Non-deterministic Phase Semantics and the Undecidability of Boolean BI

DOMINIQUE LARCHEY-WENDLING, LORIA – CNRS
DIDIER GALMICHE, LORIA – University Henri Poincaré

We solve the open problem of the decidability of Boolean BI logic (BBI), which can be considered as the "core" of Separation and Spatial Logics. For this, we define a complete phase semantics suitable for BBI and characterize it as trivial phase semantics. We deduce an embedding between trivial phase semantics for intuitionistic linear logic (ILL) and Kripke semantics for BBI. We single out the elementary fragment of ILL which is both undecidable and complete for trivial phase semantics. Thus, we obtain the undecidability of BBI.

Categories and Subject Descriptors: F.4.1 [**Mathematical Logic and Formal Languages**]: Mathematical Logic—*Proof theory*; *Model Theory*; *Computability theory*

General Terms: Theory

Additional Key Words and Phrases: Linear logic, Boolean BI, Minsky machines encoding, Decidability

ACM Reference Format:
Larchey-Wendling, D., and Galmiche, D. 2011. Non-deterministic Phase Semantics and the Undecidability of Boolean BI. ACM Trans. Comput. Logic 1, 1, Article 1 (June 2011), 36 pages.
DOI = 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

1. INTRODUCTION

The question of the decidability of Boolean BI, the Boolean version of the logic of Bunched Implications, was a longstanding open problem. BI itself was proved decidable in [Galmiche et al. 2005] and Boolean BI was naively thought "simpler" than BI until a faithful embedding from BI into Boolean BI was discovered [Larchey-Wendling and Galmiche 2009]. Independently, Brotherston and Kanovich [Brotherston and Kanovich 2010] on the one hand, and Larchey-Wendling and Galmiche [Larchey-Wendling and Galmiche 2010] on the other hand, have recently solved the issue by different techniques: the former by focusing mainly on the relations between Boolean BI and Separation Logic [Ishtiaq and O'Hearn 2001], the latter by establishing semantic links between Intuitionistic Linear Logic (ILL) and Boolean BI. This paper is an enriched and self-contained version of the results and proofs of [Larchey-Wendling and Galmiche 2010].

The logic BI of Bunched Implications [O'Hearn and Pym 1999] is a sub-structural logic which freely combines additive connectives $\wedge$, $\vee$, $\rightarrow$ and multiplicative connectives $*$, $-\!*$. In BI, both the multiplicatives and the additives behave intuitionistically. From its inception, BI was given a nice bunched sequent proof-system enjoying cut-elimination [Pym 2002]. Later, [Galmiche et al. 2005] gave BI a sound and complete labeled tableaux system from which decidability was derived. The logic BI is sometimes called intuitionistic BI to distinguish it from other variants where either the multiplicatives or the additives include a negation and thus behave classically.

From a proof-theoretical perspective, Boolean BI (or simply BBI) can be considered to be the first investigated variant of BI which contained a negation: BBI combines intuitionistic multiplicatives

This work was supported by the ANR grant DynRes (project no. ANR-11-BS02-011), by the CNRS and the University Henri Poincaré of Nancy.
Author's addresses: Dominique Larchey-Wendling and Didier Galmiche, Bâtiment LORIA, BP 239, 54506 Vandoeuvre-lès-Nancy, France.

DOI 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

with Boolean additives. This focus on BBI is the consequence of the natural links between BBI and separation or spatial logics: for instance, the assertion language of separation logic is a theory of BBI that uses a particular model based on a partial monoid of heaps [Ishtiaq and O'Hearn 2001] or more generally a separation algebra in the case of Abstract Separation Logic [Calcagno et al. 2007]; see also [Larchey-Wendling and Galmiche 2009] for a general discussion on these links. The Hilbert proof-system of BBI was proved complete w.r.t. *relational (or non-deterministic) Kripke semantics* [Galmiche and Larchey-Wendling 2006]. However, the proof-theory of BBI was rather poorly developed because it was difficult to conceive how the bunched sequent calculus of (intuitionistic) BI could be extended to BBI without losing key properties such as e.g. cut-elimination.

Two main families of results emerged giving a contrasted view of its proof-theory. On the one hand, [Brotherston 2010] adapted the Display proof-system of Classical BI to BBI, circumventing the difficulty of the multiplicatives of BBI lacking a negation. This system was proved sound and complete w.r.t. relational Kripke semantics. Cut-elimination was also derived but, despite the expectations of Brotherston, no decidability result followed. On the other hand, [Larchey-Wendling and Galmiche 2009] proposed a labeled tableaux proof-system for (partial monoidal) BBI and by the study of the relations between the proof-search generated counter-models of BI and BBI, showed that (intuitionistic) BI could be faithfully embedded into BBI. This result, at first counter-intuitive, hinted that BBI, originally thought simpler than BI, could in fact be much more difficult to decide.

In this paper, we consider models of BBI belonging to different classes:

- ND. The class of non-deterministic monoids;
- PD. The class of partial (deterministic) monoids;
- TD. The class of total (deterministic) monoids;
- HM. The class of heaps monoids (i.e. separation logic models);
- SA. The class of separation algebras (i.e. abstract separation logic models);
- FM. The class of free monoids;
- FMf. The class of finitely generated free monoids.

Generally, each class of models defines a different notion of (universal Kripke) validity on the formulae of BBI. We denote by $\mathsf{BBI}_{\mathrm{X}}$ the set of formulae which are valid in every monoid of class X. We recall the result that the set $\mathsf{BBI}_{\mathrm{ND}}$ of BBI-formulae valid in every non-deterministic monoid is strictly included in the set $\mathsf{BBI}_{\mathrm{PD}}$ of BBI-formulae valid in every partial deterministic monoid [Larchey-Wendling and Galmiche 2010]. The classification of these classes of models with respect to Kripke validity in BBI is not finished though and we consider it to be a difficult problem.

The principal result of this paper is the *undecidability of universal validity in* $\mathsf{BBI}_{\mathrm{X}}$, whichever class X of models is chosen amongst ND, PD, TD, HM, SA, FM and FMf. This result is the consequence of the following observations:

— usual phase semantics for intuitionistic linear logic (ILL) can be easily generalized to non-deterministic monoids;
— in phase semantics, when we restrict the choice of the closure operator to the identity map, we obtain what we call trivial phase semantics;
— non-deterministic trivial phase semantics is sound but incomplete for ILL. We denote by $\mathsf{ILL}^t_{\mathrm{X}}$ the set of sequents valid in trivial phase semantics restricted to the class X;
— $\mathsf{ILL}^t_{\mathrm{X}}$ appears as (an isomorphic copy of) the fragment of $\mathsf{BBI}_{\mathrm{X}}$ where the Boolean negation has been removed. In other words, we have a faithful embedding $\mathsf{ILL}^t_{\mathrm{X}} \longrightarrow \mathsf{BBI}_{\mathrm{X}}$;
— ILL contains a fragment called the elementary fragment (eILL) which is complete for trivial phase semantics, whichever class X is considered, i.e. the (potentially) different trivial phase semantics for ILL collapse to one on the elementary fragment;
— validity in eILL can be used to encode computations of Minsky machines, which implies the undecidabilty of validity in eILL;
— as eILL is a fragment of $\mathsf{ILL}^t_{\mathrm{X}}$, we obtain the undecidability of $\mathsf{ILL}^t_{\mathrm{X}}$ which is then transfered to $\mathsf{BBI}_{\mathrm{X}}$ by the faithful embedding.

We point out that the elementary fragment eILL is not (isomorphic to) the minimal fragment of Boolean/Classical BI identified in [Brotherston and Kanovich 2010]. We complete the picture with additional results of undecidability on the models based on the free monoid $(\mathbb{N} \times \mathbb{N}, +, (0, 0))$ and the models based on the partial monoid $(\mathbb{P}_f(\mathbb{N}), \uplus, \emptyset)$, i.e. the RAM-domain model [Brotherston and Kanovich 2010] which is the simplest model of separation logic. This last result is obtained using bisimulation techniques and establishes a link between our results and those of [Brotherston and Kanovich 2010].

Compared to the initial conference paper [Larchey-Wendling and Galmiche 2010], this paper contains a more extensive study of the semantics of the eILL fragment with completeness results for various classes of models. We did not consider models of separation logic like those of HM and SA; on the contrary, we focused on the links between BBI and linear logic. Such models of separation logic are now taken into account. We enrich this study according to these two (perhaps a bit conflictual) considerations:

— on the one hand, we think that the faithful embedding of the elementary fragment of ILL into BBI is a key point here. Strictly speaking, the detour through ILL and (trivial) phase semantics is not absolutely necessary and we could have implemented the encoding of Minsky machines directly into BBI and Kripke semantics, exactly as this was later done for Classical BI in [Larchey-Wendling 2010]. But then, the intuition behind the encoding is arguably much more difficult to grasp. We also feel that the existence of the elementary fragment of ILL is important in itself, and in particular, no knowledge of bunched logics is required to understand the encoding of Minsky machines in eILL. This can be especially useful for readers more familiar with linear logic than with bunched logics;
— on the other hand, to position our approach w.r.t. the alternate undecidability result of [Brotherston and Kanovich 2010], we wish that this enriched version includes the models of (propositional) separation logic. We claim that the encoding of [Brotherston and Kanovich 2010] can be understood as a variant of ours with the main difference[1] that they use the RAM-domain monoid $(\mathbb{P}_f(\mathbb{N}), \uplus, \emptyset)$ as a model, which is the simplest model of separation logic, but not the simplest model of BBI. On the contrary, we use the free monoid $(\mathbb{N} \times \mathbb{N}, +, (0, 0))$ as a model. Then, we adapt our technique to the RAM-domain model using a bisimulation between $\mathbb{P}_f(\mathbb{N})$ and $\mathbb{N} \times \mathbb{N}$.

