the \(\exists\)-right (resp. \(\forall\)-left) rule of LMSO, followed with the \?-right (resp. \!-left) rule to derive

\[ \varphi^L \vdash ?\exists Z \varphi^L, \varphi^L \quad \text{resp.} \quad \varphi^L \vdash \forall X \varphi^L \]

But then we are done since \(?\exists Z \varphi^L = (\exists Z \varphi)^L\) (resp. \(?\forall Z \varphi^L = (\forall Z \varphi)^L\)).

- We finally discuss the remaining axioms schemes of MSO\(^+\).
− **Induction.** The induction scheme of LMSO requires one hypothesis to be under an exponential modality $!(-)$ to accommodate arbitrary negative formulae; the situation is resolved by cutting with the LMSO axiom enabling to remove exponentials over deterministic formulae.

By the induction hypothesis (and since $(-)^L$ commutes over substitution), we have proofs

$$\frac{\pi}{\varphi^L, 0(z) \vdash \varphi^L[z/x], \overline{\psi}} \quad \text{and} \quad \frac{\pi'}{S(y, z), \varphi^L[y/x] \vdash \varphi^L[z/x], \overline{\psi'}}$$

Noticing that all involved formulae above are deterministic, we may give the following derivation in LMSO:

$$\frac{\pi}{\varphi^L, S(y, z), \varphi^L[y/x] \vdash \varphi^L[z/x], \overline{\psi'}}$$

$$\frac{\pi'}{S(y, z), !\varphi^L[y/x] \vdash \varphi^L[z/x], \overline{\psi'}}$$

− **Comprehension.** The translation of an instance of the Comprehension scheme of MSO$^+$ is an instance of the Deterministic Comprehension scheme of LMSO.

− **Definition of Mealy Machines.** The axiom scheme defining terms in MSO$^+$ is as follows

$$\vdash \forall X \forall x (x \in t_M(X) \iff \delta_M(x, X))$$

Clearly, it is equivalent to the following scheme where we make the universal quantification implicit by using formulae with free variables

$$\vdash N(x) \rightarrow (x \in t_M(X) \iff \delta_M(x, X))$$

which translate to the following, which is then clearly derivable from the corresponding scheme in LMSO by instantiating the universal quantifiers by the free variables

$$\vdash N(x) \rightarrow (x \in t_M(X) \iff \delta_M(x, X)^L)$$

\[ \square \]

**Corollary B.2** (Cor. 3.3). *If an MSO$^+$-formula $\varphi(Y; Z)$ admits a (f.s.) causal realizer, then LMSO $\vdash \forall Y. \exists Z. \varphi^L(Y; Z)$.

**Proof.** Assume that $\varphi(Y; Z)$ is realized by f.s. causal functions $\Phi$ of Mealy machines $\mathcal{M}$. Then

$$\mathcal{M} \models \forall Y. \varphi(Y; t_M(Y))$$

It follows from the completeness of MSO$^+$ (Thm. A.1) that we have

$$\text{MSO}^+ \vdash \forall Y. \varphi(Y; t_M(Y))$$

from which we deduce by correctness of $(-)^L$ (Thm. B.1) that

$$\text{LMSO} \vdash \forall Y. \varphi^L(Y; t_M(Y))$$

But this implies

$$\text{LMSO} \vdash \varphi^L(Y; t_M(Y))$$

and we easily deduce the result. \[ \square \]

**C  Proofs of §5 (The Realizability Model of LMSO)**

**C.1  Proofs of §5.1 (The Realizability Interpretation of LMSO)**

**Proposition C.1** (Prop. 5.2). *Given a positive (resp. negative) automaton $A : \Sigma$, there is a deterministic automaton $\tilde{A} : \Sigma$ (resp. $\tilde{A} : \Sigma$) which recognises the same language as $A$.*