In Section 2 we present the notion of non-deterministic monoid which is a generalization of the usual notion of commutative monoid where the composition may yield zero, one or arbitrarily many results. We introduce different sub-classes of non-deterministic monoids of interest for the semantics of either ILL, BBI or separation logic.

In Section 3 we present non-deterministic phase semantics for ILL where we generalize the well known result of soundness/completeness to our non-deterministic monoidal framework. The proofs are just simple generalizations of existing proofs and are delayed to Appendices A and B. We mention that completeness is obtained for most of the classes of non-deterministic monoids discussed in Section 2. Then we introduce trivial phase semantics which is the restriction of phase semantics where the closure operator is forced to be the identity. We mention the equivalence of trivial phase semantics with a corresponding Kripke semantics. We discuss the incompleteness of trivial phase semantics for ILL and the impact of the choice of the class of non-deterministic monoids.

In Section 4, we introduce the elementary fragment of ILL denoted eILL. We provide a goal-directed proof system called G-eILL and we show the soundness/completeness of G-eILL for the fragment eILL. We also show the completeness of trivial phase semantics for eILL using a simplified version of Okada's argument [Okada 2002]. This completeness holds for all classes of non-deterministic monoids discussed in Section 2, i.e. these (potentially) different trivial phase seman-

[1]The model used in [Brotherston and Kanovich 2010] is arguably the main difference with our approach but it is certainly not the sole difference: for instance, the fragment of BBI they use is not the direct image of the elementary fragment of ILL.

tics collapse on the elementary fragment. We also prove cut-elimination for eILL using a semantic argument and compare this proof with Okada's one.

In Section 5, we prove the undecidability of validity in eILL. We describe first informally then formally how to encode the computation steps of Minsky machines using the rules of G-eILL. The completeness of the encoding is obtained by a simple semantic argument comparable to the one we used for the completeness of trivial phase semantics for eILL.

In Section 6, we introduce Boolean BI and its Kripke semantics. We show that depending on the class of non-deterministic monoids, Kripke semantics might define differents sets of (universally) valid formulae.

In Section 7, we present a syntactic embedding of ILL into BBI which is faithful if the semantics of ILL is restricted to trivial phase semantics. Since eILL is complete for trivial phase semantics, we obtain a faithful embedding of eILL into BBI and conclude that (universal) validity is undecidable in BBI for each class of model discussed in Section 2. Using bisimulation, we also relate heap monoids (in particular the RAM-domain monoid) and free monoids to derive the undecidability of propositional separation logic, establishing a logical bridge with the results of [Brotherston and Kanovich 2010].

2. CLASSES OF NON-DETERMINISTIC MONOIDS

In this section, we define the algebraic notion of non-deterministic (commutative) monoid. We denote algebraic structures by $\mathcal{M}$, $\mathcal{N}$,... classes of structures by C, D,... sets by X, Y,... elements by x, y,... and well known constructs like the powerset by $\mathbb{P}(\mathsf{X})$ or the set of (finite) multisets by $\mathbb{M}_f(\mathsf{X})$. The symbol $\mathbb{N} = \{0, 1, 2, \ldots\}$ denotes the set of natural numbers. The symbol $\emptyset$ is used either to denote the empty set, the empty multiset or the empty class.

2.1. Non-deterministic monoids

Let us consider a set M and its powerset $\mathbb{P}(\mathsf{M})$, i.e. the set of subsets of M. A *composition* is a binary function $\circ : \mathsf{M} \times \mathsf{M} \longrightarrow \mathbb{P}(\mathsf{M})$ which is naturally extended to a binary operator on $\mathbb{P}(\mathsf{M})$ by

$$\mathsf{X} \circ \mathsf{Y} = \bigcup \{x \circ y \mid x \in \mathsf{X} \text{ and } y \in \mathsf{Y}\} \tag{1}$$

for any subsets X, Y of M. Using this extension, we can view an element m of M as the singleton set $\{m\}$ and derive equations like $m \circ \mathsf{X} = \{m\} \circ \mathsf{X}$ and $a \circ b = \{a\} \circ \{b\}$ by a slight abuse of notation.

Definition 2.1. A *non-deterministic (or relational) monoid* is a triple $(\mathsf{M}, \circ, \epsilon)$ where M is a set, $\epsilon \in \mathsf{M}$ is the *neutral element* and $\circ : \mathsf{M} \times \mathsf{M} \longrightarrow \mathbb{P}(\mathsf{M})$ is the *composition operator*. In addition, the following axioms are mandatory:

$$\begin{array}{ll} \forall a \in \mathsf{M}, \epsilon \circ a = \{a\} & \text{(neutrality)} \\ \forall a, b \in \mathsf{M}, a \circ b = b \circ a & \text{(commutativity)} \\ \forall a, b, c \in \mathsf{M}, a \circ (b \circ c) = (a \circ b) \circ c & \text{(associativity)} \end{array}$$

The class of non-deterministic monoids is denoted ND.

Associativity should be understood using the extension of $\circ$ to $\mathbb{P}(\mathsf{M})$ as defined by Equation (1). The extension of $\circ$ to $\mathbb{P}(\mathsf{M})$ induces a commutative monoidal structure with unit element $\{\epsilon\}$ on $\mathbb{P}(\mathsf{M})$. As a consequence, the structure $(\mathbb{P}(\mathsf{M}), \circ, \{\epsilon\})$ is a (usual) commutative monoid.

The term *non-deterministic* was introduced in [Galmiche and Larchey-Wendling 2006] in order to emphasize the fact that the composition $a \circ b$ may yield not only one but an arbitrary number of results including the possible incompatibility of a and b in which case $a \circ b = \emptyset$. If $(\mathsf{M}, +, 0)$ is a (usual) commutative monoid then, defining $a \circ b = \{a + b\}$ and $\epsilon = 0$ induces a non-deterministic monoid $(\mathsf{M}, \circ, \epsilon)$. Using the bijection $x \mapsto \{x\}$ mapping elements of M to singletons in $\mathbb{P}(\mathsf{M})$, we can view (usual) commutative monoids as a particular case of non-deterministic monoids (later called total deterministic monoids). Partial monoids can also be represented using the empty set $\emptyset$ as the result of undefined compositions (see Section 2.2).

The term *relational* is sometimes used because the operator $\circ : \mathsf{M} \times \mathsf{M} \longrightarrow \mathbb{P}(\mathsf{M})$ can equivalently be understood as a ternary relation $- \circ - \ni - : \mathsf{M}\times\mathsf{M}\times\mathsf{M} \longrightarrow \{0,1\}$ obtained by uncurrying the map $\circ$ using the isomorphism $\mathsf{M} \times \mathsf{M} \longrightarrow \mathbb{P}(\mathsf{M}) \simeq \mathsf{M} \times \mathsf{M} \times \mathsf{M} \longrightarrow \{0,1\}$. In that case, the axioms correspond to those of an internal monoid in the category of relations [Ghilardi and Meloni 1990]. The two presentations are equivalent but we rather use the monoidal presentation in this paper because it better suits the context and habits of phase semantics and Kripke semantics.

2.2. Sub-classes of non-deterministic monoids

The class ND of non-derterministic monoids is the largest class of structures we consider in this paper. We are now going to define sub-classes of ND. Let $(\mathsf{M}, \circ, \epsilon)$ be a non-deterministic monoid of class ND. It is a *partial deterministic monoid* if for all $x, y \in \mathsf{M}$, the composition $x \circ y$ is either empty or a singleton. It is a *total deterministic monoid* if for all $x, y \in \mathsf{M}$, the composition $x \circ y$ is a singleton. We use PD (resp. TD) to represent the sub-class of partial deterministic (resp. total deterministic) monoids. The reader may have noticed that total deterministic monoids (of class TD) exactly correspond to those non-deterministic monoids derived from usual commutative monoids via the map $x \mapsto \{x\}$ because the composition $\circ$ is a functional relation in this case (exactly one image for each pair of parameters).

Let us give an example of non-deterministic monoid which shows that the class ND contains structures that have properties which are fundamentally different from those of partial or total monoids. The non-deterministic monoid $(\{\epsilon, \mathtt{x}, \mathtt{y}\}, \circ, \epsilon)$ built over this three element set and defined by the following composition operator:

$\circ$	ϵ	$\mathtt{x}$	$\mathtt{y}$
ϵ	$\{\epsilon\}$	$\{\mathtt{x}\}$	$\{\mathtt{y}\}$
$\mathtt{x}$	$\{\mathtt{x}\}$	$\{\epsilon, \mathtt{y}\}$	$\{\mathtt{y}\}$
$\mathtt{y}$	$\{\mathtt{y}\}$	$\{\mathtt{y}\}$	$\{\mathtt{y}\}$

is an example of such non-deterministic monoid. It is a witness that PD is a proper sub-class of ND. But also, we see that in this monoid, x is both self inverse ($\epsilon \in x \circ x$) and this same composition yields the absorbing element ($\mathtt{y} \in x \circ x$). In Section 6.1, we will see that BBI is able to witness the difference between the class ND and the class PD.