**Proof.** We first discuss the case of a positive $A : \Sigma$. Consider the (usual) deterministic automaton $\mathcal{S}$ over $\Sigma \times A_0$ with the same states as $A$ and with transition function $\delta_S$ defined as $\delta_S(q, (a, a^p, \omega)) := \tilde{\delta}_A(q, a, a^p, \omega)$ (where $\omega$ is the unique element of $A_0 \simeq \{\omega\}$). Then $B \in \mathcal{L}(\mathcal{A})$ iff there is some $R \in A_0^\omega$ s.t. $(B, R) \in \mathcal{L}(\mathcal{A})$. Since $\Omega_A$ is $\omega$-regular, it is recognized by a non-det. Büchi automaton $\mathcal{C}$ over $\Sigma_A$. We then obtain a non-det. Büchi automaton $\mathcal{B}$ over $\Sigma \times U$ with state set $Q_A \times Q_C$ and s.t. $\mathcal{L}(\mathcal{B}) = \mathcal{L}(\mathcal{S})$. It follows that $B \in \mathcal{L}(\mathcal{A})$ iff $B \in \mathcal{L}(\exists_U \mathcal{B})$, where $\exists_U \mathcal{B}$ is the usual projection of $\mathcal{B}$ on $\Sigma$. By McNaughton’s Thm. 2.10, $\exists_U \mathcal{B}$ is equivalent to a deterministic (say Muller) automaton $\mathcal{D}$ over $\Sigma$. We let $\tilde{A}$ be $\mathcal{D}$ seen as a uniform automaton. For a negative $A$, we let $\tilde{A} := (\tilde{\tilde{A}})^*$ (where $(-)^*$ is defined in §4.5). \[ \square \]
C.2 Proofs of §5.2 (Correctness of PLMSO w.r.t. $\vdash$

Proposition C.2 (Prop. 5.6). Given PLMSO-formulae $\varphi^+$ and $\psi^-$, then $[\varphi^+] \mapsto [\psi^-]$ is realized iff $\mathcal{R} |\vdash [\varphi^+] \rightarrow [\psi^-]$.

Proof. The left-to-right direction directly follows from Prop. 4.16.

The proof of the right-to-left direction combines [25, Prop. 7.7] with Corollary 4.22. We give here a detailed argument, since it is representative of how the structures of the categories $\mathcal{A}ut^\circ(-)$ can be used in realizability. So assume $\mathcal{R} |\vdash [\varphi^+] \rightarrow [\psi^-]$, and assume the free variables of $\varphi^+, \psi^-$ are among $X = X_1, \ldots, X_n$. By Prop. 5.5 we have $\mathcal{L}([\varphi^+]) \subseteq \mathcal{L}([\varphi^-])$, and by Corollary 4.22 we get $\emptyset$. Then it follows from Proposition 4.17 that the language of $[[\varphi^+]] \times [[\varphi^-]]$ is empty. Since $[[\varphi^+]] \times [[\varphi^-]]$ is a positive automaton, by Proposition 4.21 it follows that the automaton $2^n(\times [\varphi^+]) : I_2^n$ has also an empty language. But by Proposition 4.17 this implies that $2^n(\times [\varphi^+] \rightarrow [\varphi^-]) \mapsto \perp$ (where $\perp$ lives in $\mathcal{A}ut_1$) accepts the only $\omega$-word (say $\bullet\cdot$) on $1$. This means that there is a DA$_1$-map

$$\mathcal{T} \longrightarrow \bigl(2^n(\times [\varphi^+] \rightarrow [\varphi^-]) \mapsto \perp\bigr)(\bullet\cdot)$$