A typical sub-class of partial deterministic monoids is obtained by considering disjoint union over the powerset. Given a set X, consider the partial deterministic monoid $(\mathbb{P}(\mathsf{X}), \uplus, \emptyset)$ where $\emptyset$ is the empty subset of X and $\uplus$ is defined for $\mathsf{A}, \mathsf{B} \subseteq \mathsf{X}$ by

$$\mathsf{A} \uplus \mathsf{B} = \begin{cases} \emptyset & \text{when } \mathsf{A} \cap \mathsf{B} \neq \emptyset \\ \{\mathsf{A} \cup \mathsf{B}\} & \text{when } \mathsf{A} \cap \mathsf{B} = \emptyset \end{cases}$$

One could even restrict to finite subsets of X by considering the partial monoid $(\mathbb{P}_f(\mathsf{X}), \uplus, \emptyset)$ where $\mathbb{P}_f(\mathsf{X})$ is the set of finite subsets of X. The partial monoid $(\mathbb{P}_f(\mathbb{N}), \uplus, \emptyset)$ is called the *RAM-domain model* [Brotherston and Kanovich 2010] and is considered te be the simplest model of (propositional) separation logic.

A (more general) sub-class of partial deterministic monoids is of particular importance to separation logic [Ishtiaq and O'Hearn 2001]. Given an (infinite) set L of *locations* and a (non-empty) set V of *values*, a *heap* is a partial function from locations to values defined only on a finite number of locations. We define

$$\mathbb{H}_{\mathsf{L},\mathsf{V}} = \{h : \mathsf{L} \longrightarrow_f \mathsf{V} \mid \mathrm{def}(h) \text{ is finite}\} \qquad \text{where } \mathrm{def}(h) = \{l \in \mathsf{L} \mid h(l) \text{ is defined}\}$$

so $\mathrm{def}(h)$ is the (finite) set of locations on which h is defined. The binary composition $s \uplus t$ of two heaps $s, t \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ is defined by

$$s \uplus t = \begin{cases} \emptyset & \text{when } \mathrm{def}(s) \cap \mathrm{def}(t) \neq \emptyset \\ \{r\} & \text{when } \mathrm{def}(s) \cap \mathrm{def}(t) = \emptyset \end{cases} \qquad \text{with } \mathrm{graph}(r) = \mathrm{graph}(s) \cup \mathrm{graph}(t)$$

The heap defined nowhere (i.e. with an empty graph) is denoted $\varnothing$. The heap monoid $(\mathbb{H}_{\mathsf{L},\mathsf{V}}, \uplus, \varnothing)$ is a partial deterministic monoid of class PD. We point out that when $\mathsf{V} = \{*\}$ is a singleton set, then the heap monoid $(\mathbb{H}_{\mathsf{L},\{*\}}, \uplus, \varnothing)$ is isomorphic to the finite powerset monoid $(\mathbb{P}_f(\mathsf{L}), \uplus, \emptyset)$. In particular, $(\mathbb{H}_{\mathbb{N},\{*\}}, \uplus, \varnothing)$ is isomorphic to the RAM-domain monoid $(\mathbb{P}_f(\mathbb{N}), \uplus, \emptyset)$. Hence, the class of heap monoids contains (an isomorphic copy of) the class of finite powersets. The *class of heap monoids* is denoted HM:

$$\mathrm{HM} = \{(\mathbb{H}_{\mathsf{L},\mathsf{V}}, \uplus, \varnothing) \mid \mathsf{L} \text{ is infinite and } \mathsf{V} \text{ is not empty}\}$$

It is obviously a sub-class of PD. Since for any non-empty heap h we have $h \uplus h = \emptyset$ (but $\varnothing \uplus \varnothing = \{\varnothing\}$), it is clear that no heap monoid $\mathbb{H}_{\mathsf{L},\mathsf{V}}$ is a total deterministic monoid (because neither L nor V is empty). Hence, HM and TD are two disjoint sub-classes of PD.

The *class of separation algebras* [Calcagno et al. 2007] denoted SA is an abstraction of HM. It is composed of *cancellative* partial (commutative) monoids, i.e. in our setting, a partial deterministic monoid $(\mathsf{M}, \circ, \epsilon)$ of class PD which moreover verifies the axiom

$$\forall a, b, c \in \mathsf{M}, c \circ a = c \circ b \neq \emptyset \Rightarrow a = b \qquad \text{(cancellativity)}$$

Hence the inclusion SA $\subseteq$ PD is obvious. But it is easy to prove that heap monoids are cancellative, and thus the inclusion HM $\subseteq$ SA also holds. Both of these inclusions are strict: for instance, the monoid $(\mathbb{P}(\mathsf{X}), \cup, \emptyset)$ is total (hence partial) deterministic but not cancellative, therefore it is a witness for the relation PD $\nsubseteq$ SA; the free monoid $(\mathbb{N}, +, 0)$ is a cancellative total (hence partial) deterministic monoid but does not belong to HM, hence it is a witness for the relation SA $\nsubseteq$ HM.

Another important sub-class of non-deterministic monoids is the *class* FM *of free monoids* $(\mathbb{M}_f(\mathsf{X}), \star, \pi)$ where X is a set, $\mathbb{M}_f(\mathsf{X})$ denotes the set of multisets of elements of X, and $\star$ (resp. π) denotes multiset addition (resp. the empty multiset). When X is not empty, $\mathbb{M}_f(\mathsf{X})$ contains an element $x \neq \pi$ and in this case, $x \star x \neq \{x\}$. Since there are total deterministic monoids satisfying the axiom $x \star x = \{x\}$ (for example lattices), we deduce that FM is a proper sub-class of TD.

We finish with the class FMf of *finitely generated free monoids* which is the sub-class of FM of non-deterministic monoids of the form $(\mathbb{M}_f(\mathsf{X}), \star, \pi)$ where X is a *non-empty finite set*. The class FMf is obviously a strict sub-class of FM.

Proposition 2.2. FMf $\subsetneq$ FM $\subsetneq$ TD $\subsetneq$ PD $\subsetneq$ ND, HM $\subsetneq$ SA $\subsetneq$ PD, FM $\subsetneq$ SA *and* HM$\cap$TD $= \emptyset$.

3. SEQUENT CALCULUS AND PHASE SEMANTICS FOR ILL

Linear Logic and Intuitionistic Linear Logic (denoted ILL) are well-know sub-structural logics introduced by Girard in [Girard 1987] to better study the impact of structural rules on the proof-theoretical as well as semantical properties of logics. The reader can consult [Troelstra 1992] for an overview on those topics.

The formulae of ILL are defined by the following grammar:

$$A ::= v \mid c \mid !A \mid A \circledast A \quad \text{with } v \in \mathsf{Var}, c \in \{1, \top, \bot\}^2 \text{ and } \circledast \in \{\otimes, \multimap, \&, \oplus\}$$

A *sequent* is a pair denoted $\Gamma \vdash A$ where Γ is a *(finite) multiset of formulae* and A is a *single formula*. The *sequent calculus* S-ILL (see Figure 1) is provided for ILL and the *set of derivable sequents* is the least set closed under its rules. Notice that Γ, Δ denote multisets of formulae and A, B, C denote formulae. In rule $\langle !_R \rangle$, $!\,\Gamma$ denotes the multiset $!\,\Gamma = !\,A_1, \ldots, !\,A_k$ if $\Gamma = A_1, \ldots, A_k$.[3]

The notion of sequent calculus proof is defined as usual: an ordered tree where each node together with its sons corresponds to an instance of one of the rules of S-ILL. Hence, a sequent is derivable if and only if there exists a proof of it in S-ILL. By historical definition of ILL [Girard 1987], the

[2]Sometimes the neutral of $\oplus$ is denoted 0, but we favor $\bot$ as in [Troelstra 1992].

[3]Notice that when multisets are considered as syntactic objects, it is usual to denote the composition of multisets by a comma and the empty multiset by void. On the contrary, when multisets are considered as semantic objects, the composition of multisets and the empty multiset might have different denotations: for instance, we will use $\star$ and π in this paper.

$$\frac{}{A \vdash A}\,\langle\mathrm{id}\rangle \qquad \frac{}{\Gamma, \bot \vdash A}\,\langle\bot_L\rangle \qquad \frac{}{\Gamma \vdash \top}\,\langle\top_R\rangle \qquad \frac{}{\vdash 1}\,\langle 1_R\rangle \qquad \frac{\Gamma \vdash A \qquad A, \Delta \vdash B}{\Gamma, \Delta \vdash B}\,\langle\mathrm{cut}\rangle$$

$$\frac{\Gamma, A \vdash B}{\Gamma, !A \vdash B}\,\langle !_L\rangle \qquad \frac{!\Gamma \vdash B}{!\Gamma \vdash !B}\,\langle !_R\rangle \qquad \frac{\Gamma \vdash B}{\Gamma, !A \vdash B}\,\langle\mathrm{w}\rangle \qquad \frac{\Gamma, !A, !A \vdash B}{\Gamma, !A \vdash B}\,\langle\mathrm{c}\rangle \qquad \frac{\Gamma \vdash A}{\Gamma, 1 \vdash A}\,\langle 1_L\rangle$$

$$\frac{\Gamma, A \vdash C}{\Gamma, A \,\&\, B \vdash C}\,\langle\&_L^1\rangle \qquad \frac{\Gamma, B \vdash C}{\Gamma, A \,\&\, B \vdash C}\,\langle\&_L^2\rangle \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \,\&\, B}\,\langle\&_R\rangle$$

$$\frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \oplus B \vdash C}\,\langle\oplus_L\rangle \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \oplus B}\,\langle\oplus_R^1\rangle \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \oplus B}\,\langle\oplus_R^2\rangle$$

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C}\,\langle\otimes_L\rangle \qquad \frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B}\,\langle\otimes_R\rangle \qquad \frac{\Gamma \vdash A \qquad \Delta, B \vdash C}{\Gamma, \Delta, A \multimap B \vdash C}\,\langle\multimap_L\rangle \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B}\,\langle\multimap_R\rangle$$

Fig. 1. Sequent calculus **S-ILL** for **ILL**

sequents which are provable in S-ILL are exactly the *valid sequents* of ILL, and a formula A of ILL is valid if $\vdash A$ is a valid sequent.

3.1. Non-deterministic phase spaces for ILL

We extend the notion of intuitionistic phase space [Girard 1987] to non-deterministic monoids and show that this semantic interpretation is sound and complete w.r.t. S-ILL, and thus equivalent to the original notion (see Corollary 3.6).

Definition 3.1. A *non-deterministic (intuitionistic) phase space* is given by a non-deterministic monoid $\mathcal{M} = (\mathsf{M}, \circ, \epsilon)$ together with a stable closure operator $(\cdot)^\diamond : \mathbb{P}(\mathsf{M}) \longrightarrow \mathbb{P}(\mathsf{M})$ and a sub-monoid K included in $\mathsf{J} = \{x \in \mathsf{M} \mid x \in \{\epsilon\}^\diamond \cap (x \circ x)^\diamond\}$.

— the *closure property* corresponds to the condition

$$\mathsf{X} \subseteq \mathsf{Y}^\diamond \quad \text{iff} \quad \mathsf{X}^\diamond \subseteq \mathsf{Y}^\diamond \qquad \text{for any } \mathsf{X}, \mathsf{Y} \in \mathbb{P}(\mathsf{M})$$

We recall that the monoidal composition $\circ$ is naturally extended to $\mathbb{P}(\mathsf{M})$ by Equation (1) providing a (commutative) monoidal structure on $\mathbb{P}(\mathsf{M})$ with unit $\{\epsilon\}$. A subset X of M is $(\cdot)^\diamond$-*closed* (or simply closed when the closure operator is obvious from the context) if $\mathsf{X}^\diamond = \mathsf{X}$ or equivalently $\mathsf{X}^\diamond \subseteq \mathsf{X}$. The set of closed subsets is denoted $\mathcal{M}^\diamond = \{\mathsf{X} \in \mathbb{P}(\mathsf{M}) \mid \mathsf{X}^\diamond = \mathsf{X}\}$, not to be confused with $\mathsf{M}^\diamond$ where M is viewed as the (total) subset of M (and in this case, $\mathsf{M}^\diamond = \mathsf{M}$). Any intersection of closed subsets is a closed subset and thus $\mathcal{M}^\diamond$ is invariant under arbitrary intersections, inducing a complete lattice structure on $(\mathcal{M}^\diamond, \subseteq)$. These previous properties are independent of the monoidal structure.

— the *stability property*[4] corresponds to the condition

$$\mathsf{X}^\diamond \circ \mathsf{Y}^\diamond \subseteq (\mathsf{X} \circ \mathsf{Y})^\diamond \qquad \text{for any } \mathsf{X}, \mathsf{Y} \in \mathbb{P}(\mathsf{M})$$

Let $\multimap$ be the adjoint of $\circ$ as a binary operator on $\mathbb{P}(\mathsf{M})$. It is defined by $\mathsf{X} \multimap \mathsf{Y} = \{k \in \mathsf{M} \mid k \circ \mathsf{X} \subseteq \mathsf{Y}\}$ for any $\mathsf{X}, \mathsf{Y} \in \mathbb{P}(\mathsf{M})$. In the lattice $(\mathbb{P}(\mathsf{M}), \subseteq)$, the operator $\multimap$ is contra-variant in its first parameter and co-variant in its second and the following adjoint property holds

$$\mathsf{Z} \subseteq \mathsf{X} \multimap \mathsf{Y} \quad \text{iff} \quad \mathsf{Z} \circ \mathsf{X} \subseteq \mathsf{Y} \qquad \text{for any } \mathsf{X}, \mathsf{Y}, \mathsf{Z} \in \mathbb{P}(\mathsf{M})$$

By stability of the closure operator $(\cdot)^\diamond$, the subset $\mathsf{X} \multimap \mathsf{Y}$ is closed as soon as Y is closed and $\mathsf{X} \multimap \mathsf{Y}^\diamond = \mathsf{X}^\diamond \multimap \mathsf{Y}^\diamond$ holds for any $\mathsf{X}, \mathsf{Y} \in \mathbb{P}(\mathsf{M})$.

— the set K is a given *sub-monoid* of $\mathcal{M}$ included in J, i.e. K verifies both

$$\epsilon \in \mathsf{K} \subseteq \mathsf{J} \qquad \text{and} \qquad \mathsf{K} \circ \mathsf{K} \subseteq \mathsf{K}$$

[4] A stable closure is a *quantic nucleus* in quantale theory [Yetter 1990]. The "stability" property itself seems to have no well established terminology.

We see that we have a (quite direct) generalization of the usual notion of phase space in the case where the monoid is neither supposed to be total nor deterministic. In the particular case of total deterministic monoids, we recover the usual notion of phase space.

The interpretation of ILL connectives is done in the following way. Given an *interpretation* of logical variables as closed subsets $[\![\cdot]\!] : \mathsf{Var} \longrightarrow \mathcal{M}^\diamond$, this interpretation is extended to all the formulae of ILL by structural induction as follows:

$$\begin{array}{rclcrcl} [\![\bot]\!] &=& \emptyset^\diamond & \quad & [\![A \oplus B]\!] &=& ([\![A]\!] \cup [\![B]\!])^\diamond \\ [\![\top]\!] &=& \mathsf{M} & & [\![A \,\&\, B]\!] &=& [\![A]\!] \cap [\![B]\!] \\ [\![1]\!] &=& \{\epsilon\}^\diamond & & [\![A \otimes B]\!] &=& ([\![A]\!] \circ [\![B]\!])^\diamond \\ [\![!A]\!] &=& (\mathsf{K} \cap [\![A]\!])^\diamond & & [\![A \multimap B]\!] &=& [\![A]\!] \multimap [\![B]\!] \end{array}$$

When the interpretation is done in a total deterministic monoid, we obtain *exactly the same value* for $[\![A]\!]$ as in the usual phase semantics interpretation.

Definition 3.2. A sequent $A_1, \ldots, A_k \vdash B$ of ILL is *valid in the interpretation* $[\![\cdot]\!]$ if the inclusion $[\![A_1]\!] \circ \cdots \circ [\![A_k]\!] \subseteq [\![B]\!]$ holds.

We recall the soundness theorem which states that provability in S-ILL entails semantic validity in non-deterministic intuitionistic phase semantics.

THEOREM 3.3 (SOUNDNESS OF PHASE SEMANTICS). *If the sequent* $A_1, \ldots, A_k \vdash B$ *has a proof in* S-ILL *then the inclusion relation* $[\![A_1]\!] \circ \cdots \circ [\![A_k]\!] \subseteq [\![B]\!]$ *holds.*

PROOF. The proof of this theorem can be done directly by generalizing the soundness proof of usual phase semantics [Girard 1987], or else, as done in Appendix A by using the algebraic semantic characterization of ILL of [Troelstra 1992]. □

Definition 3.4. We denote by ILL_p the set of sequents which have a proof in S-ILL. We denote by $\mathsf{ILL}_{\mathrm{X}}$ the set of sequents which are valid in every non-deterministic phase semantic interpretation where the base monoid is of the class X.