Since $2^n(\times [\varphi^+] \rightarrow [\varphi^-]) \mapsto \perp$ and $2^n(\times [\varphi^+] \rightarrow [\varphi^-]) \mapsto \perp$ are isomorphic as DA$_1$-objects, Proposition 4.17 gives a DA$_1$-map

$$2^n(\times [\varphi^+] \rightarrow [\varphi^-]) \longrightarrow \perp$$

Now apply Proposition 4.20 to obtain a DA$_2$-map

$$[\varphi^+] \times [\varphi^-] \longrightarrow \perp(I_2^n)$$

where $I_2^n$ is the unique $S$-map $2^n \rightarrow I$. Note that the $\perp$ in $\mathcal{A}ut_{i2^n}$ is isomorphic in $\mathcal{A}ut_{2^n}$ to $\perp(I_2^n) : 2^n$, so that we actually have a DA$_2$-map

$$[\varphi^+] \times [\varphi^-] \longrightarrow \perp$$

where $\perp$ lives in $\mathcal{A}ut_{2^n}$. By applying again Proposition 4.17 we get a realizer of

$$[\varphi^+] \longrightarrow ([\varphi^-]) \mapsto \perp$$

and we can conclude using, the esos $(A \rightarrow \perp) \simeq A^\perp$ and $(A^\perp) \simeq A$ of §4.5.

C.3 Proofs of §5.3 (Adequacy and Realized Axioms)

Theorem C.3 (Thm. 5.7). Given LMSO-formulae $\varphi = \varphi_1, \ldots, \varphi_n$ and $\psi = \psi_1, \ldots, \psi_m$, from a derivation of $\varphi \vdash_{\text{LMSO}} \psi$, one can extract a f.s. realizer of $[\varphi_1] \circ \ldots \circ [\varphi_n] \mapsto [\psi_1] \circ \ldots \circ [\psi_m]$.

Proof. The proof of Thm. 5.7 is as usual by induction on derivations. It is convenient to decompose it as follows.

- The rules of the first line of Fig. 4, follow from the symmetric monoidal structures of $(\mathcal{A}ut_{2^n}, \delta, \perp)$ and $(\mathcal{A}ut_{2^n}, \otimes, \top)$.
- The weakening rules as well as a the $\perp$-left and $\top$-right rules follow from the weakening maps of $\mathcal{D}Z^W$.
- The contraction rules follow from the fact that $(\otimes, \top)$ (resp. $(\delta, \perp)$) gives products (resp. co-products) of positive (resp. negative) automata.
- The $\otimes$-left rule and the $\delta$-right rule are trivial. The two other rules for $\otimes$ and $\delta$ are based on the monoidal structure $(\otimes, I)$ of $\mathcal{D}Z$, together with some tautological reasoning on winning.
- The $\top$-left rule follows from the monoidal closed structure of $(\otimes, \top, \rightarrow)$ in $\mathcal{A}ut_{\rightarrow}$. The $\rightarrow$-left rule in addition uses realizers of

$$\begin{align*}
(A \otimes B) &\longrightarrow (A \delta B) \\
(A \delta B) \circ C &\longrightarrow (A \otimes C) \delta B
\end{align*}$$

which are themselves provided by adequacy for the $\otimes$ and $\delta$ rules.
- The quantifier rules rely on Prop. 4.20, together with the monoidal closure of of $(\otimes, \top, \rightarrow)$ in $\mathcal{A}ut_{\rightarrow}$.
- The $!$-left and $?$-right rules follow from the existence of trivial realizers for

$$!(A^!) \longrightarrow A^! \quad \text{and} \quad A^+ \longrightarrow (?A^+)$$

given by combining Prop. C.1 with Prop. C.2. The other rules for $!(\cdot)$ and $?(\cdot)$ directly follow from Prop. C.1 and Prop. C.2.
- For the most part, the arithmetic rules of Fig. 2 only comprise deterministic formulae. Since those are sound for MSO$^+$, by Prop. C.2, they are realized. As those making general formulae intervene, notice that they have a single premise, whose set of $P$ and $O$ moves are isomorphic to the conclusion. It is fairly straightforward to check that realizers of the premise are also realizers of the conclusion.
- The adequacy for the axioms schemes of Deterministic Comprehension, Definitions of Mealy Machines and Induction directly follows from Prop. C.2.
We consider the case of Polarized Double-Negation Elimination. Assume that $A$ is positive (resp. negative) so that $A_0 \simeq \{\bullet\}$ (resp. $A_0 \simeq \{\bullet\}$). In this case, we have