In this paper, the class X ranges over the following classes ND, PD, TD, HM, SA, FM and FMf. Let us consider the following inclusion sequence:

$$\mathsf{ILL}_p \subseteq \mathsf{ILL}_{\mathrm{ND}} \subseteq \mathsf{ILL}_{\mathrm{PD}} \subseteq \mathsf{ILL}_{\mathrm{TD}} \subseteq \mathsf{ILL}_{\mathrm{FM}} \subseteq \mathsf{ILL}_p \qquad (2)$$

The first inclusion $\mathsf{ILL}_p \subseteq \mathsf{ILL}_{\mathrm{ND}}$ is given by Theorem 3.3. The following inclusions $\mathsf{ILL}_{\mathrm{ND}} \subseteq \mathsf{ILL}_{\mathrm{PD}} \subseteq \mathsf{ILL}_{\mathrm{TD}} \subseteq \mathsf{ILL}_{\mathrm{FM}}$ are obvious consequences of the inclusions FM $\subseteq$ TD $\subseteq$ PD $\subseteq$ ND between classes of non-deterministic monoids. The last inclusion $\mathsf{ILL}_{\mathrm{FM}} \subseteq \mathsf{ILL}_p$ is just a reformulation of the completeness of the phase semantics w.r.t. S-ILL:

THEOREM 3.5 (COMPLETENESS OF PHASE SEMANTICS). *If the sequent* $\Gamma \vdash A$ *is valid in every free monoidal phase semantic interpretation* $(\mathsf{M}, \circ, \epsilon, (\cdot)^\diamond, \mathsf{K}, [\![\cdot]\!])$ *(i.e. with* $(\mathsf{M}, \circ, \epsilon)$ *of the class* FM*), then* $\Gamma \vdash A$ *has a proof in* S-ILL.

PROOF. The proof is based on a very nice semantic argument first introduced by [Okada 2002]. Nevertheless, as its understanding is not really critical to the developments of this paper, it is postponed to Appendix B. □

COROLLARY 3.6. $\mathsf{ILL}_p = \mathsf{ILL}_{\mathrm{ND}} = \mathsf{ILL}_{\mathrm{PD}} = \mathsf{ILL}_{\mathrm{TD}} = \mathsf{ILL}_{\mathrm{SA}} = \mathsf{ILL}_{\mathrm{FM}}$ *and non-deterministic phase semantics is both sound and complete w.r.t.* S-ILL.

PROOF. With Theorem 3.5, we have closed the circular inclusion sequence (2) and we deduce $\mathsf{ILL}_p = \mathsf{ILL}_{\mathrm{ND}} = \mathsf{ILL}_{\mathrm{PD}} = \mathsf{ILL}_{\mathrm{TD}} = \mathsf{ILL}_{\mathrm{FM}}$. In particular $\mathsf{ILL}_p = \mathsf{ILL}_{\mathrm{ND}}$. For the class SA, consider the inclusion sequence FM $\subseteq$ SA $\subseteq$ PD which leads to the the circular inclusion sequence $\mathsf{ILL}_{\mathrm{PD}} \subseteq \mathsf{ILL}_{\mathrm{SA}} \subseteq \mathsf{ILL}_{\mathrm{FM}} = \mathsf{ILL}_{\mathrm{PD}}$. □

Remark: we leave open the questions of determining whether $\mathsf{ILL}_p = \mathsf{ILL}_\mathrm{X}$ or else $\mathsf{ILL}_p \subsetneq \mathsf{ILL}_\mathrm{X}$ when X = HM or X = FMf.[5]

3.2. Trivial phase semantics for ILL

In this section, we define trivial phase semantics which is a particular case of phase semantics where the choice of the least closure operator, i.e. the identity closure, is mandatory.

Definition 3.7. Given a non-deterministic monoid $\mathcal{M} = (\mathsf{M}, \circ, \epsilon)$, the *trivial phase space* is defined by taking the identity map on $\mathbb{P}(\mathsf{M})$ as closure operator (i.e. for all $\mathsf{X} \in \mathbb{P}(\mathsf{M})$, $\mathsf{X}^\diamond = \mathsf{X}$) and by taking $\mathsf{K} = \{\epsilon\}$.

It is clear that the identity on $\mathbb{P}(\mathsf{M})$ is both a closure and stable. Obviously also, $\mathsf{K} = \{\epsilon\}$ verifies the conditions $\epsilon \in \mathsf{K} \subseteq \mathsf{J}$ and $\mathsf{K} \circ \mathsf{K} \subseteq \mathsf{K}$.[6] In a trivial phase space, every subset of M is closed and thus $\mathcal{M}^\diamond = \mathbb{P}(\mathsf{M})$. Starting from an interpretation of logical variables $[\![\cdot]\!] : \mathsf{Var} \longrightarrow \mathcal{M}^\diamond$, the interpretation of ILL connectives simplifies to:

$$\begin{array}{rclcrcl} [\![\bot]\!] &=& \emptyset & \quad & [\![A \oplus B]\!] &=& [\![A]\!] \cup [\![B]\!] \\ [\![\top]\!] &=& \mathsf{M} & & [\![A \,\&\, B]\!] &=& [\![A]\!] \cap [\![B]\!] \\ [\![1]\!] &=& \{\epsilon\} & & [\![A \otimes B]\!] &=& [\![A]\!] \circ [\![B]\!] \\ [\![!\,A]\!] &=& \{\epsilon\} \cap [\![A]\!] & & [\![A \multimap B]\!] &=& [\![A]\!] \multimap [\![B]\!] \end{array} \tag{3}$$

Beware that *trivial phase semantics is not complete for (the whole)* ILL. Indeed, the additive connectives $\oplus$ and & are interpreted by set union and intersection and thus, become distributive over each other. This is not the case in (general) phase semantics. In particular, the formula $A \,\&\, (B \oplus C) \multimap (A \,\&\, B) \oplus (A \,\&\, C)$ is valid in trivial phase semantics but has no proof in S-ILL.

3.3. Kripke semantics for trivial ILL

From the equations defining trivial phase semantics (3), we derive the following Kripke semantic interpretation for the connectives of (trivial) ILL. Given a non-deterministic monoid $\mathcal{M} = (\mathsf{M}, \circ, \epsilon)$ and an interpretation of propositional variables $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$, we define the binary Kripke forcing relation by induction on the structure of ILL-formulae:

$$\begin{array}{rcl} m \Vdash_\delta v & \text{iff} & m \in \delta(v) \\ m \Vdash_\delta \bot & \text{iff} & \text{never} \\ m \Vdash_\delta \top & \text{iff} & \text{always} \\ m \Vdash_\delta 1 & \text{iff} & m = \epsilon \\ m \Vdash_\delta !\,A & \text{iff} & m = \epsilon \text{ and } \epsilon \Vdash_\delta A \end{array} \qquad \begin{array}{rcl} m \Vdash_\delta A \oplus B & \text{iff} & m \Vdash_\delta A \text{ or } m \Vdash_\delta B \\ m \Vdash_\delta A \,\&\, B & \text{iff} & m \Vdash_\delta A \text{ and } m \Vdash_\delta B \\ m \Vdash_\delta A \otimes B & \text{iff} & \exists a, b,\ m \in a \circ b \text{ and } a \Vdash_\delta A \text{ and } b \Vdash_\delta B \\ m \Vdash_\delta A \multimap B & \text{iff} & \forall a, b\ (b \in a \circ m \text{ and } a \Vdash_\delta A) \Rightarrow b \Vdash_\delta B \end{array}$$

and obtain the following soundness/completeness result. Recall that the identity $\mathcal{M}^\diamond = \mathbb{P}(\mathsf{M})$ holds in trivial phase semantics.

PROPOSITION 3.8. *Let $\mathcal{M} = (\mathsf{M}, \circ, \epsilon)$ be a non-deterministic monoid. If the trivial phase semantics interpretation $[\![\cdot]\!] : \mathsf{Var} \longrightarrow \mathcal{M}^\diamond$ and the Kripke interpretation $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$ are identical maps then the trivial phase semantics and the Kripke semantics are in the following relation for any* ILL*-formula F and any $m \in \mathsf{M}$:*

$$m \in [\![F]\!] \quad \textit{iff} \quad m \Vdash_\delta F$$

PROOF. By induction on F. □

In this Kripke semantics for (trivial) ILL, we observe that the additive connectives are interpreted by Boolean operations and that the exponential is interpreted by a Boolean conjunction with the unit.

[5]But we don't view these questions as either central or very difficult. For instance, as the cut-free S-ILL calculus enjoys the sub-formula property, it should be possible to restrict the models used in the completeness proof to the multiset of sub-formulae occuring in the initial sequent, hence obtaining $\mathsf{ILL}_p = \mathsf{ILL}_{\mathrm{FMf}}$.

[6]No other choice for K is possible because $\mathsf{J} = \{x \in \mathsf{M} \mid x \in \{\epsilon\}^\diamond \cap (x \circ x)^\diamond\} = \{\epsilon\}$ when $(\cdot)^\diamond$ is the identity map on $\mathbb{P}(\mathsf{M})$.

$$\frac{}{!\,\Sigma, u \vdash u}\ \langle \mathrm{Ax} \rangle \qquad \frac{!\,\Sigma, \Gamma \vdash u}{!\,\Sigma, \Gamma \vdash v}\ u \multimap v \in \Sigma \qquad \frac{!\,\Sigma, \Gamma, u \vdash v}{!\,\Sigma, \Gamma \vdash w}\ (u \multimap v) \multimap w \in \Sigma$$

$$\frac{!\,\Sigma, \Gamma \vdash u \qquad !\,\Sigma, \Delta \vdash v}{!\,\Sigma, \Gamma, \Delta \vdash w}\ u \multimap (v \multimap w) \in \Sigma \qquad \frac{!\,\Sigma, \Gamma \vdash u \qquad !\,\Sigma, \Gamma \vdash v}{!\,\Sigma, \Gamma \vdash w}\ (u \,\&\, v) \multimap w \in \Sigma$$

Fig. 2. G-eILL: a goal-directed sequent calculus for eILL

Moreover, the linear connectives of trivial ILL are interpreted as the linear connectives of Boolean BI; see Section 6.1. We remark that since every subset of M is closed in trivial phase semantics, the Boolean complement could in principle be added as an operator: we will see that in fact, Boolean BBI is exactly what you get when you add a Boolean negation to trivial ILL; see Section 7.1 for a precise formulation of this claim. But beware that the apparent simplicity of the claim is the consequence of the generalization of phase semantics to non-deterministic monoids, and the focus on trivial phase semantics (which is not a complete semantics for ILL).

Definition 3.9. We denote by $\mathsf{ILL}^t_{\mathrm{X}}$ the set of sequents which are valid in every trivial phase semantic interpretation where the base (non-deterministic) monoid is of the class X.

Contrary to what happens in ordinary phase semantics where the choice of the class X has no impact on $\mathsf{ILL}_{\mathrm{X}}$ (at least for most of the classes we consider), we do not know whether inclusions like $\mathsf{ILL}^t_{\mathrm{ND}} \subseteq \mathsf{ILL}^t_{\mathrm{PD}}$ or $\mathsf{ILL}^t_{\mathrm{PD}} \subseteq \mathsf{ILL}^t_{\mathrm{TD}}$ are strict or not in trivial phase semantics. We will see that we have some answers for Boolean BI (see Section 6.2) but all involve Boolean negations, and Boolean negation is not available in (trivial) ILL. We view these open questions as potentially difficult.

As a final remark on trivial ILL, we point out that we do not have any specific proof-system for it, except those you could get by restricting an existing proof-system for Boolean BI to the fragment corresponding to trivial ILL (i.e. by removing the Boolean negation).

The central and key result of this paper is that ILL *contains a fragment which is both undecidable and complete for trivial phase semantics*. We call it the elementary fragment of ILL.

4. ELEMENTARY INTUITIONISTIC LINEAR LOGIC AND TRIVIAL PHASE SEMANTICS

We define and characterize *elementary* ILL (denoted eILL), an extension of the fragment $\mathsf{s\text{-}IMELL}_0^{\multimap}$ of ILL [de Groote et al. 2004]. We provide a simple goal-directed proof system, denoted G-eILL, which is itself an extension of the goal-directed proof system of $\mathsf{s\text{-}IMELL}_0^{\multimap}$, obtained by the addition of a new additive rule. Then we show that the proof system G-eILL and trivial phase semantics are both sound and complete w.r.t. the fragment eILL. We also show that validity in trivial phase semantics does not depend on a particular class of models on the elementary fragment: all classes among ND, PD, TD, FM and FMf define the same set of (universally) valid elementary sequents. This result will be completed for the classes HM and SA in Section 7.3 (see Theorem 7.8).

4.1. The eILL fragment of ILL

Definition 4.1. A formula of ILL is $(\multimap, \&)$-*elementary* if it is of the form $u \multimap v$, $(u \multimap v) \multimap w$, $u \multimap (v \multimap w)$ or $(u \,\&\, v) \multimap w$ where u, v and w are logical variables in Var. *The sequents of the fragment* eILL are those of the form $!\,\Sigma, \Gamma \vdash c$ where Γ is a multiset of variables, c is a variable and Σ is a multiset of $(\multimap, \&)$-elementary formulae.

From this definition, it is obvious that membership in the fragment eILL is a recursive property. Compared to $\mathsf{s\text{-}IMELL}_0^{\multimap}$, the only new form is $(u \,\&\, v) \multimap w$. The validity of sequents in eILL can be established using the proof system S-ILL but we rather provide an alternative goal-directed proof system called G-eILL in Figure 2. We point out that the backward application of the rules of G-eILL preserve elementary sequents. Hence, using G-eILL, backward proof-search starting from an elementary sequent could be done entirely within eILL, which would not be the case using S-ILL.

Apart from the axiom rule $\langle \mathrm{Ax} \rangle$, each other rule $\langle {\multimap} \rangle$, $\langle ({\multimap}){\multimap} \rangle$, $\langle {\multimap}({\multimap}) \rangle$ or $\langle (\&){\multimap} \rangle$ is named according to the form of its side condition. Compared to s-IMELL$_0^{\multimap}$, the only new rule is $\langle (\&){\multimap} \rangle$ (see [de Groote et al. 2004]). In this paper, the authors did not provide a proof of soundness/completeness of the system s-IMELL$_0^{\multimap}$, leaving it to the reader. Here we present a full proof of soundness/completeness for our extension G-eILL in order to derive the completeness of trivial phase semantics for this fragment.

4.2. Completeness results for eILL

Even though validity in eILL is the same as in the whole ILL (established for instance by a proof in S-ILL), here we show that in this specific fragment, validity is also sound and complete both w.r.t. the system G-eILL and w.r.t. finitely generated free monoidal trivial phase semantics.

Lemma 4.2. *Every proof of a sequent in* G-eILL *can be transformed into a proof (of the same sequent) which uses only rules* $\langle \mathrm{id} \rangle$, $\langle \mathrm{w} \rangle$, $\langle \mathrm{c} \rangle$, $\langle {\multimap_L} \rangle$, $\langle {\multimap_R} \rangle$, $\langle !_L \rangle$ *and* $\langle \&_R \rangle$ *of* S-ILL.

Proof. We proceed by induction on the proofs in G-eILL and by case analysis, depending on the last rule applied. Let n be the cardinal of the multiset Σ. For each rule of G-eILL, we propose a corresponding (open) proof tree in S-ILL:

— case of rule $\langle \mathrm{Ax} \rangle$:

$$\dfrac{\dfrac{\dfrac{}{u \vdash u}\langle \mathrm{id} \rangle}{\vdots}\langle \mathrm{w} \rangle \ \text{applied } n \text{ times}}{!\,\Sigma, u \vdash u}\langle \mathrm{w} \rangle$$

— case of rule $\langle {\multimap} \rangle$:

$$\dfrac{\dfrac{\dfrac{!\,\Sigma, \Gamma \vdash u \qquad \dfrac{}{v \vdash v}\langle \mathrm{id} \rangle}{!\,\Sigma, \Gamma, u \multimap v \vdash v}\langle {\multimap_L} \rangle}{!\,\Sigma, \Gamma, !(u \multimap v) \vdash v}\langle !_L \rangle}{!\,\Sigma, \Gamma \vdash v}\langle \mathrm{c} \rangle$$

— case of rule $\langle ({\multimap}){\multimap} \rangle$:

$$\dfrac{\dfrac{\dfrac{\dfrac{!\,\Sigma, \Gamma, u \vdash v}{!\,\Sigma, \Gamma \vdash u \multimap v}\langle {\multimap_R} \rangle \qquad \dfrac{}{w \vdash w}\langle \mathrm{id} \rangle}{!\,\Sigma, \Gamma, (u \multimap v) \multimap w \vdash w}\langle {\multimap_L} \rangle}{!\,\Sigma, \Gamma, !((u \multimap v) \multimap w) \vdash w}\langle !_L \rangle}{!\,\Sigma, \Gamma \vdash w}\langle \mathrm{c} \rangle$$

— case of rule $\langle {\multimap}({\multimap}) \rangle$:

$$\dfrac{\dfrac{\dfrac{\dfrac{!\,\Sigma, \Gamma \vdash u \qquad \dfrac{!\,\Sigma, \Delta \vdash v \qquad \dfrac{}{w \vdash w}\langle \mathrm{id} \rangle}{!\,\Sigma, \Delta, v \multimap w \vdash w}\langle {\multimap_L} \rangle}{!\,\Sigma, \Gamma, !\,\Sigma, \Delta, u \multimap (v \multimap w) \vdash w}\langle {\multimap_L} \rangle}{!\,\Sigma, \Gamma, !\,\Sigma, \Delta, !(u \multimap (v \multimap w)) \vdash w}\langle !_L \rangle}{\vdots}\langle \mathrm{c} \rangle \ \text{applied } n+1 \text{ times}}{!\,\Sigma, \Gamma, \Delta \vdash w}\langle \mathrm{c} \rangle$$

— case of rule $\langle(\&)\multimap\rangle$:

$$\dfrac{\dfrac{\dfrac{\dfrac{!\,\Sigma,\Gamma\vdash u \quad !\,\Sigma,\Gamma\vdash v}{!\,\Sigma,\Gamma\vdash u\,\&\,v}\langle\&_R\rangle \quad \dfrac{}{w\vdash w}\langle\mathrm{id}\rangle}{!\,\Sigma,\Gamma,(u\,\&\,v)\multimap w\vdash w}\langle\multimap_L\rangle}{!\,\Sigma,\Gamma,!((u\,\&\,v)\multimap w)\vdash w}\langle !_L\rangle}{!\,\Sigma,\Gamma\vdash w}\langle\mathrm{c}\rangle$$

Combining those (open) proof trees, it is obvious to design a recursive algorithm which transforms G-eILL proofs into S-ILL proofs. □

Lemma 4.3. *If the sequent $!\,\Sigma,\Gamma\vdash c$ of* eILL *is valid in every finitely generated free monoidal trivial phase semantic interpretation*[7] *then it has a proof in* G-eILL.