$$( (A \to \bot)_p \simeq \{\bullet\} \text{ and } (A \to \bot)_0 \simeq A_0 \text{ resp. } ((A \to \bot)_p \simeq A_0 \text{ and } (A \to \bot)_0 \simeq \{\bullet\} )$$

so that

$$((A \to \bot)_0 \to \bot)_p \simeq A_0 \text{ and } ((A \to \bot)_0 \to \bot)_0 \simeq \{\bullet\} \text{ and } ((A \to \bot)_0 \to \bot)_0 \simeq A_0$$

resp. $$((A \to \bot)_0 \to \bot)_p \simeq \{\bullet\} \text{ and } ((A \to \bot)_0 \to \bot)_0 \simeq A_0$$

The result then follows from the definitions of transition functions and acceptance conditions for $\bot$ and $\to$.

\[\square\]

At this juncture, we show the adequacy of the additional principles realized in the model exhibited in §5. For clarity’s sake, we reframe the examples using arbitrary alphabets and working directly with automata corresponding to the formulae in play. When $A : \Sigma$ is an automaton and $f : \Gamma \to \Sigma$ is an ordinary function on alphabets, we use the notation $A[f]$ for the automaton over $\Gamma$ with all components equal to those of $A$, except for its transition function $\vartheta_A[f]$, which is defined as

$$\vartheta_A[f](q, b, a^p, a^0) := \vartheta_A(q, f(b), a^p, a^0)$$

In most case, the map $f$ is a projection $\pi_\Sigma : \Sigma_1 \times \cdots \times \Sigma_n \to \Sigma_i$ corresponding to restriction or renaming variables in the various principles.

**Proposition C.4** (Ex. 5.9). For negative $A : \Sigma$ and $B : \Sigma \times \Gamma$, there is an $\Aut_{\Sigma}$-isomorphism between $A \to \exists_B$ and $\exists_{\Gamma}(A[\pi_\Sigma] \to B)$. Similarly, if $A : \Sigma \times \Gamma$ and $B : \Sigma$ are deterministic, there is an $\Aut_{\Sigma}$-isomorphism between $(\forall_{\Gamma} A) \to B$ and $\exists_{\Gamma}(A \to B[\pi_\Sigma])$.

**Proof.** Let $A : \Sigma$ and $B : \Sigma \times \Gamma$ be negative, i.e. such that $A_0 \simeq B_0 \simeq \{\bullet\}$. Up to isomorphisms of the moves, both $A \to \exists_B$ and $\exists_{\Gamma}(A[\pi_\Sigma] \to B)$ have structure $$(\Gamma \times A[\pi_\Sigma], B_0, Q_A \times Q_B, (q_A, q_B), \vartheta, \Omega_{A \to B})$$

where

$$\vartheta'((q_A, q_B), a, (b, f), x) = (\vartheta_A((q_A, a), f(x)), \vartheta_B(q_B, (a, b), \bullet, x))$$

Consider now deterministic $A : \Sigma \times \Gamma$ and $B : \Sigma$. Computing $((\forall_{\Gamma} A) \to B$ and $\exists_{\Gamma}(A \to B[\pi_\Sigma])$ yields, up to isomorphisms of moves

$$(\forall_{\Gamma} A, \bullet, Q_A \times Q_B, (q_A, q_B), \vartheta', \Omega_{A \to B})$$

where

$$\vartheta'((q_A, q_B), a, (b, \bullet)) = (\vartheta_A((q_A, a), b, \bullet), \vartheta_B(q_B, a, \bullet, \bullet))$$

\[\square\]

**Proposition C.5** (Ex. 5.10). For any negative $A : \Theta \times \Gamma \times \Sigma$, there is an $\Aut_{\Theta}$-isomorphism between $$(\forall_{\Gamma} \exists_{\Sigma} A)$$ and $\exists_{\Theta \times \Gamma \times \Sigma} A[(\pi_{\Theta}, app \circ \pi_{\Gamma \times \Sigma}, \pi_{\Sigma})]$.