Proof. Let us consider a fixed sequent $!\,\Sigma_0,\Gamma_0\vdash c_0$ where $\Sigma_0 = \sigma_1,\ldots,\sigma_k$ is composed of k elementary formulae. We suppose that $!\,\Sigma_0,\Gamma_0\vdash c_0$ is valid in trivial phase semantic interpretation in class FMf. We show that $!\,\Sigma_0,\Gamma_0\vdash c_0$ has a proof in G-eILL using a semantic argument.

Let us choose a finite non-empty subset $\mathsf{L}\subseteq\mathsf{Var}$ such that every variable occuring in the sequent $!\,\Sigma_0,\Gamma_0\vdash c_0$ belongs to L (there are only finitely many variables occuring in the sequent). We consider the free commutative monoid $\mathsf{M}=\mathbb{M}_f(\mathsf{L})$ over the set L, i.e. the set of finite multisets of elements of L endowed with multiset addition (denoted by the comma) as monoidal composition and with the empty multiset (denoted $\pi=\lfloor\emptyset\rfloor$) as neutral element. We write $\lfloor a,a,b\rfloor$ for the multiset composed of two occurrences of a and one of b. Let us define the finitely generated free commutative monoid $(\mathsf{M},\star,\pi)$ of class FMf where $\mathsf{M}=\mathbb{M}_f(\mathsf{L})$, $\pi=\lfloor\emptyset\rfloor$ and $\star:\mathsf{M}\times\mathsf{M}\longrightarrow\mathbb{P}(\mathsf{M})$ is defined by $\lfloor\Gamma\rfloor\star\lfloor\Delta\rfloor=\{\lfloor\Gamma,\Delta\rfloor\}$.[8] The adjoint of $\star$ is denoted $\multimap\!\!\star$.

We consider the following semantic interpretation in the trivial phase space based on $(\mathsf{M},\star,\pi)$:

$$[\![u]\!]=\{\lfloor\Gamma\rfloor\in\mathsf{M}\mid\,!\,\Sigma_0,\Gamma\vdash u \text{ has a proof in G-eILL}\}\quad\text{for } u\in\mathsf{Var}$$

Let us now show that $\pi\in[\![\sigma_i]\!]$ holds for any $\sigma_i\in\Sigma_0$. We proceed by case analysis:

— if $\sigma_i=u\multimap v$. We have $\pi\in[\![u\multimap v]\!]$ iff $\lfloor\emptyset\rfloor\star[\![u]\!]\subseteq[\![v]\!]$ iff $[\![u]\!]\subseteq[\![v]\!]$. So let us consider one $\lfloor\Gamma\rfloor$ such that $\lfloor\Gamma\rfloor\in[\![u]\!]$ and prove that $\lfloor\Gamma\rfloor\in[\![v]\!]$. By definition of $[\![u]\!]$, the sequent $!\,\Sigma_0,\Gamma\vdash u$ has a proof in G-eILL and $\lfloor\Gamma\rfloor\in\mathsf{M}$. Then, by rule $\langle\multimap\rangle$, the sequent $!\,\Sigma_0,\Gamma\vdash v$ has a proof in G-eILL. So we deduce $\lfloor\Gamma\rfloor\in[\![v]\!]$. Hence $[\![u]\!]\subseteq[\![v]\!]$ and we obtain $\pi\in[\![\sigma_i]\!]$;

— if $\sigma_i=(u\multimap v)\multimap w$. We have $\pi\in[\![(u\multimap v)\multimap w]\!]$ iff $[\![u]\!]\multimap\!\!\star[\![v]\!]\subseteq[\![w]\!]$. Let use choose $\lfloor\Gamma\rfloor\in[\![u]\!]\multimap\!\!\star[\![v]\!]$. Then $\{\lfloor\Gamma\rfloor\}\star[\![u]\!]\subseteq[\![v]\!]$. By rule $\langle\mathrm{Ax}\rangle$, $!\,\Sigma_0,u\vdash u$ has a proof in G-eILL. As u occurs in σ_i, we deduce $u\in\mathsf{L}$ and thus $\lfloor u\rfloor\in\mathsf{M}$. We derive $\lfloor u\rfloor\in[\![u]\!]$. Thus $\{\lfloor\Gamma,u\rfloor\}=\lfloor\Gamma\rfloor\star\lfloor u\rfloor\subseteq[\![v]\!]$. Thus $!\,\Sigma_0,\Gamma,u\vdash v$ has a proof in G-eILL. By rule $\langle(\multimap)\multimap\rangle$, $!\,\Sigma_0,\Gamma\vdash w$ has a proof in G-eILL. We conclude $\lfloor\Gamma\rfloor\in[\![w]\!]$. Thus $[\![u]\!]\multimap\!\!\star[\![v]\!]\subseteq[\![w]\!]$ holds, hence $\pi\in[\![\sigma_i]\!]$;

— if $\sigma_i=u\multimap(v\multimap w)$. We have $\pi\in[\![u\multimap(v\multimap w)]\!]$ iff $[\![u]\!]\star[\![v]\!]\subseteq[\![w]\!]$. Let us choose $\lfloor\Gamma\rfloor\in[\![u]\!]$ and $\lfloor\Delta\rfloor\in[\![v]\!]$ and let us prove $\lfloor\Gamma\rfloor\star\lfloor\Delta\rfloor\subseteq[\![w]\!]$. Both $!\,\Sigma_0,\Gamma\vdash u$ and $!\,\Sigma_0,\Delta\vdash v$ have a proof in G-eILL. By rule $\langle\multimap(\multimap)\rangle$, the sequent $!\,\Sigma_0,\Gamma,\Delta\vdash w$ has a proof in G-eILL. As $\lfloor\Gamma,\Delta\rfloor\in\mathsf{M}$, we derive $\lfloor\Gamma\rfloor\star\lfloor\Delta\rfloor=\{\lfloor\Gamma,\Delta\rfloor\}\subseteq[\![w]\!]$. We deduce $[\![u]\!]\star[\![v]\!]\subseteq[\![w]\!]$ and thus conclude $\pi\in[\![\sigma_i]\!]$;

— if $\sigma_i=(u\,\&\,v)\multimap w$. We have $\pi\in[\![(u\,\&\,v)\multimap w]\!]$ iff $[\![u]\!]\cap[\![v]\!]\subseteq[\![w]\!]$. If $\lfloor\Gamma\rfloor\in[\![u]\!]\cap[\![v]\!]$ then $\lfloor\Gamma\rfloor\in\mathsf{M}$ and both $!\,\Sigma_0,\Gamma\vdash u$ and $!\,\Sigma_0,\Gamma\vdash v$ have a proof in G-eILL. By rule $\langle(\&)\multimap\rangle$, the sequent $!\,\Sigma_0,\Gamma\vdash w$ has a proof in G-eILL. Thus $\lfloor\Gamma\rfloor\in[\![w]\!]$. We have proved that $[\![u]\!]\cap[\![v]\!]\subseteq[\![w]\!]$ and we conclude $\pi\in[\![\sigma_i]\!]$.

[7] i.e. every trivial phase semantic interpretation in the class FMf.

[8] Here, $\Gamma\mapsto\lfloor\Gamma\rfloor$ is the identity map on $\mathbb{M}_f(\mathsf{Var})$ but the extra notation $\lfloor\cdot\rfloor$ in the expression $\{\lfloor\Gamma,\Delta\rfloor\}$ has the side effect of removing the ambiguity on the denotation of the comma: here, it denotes the composition of multisets, not the addition of elements in a set.

So, for any $i \in [1,k]$ the inclusion $\pi \in [\![\sigma_i]\!]$ holds and as a consequence, $[\![!\,\sigma_i]\!] = \{\pi\}$ because the identity $[\![!\,\sigma_i]\!] = \{\pi\} \cap [\![\sigma_i]\!]$ holds in trivial phase semantics. Let us write $\Gamma_0 = \lfloor a_1, \ldots, a_p \rfloor$. Since L contains all the variables occuring in the sequent $!\,\Sigma_0, \Gamma_0 \vdash c_0$, we have $\lfloor a_1, \ldots, a_p \rfloor \in \mathsf{M}$. Since the sequent $!\,\Sigma_0, \Gamma_0 \vdash c_0$ of eILL is valid in every finitely generated free monoidal trivial phase semantics interpretation, as a particular case, it is valid in the interpretation $(\mathsf{M}, \star, \pi, [\![\cdot]\!])$ and thus the inclusion

$$[\![!\,\sigma_1]\!] \star \cdots \star [\![!\,\sigma_k]\!] \star [\![a_1]\!] \star \cdots \star [\![a_p]\!] \subseteq [\![c_0]\!]$$

holds. By rule $\langle \mathrm{Ax} \rangle$, for any $i \in [1,p]$ the sequent $!\,\Sigma_0, a_i \vdash a_i$ has a proof in $\mathsf{G\text{-}eILL}$ and since $a_i \in \mathsf{L}$, then the relation $\lfloor a_i \rfloor \in [\![a_i]\!]$ holds. Remember that for any $i \in [1,k]$, we have $\lfloor \emptyset \rfloor = \pi \in [\![!\,\sigma_i]\!]$. So

$$\lfloor \Gamma_0 \rfloor \in \{\lfloor a_1, \ldots, a_p \rfloor\} = \lfloor \emptyset \rfloor \star \cdots \star \lfloor \emptyset \rfloor \star \lfloor a_1 \rfloor \star \cdots \star \lfloor a_p \rfloor \subseteq [\![c_0]\!]$$

holds and we conclude that $!\,\Sigma_0, \Gamma_0 \vdash c_0$ has a proof in $\mathsf{G\text{-}eILL}$. □

THEOREM 4.4. *The system* $\mathsf{G\text{-}eILL}$ *is sound and complete for the fragment* eILL. *Given a class* $\mathrm{X} \in \{\mathrm{ND}, \mathrm{PD}, \mathrm{TD}, \mathrm{FM}, \mathrm{FMf}\}$, *the trivial phase semantics over the class* X *is sound and complete for the fragment* eILL.