**Proof.** Let $A : \Theta \times \Gamma \times \Sigma$ be the negative automaton under consideration. Notice that, up to isomorphisms of moves, $$(\forall_{\Gamma} \exists_{\Sigma} A) : \Theta$$ is the structure

$$(\Gamma^\Theta, A_0 \times \Sigma, Q_A, q^0_A, \vartheta, \Omega_A)$$

where $\vartheta(q, (d, f, (a^0, a))) = \vartheta_A((q, (d, f(d), a), (a^0, a)))$.

On the other hand (still up to isomorphisms of moves), $A[(\pi_{\Theta}, app \circ \pi_{\Gamma \times \Sigma}, \pi_{\Sigma})] : \Theta \times \Gamma^\Sigma \times \Sigma$ is the structure

$$(\Gamma^\Theta, A_0 \times \Sigma, Q_A, q^0_A, \delta, \Omega_A)$$

where $\delta(q, (d, f, a), a^0) = \delta_A((q, (d, f(a), a), a^0))$.

It follows that up to isomorphisms of moves, $A[(\pi_{\Theta}, app \circ \pi_{\Gamma \times \Sigma}, \pi_{\Sigma})] : \Theta$ is the structure

$$(\Gamma^\Theta, A_0 \times \Sigma, Q_A, q^0_A, \delta'', \Omega_A)$$

where

$$\delta''(q, (d, f, (a^0, a))) = \delta'(q, (d, f, (a^0, a))) = \delta_A((q, (d, f(a), a), a^0)) = \vartheta(q, (d, f, (a^0, a)))$$

\[\square\]

**Proposition C.6** (Ex. 5.11). For arbitrary $A$ in $\Aut_{\Sigma}$, there exists a map

$$(A \to \bot) \to \bot$$

which is a retract of the canonical map $A \to ((A \to \bot) \to \bot)$.
Note that in general, there can not be an isomorphism between $\mathcal{A}$ and $(\mathcal{A} \rightarrow \bot) \rightarrow \bot$, simply because of the cardinality mismatch between the Proponent moves in the respective components whenever $\mathcal{A}$ is not polarized.

Proof. Let $\mathcal{A} = (P, O, Q_\mathcal{A}, q'_\mathcal{A}, \Omega_\mathcal{A})$ be a uniform automaton over $\Sigma$.

We have, up to isomorphisms of moves and states,

$$[(\mathcal{A} \rightarrow \bot) \rightarrow \bot] = (P^{O^P}, O^P, Q_\mathcal{A}, q'_\mathcal{A}, \Omega_\mathcal{A})$$

In the zigzag game $[(\mathcal{A} \rightarrow \bot) \rightarrow \bot] \rightarrow \mathcal{D}_{\mathcal{Z}[\Sigma]} \mathcal{A}$, a round plays out as follows:

- Opponent first plays some letter $a \in \Sigma$ and a move $F \in P^{O^P}$,
- Proponent then plays a move $p \in P$,
- Opponent answers with $o \in O$,
- Proponent closes the round with $f \in O^P$.

Recall that Proponent wins if and only if, whenever the sequence of states generated by $(a_n, F_n(f_n), f_n(F_n(f_n)))_{n \in \omega}$ is in $\Omega_\mathcal{A}$, so is the sequence generated by $(a_n, p_n, o_n)_{n \in \omega}$. For Proponent to have a winning strategy, it is sufficient that it may be able to enforce the following correspondence between the runs of $(\mathcal{A} \rightarrow \bot) \rightarrow \bot$ and $\mathcal{A}$

$$F_n(f_n) = p_n \text{ and } f_n(F_n(f_n)) = o_n$$

for every $n \in \mathbb{N}$.

Proponent may force this behaviour thanks to the following.

**Lemma C.7.** Let $P$ and $O$ be sets such that $O$ may be well-ordered. Then the following is true

$$\forall F \in P^{O^P}. \exists p \in P. \forall o \in O. \exists f \in O^P. [F(f) = p \text{ and } f(p) = o]$$

**Proof of the Lemma.** Fix $F \in P^{O^P}$. The negation of our statement is equivalent to

$$\forall p \in P. \exists o \in O. \neg \left( \exists f \in O^P. [F(f) = p \land f(p) = o] \right)$$

Using an instance of choice available thanks to the fact that $O$ may be well-ordered, this is in turn equivalent to

$$\exists \tilde{o} \in O^P. \forall p \in P. \neg \left( \exists f \in O^P. [F(f) = p \land f(p) = \tilde{o}(p)] \right)$$

It follows that we only need to prove

$$\forall F \in P^{O^P}. \forall \tilde{o} \in O^P. \exists p \in P. \exists f \in O^P. [F(f) = p \text{ and } f(p) = \tilde{o}(p)]$$

But this is now easy: given $F \in P^{O^P}$ and $\tilde{o} \in O^P$, we can take $f := \tilde{o}$ and $p := F(\tilde{o})$ to conclude. \hfill \Box

We now return to the proof of Prop. C.6. Since $O$ is always finite in our case, we can use the Lemma to show that Proponent has some memoryless winning strategy in $[(\mathcal{A} \rightarrow \bot) \rightarrow \bot] \rightarrow \mathcal{A}$.

Furthermore, as the canonical Proponent strategy in the game $\mathcal{A} \rightarrow (\mathcal{A} \rightarrow \bot) \rightarrow \bot$ takes a Proponent move $p \in P$ to the constant proponent move $\tilde{p} \in P^{O^P}$ (i.e. $\forall F \in O^P. \tilde{p}(F) = p$), and, as the strategy we exhibited enforce the aforementioned correspondence between runs of $(\mathcal{A} \rightarrow \bot) \rightarrow \bot$ and $\mathcal{A}$, we do have the announced retraction. \hfill \Box
Contents

Abstract 1
1 Introduction 1
Organization of the paper. 2
2 Church’s Synthesis and MSO⁺ 2
Notations. 2
Specifications. 2
Causal Functions and Mealy Machines. 2
The Logic MSO⁺. 2
Büchi Automata. 3
Church’s Synthesis. 3
Curry-Howard Approaches. 3
Linear Variants of SMSO. 4
3 LMSO: A Linear Variant of MSO 5
3.1 The Language of LMSO 5
3.2 The Deduction System of LMSO 5
4 Games and Automata 6
4.1 Simple Zig-Zag Games 6
Monoids and Comonoids. 6
Comonoid Indexing. 6
4.2 Games with Winning 7
4.3 Uniform Automata 7
4.4 Some Structure on Automata 8
Substitution. 8
Monoidal-Closed Structure. 8
Multiplicative Disjunction. 8
Quantifications. 8
4.5 Polarities and Duality 9
5 The Realizability Model of LMSO 9
5.1 The Realizability Interpretation of LMSO 9
Interpretation of PLMSO-Formulae. 9
5.2 Correctness of PLMSO w.r.t. N 9
5.3 Adequacy and Realized Axioms 9
6 Conclusion 10
Further Works. 10
Acknowledgments 10
References 11
A Proofs of §2 (Church’s Synthesis and MSO⁺) 11
B Proofs of §3 (LMSO: A Linear Variant of MSO) 15
B.1 Proofs of §3.2 (The Deduction System of LMSO) 15
C Proofs of §5 (The Realizability Model of LMSO) 16
C.1 Proofs of §5.1 (The Realizability Interpretation of LMSO) 16
C.2 Proofs of §5.2 (Correctness of PLMSO w.r.t. N) 17
C.3 Proofs of §5.3 (Adequacy and Realized Axioms) 17
Contents 20