PROOF. Consider the following inclusion sequence

$$\mathsf{eILL}_g \subseteq \mathsf{eILL}_p \subseteq \mathsf{eILL}^t_{\mathrm{ND}} \subseteq \mathsf{eILL}^t_{\mathrm{PD}} \subseteq \mathsf{eILL}^t_{\mathrm{TD}} \subseteq \mathsf{eILL}^t_{\mathrm{FM}} \subseteq \mathsf{eILL}^t_{\mathrm{FMf}} \subseteq \mathsf{eILL}_g$$

where eILL_g denotes the set of sequents of eILL which have a proof in $\mathsf{G\text{-}eILL}$ and $\mathsf{eILL}^t_{\mathrm{X}}$ denotes the set of sequents which are valid in every trivial phase semantic interpretation of the class X. The inclusion $\mathsf{eILL}_g \subseteq \mathsf{eILL}_p$ is a direct consequence of Lemma 4.2. The inclusion $\mathsf{eILL}_p \subseteq \mathsf{eILL}^t_{\mathrm{ND}}$ is a particular case of Theorem 3.3. The inclusion sequence $\mathsf{eILL}^t_{\mathrm{ND}} \subseteq \cdots \subseteq \mathsf{eILL}^t_{\mathrm{FMf}}$ is an obvious consequence of the inclusions FMf ⊆ FM ⊆ TD ⊆ PD ⊆ ND between classes of non-deterministic monoids. The last inclusion $\mathsf{eILL}^t_{\mathrm{FMf}} \subseteq \mathsf{eILL}_g$ is the result of Lemma 4.3. □

Remark: we solve the problem of the completeness of the fragment eILL w.r.t. trivial heap semantics or trivial separation algebra semantics by bisimulating free monoids with heap monoids; this will be addressed in Section 7.3.

4.3. Comparison with Okada's proof and semantic cut-elimination

The preceding proof could be compared to Okada's argument [Okada 2002] as reproduced in Appendix B. But there are some differences though. Okada's argument is a generalization of the Lindenbaum-Tarski algebra construction. The Lindenbaum-Tarski algebra is the cornerstone of algebraic logic and is typically used in the completeness proof for Hilbert-style proof systems. Logical formulae are interpreted by their own class in the algebra of classes of logically equivalent formulae. In the Lindenbaum-Tarski algebra, the transitivity of the relation of logical equivalence is usually grounded on some form of *cut* like for instance *modus-ponens*. The main strength of Okada's proof is that, contrary to the Lindenbaum-Tarski construction, *Okada's closure algebra can be built without using the cut rule*, leading to a proof of strong completeness from which semantic cut-elimination can be deduced as explained below.

LEMMA 4.5. *Let* $\langle \text{g-cut} \rangle$ *be the following cut rule:*

$$\frac{!\,\Sigma, \Gamma \vdash u \qquad !\,\Sigma, \Delta, u \vdash v}{!\,\Sigma, \Gamma, \Delta \vdash v}\ \langle \text{g-cut} \rangle$$

Every proof of a sequent in $\mathsf{G\text{-}eILL} + \langle \text{g-cut} \rangle$ *can be transformed into a proof (of the same sequent) which uses only rules* $\langle \mathrm{id} \rangle$, $\langle \mathrm{cut} \rangle$, $\langle \mathrm{w} \rangle$, $\langle \mathrm{c} \rangle$, $\langle \multimap_L \rangle$, $\langle \multimap_R \rangle$, $\langle !_L \rangle$ *and* $\langle \&_R \rangle$ *of* $\mathsf{S\text{-}ILL}$.

PROOF. We complete the argument developed in the proof of Lemma 4.2 with the following (open) proof tree in S-ILL, where n denotes the cardinal of the multiset Σ:

$$\cfrac{\cfrac{!\,\Sigma,\Gamma \vdash u \quad !\,\Sigma,\Delta,u \vdash v}{!\,\Sigma,!\,\Sigma,\Gamma,\Delta \vdash v}\langle\text{cut}\rangle}{\cfrac{\vdots \text{ applied } n \text{ times}}{!\,\Sigma,\Gamma,\Delta \vdash v}\langle\text{c}\rangle}\langle\text{c}\rangle$$

thus we obtain a recursive algorithm which transforms G-eILL+⟨g-cut⟩ proofs into S-ILL proofs. □

THEOREM 4.6 (SEMANTIC CUT-ELIMINATION FOR G-eILL + ⟨g-cut⟩). *The system* G-eILL+⟨g-cut⟩ *has cut-elimination, i.e. if a given sequent of* eILL *has a proof in* G-eILL + ⟨g-cut⟩ *then the same sequent has a proof in* G-eILL.

PROOF. Let $!\,\Sigma,\Gamma \vdash c$ be a sequent of the fragment eILL that has a proof in G-eILL + ⟨g-cut⟩. By Lemma 4.5, this sequent has a proof in S-ILL. Thus, as a particular case of Theorem 3.3, this sequent is valid in every finitely generated free monoidal trivial phase semantic interpretation. Hence, by Lemma 4.3, the sequent $!\,\Sigma,\Gamma \vdash c$ has a proof in G-eILL. □

Beware that there is no miracle here however: we cannot generalize this proof to the whole ILL since, as explained before, trivial phase semantics is a sound but incomplete semantics for ILL.

We also point out the following difference between Okada's proof and the proof of Lemma 4.3. The part $!\,\Sigma_0$ is fixed and only *the variables part* Γ is involved in the interpretation of logical variables. Logical variables are interpreted by the contexts that prove them as in Okada's proof but much of the complexity of his proof (i.e. the choice of the closure operator) is dismissed because there is no choice for the closure operator in trivial phase semantics.

5. THE UNDECIDABILITY OF ELEMENTARY INTUITIONISTIC LINEAR LOGIC

We propose an encoding of two counter Minsky machines in the elementary fragment of ILL.[9] The first encoding of Minsky machines in linear logic was done by Kanovich in the $(!,\oplus)$-Horn fragment of ILL [Kanovich 1994; 1995]. In this encoding, the recovery of computations from proofs is obtained through some form of proof normalization and the $\oplus$ additive connective is used to simulate forking. Lafont later showed that the use of proof normalization can be avoided and replaced by a phase semantics argument [Lafont 1996; Lafont and Scedrov 1996]. Okada finally showed that normalization/cut-elimination itself can be obtained by a phase semantics argument [Okada 2002].

In our encoding of Minsky machines in eILL, the & connective is used to simulate forking and we will show that a trivial phase semantics argument is sufficient to recover computability from provability.

5.1. Encoding Minsky machines instructions in eILL: an informal discussion

The aim of this section is to informally describe the main steps of the encoding of Minsky machines in eILL. We try to be as precise as possible but remember that the goal here is not to provide a formal proof (that is done in Section 5.3) but to give the reader some intuitions of how instructions are encoded by $(\multimap,\&)$-elementary formulae.

A two counter Minsky machine is given by two non-negative integer counters, say a and b, and a finite list of instructions positioned from 1 to l. An instruction is either an *incrementation followed by a jump* like

$$i\colon\ \texttt{a:=a+1 ; goto}\ j$$

[9] The encoding of many counters Minsky machines is also possible but this is not needed for our undecidability results.

or the combination of a *zero test followed by a decrementation and a jump* like

$$i\texttt{: if a=0 then goto } j \texttt{ else a:=a-1 ; goto } k$$

There is no instruction at position 0, but jumps can point to position 0 and when it arrives at this position, the machine stops. The state of the machine is described by the triplet (i, m, n) where i represents the position of the next instruction (unless $i = 0$ and in that case the computation is finished), and m (resp. n) represents the value of the counter a (resp. b).

The state of the machine changes as the instructions are executed following a (total) deterministic semantics until the value of i reaches 0. This operational semantics should be easily guessable by the reader; it is described precisely in the next section. We say that the state (i, m, n) is accepted by the machine if starting from the state (i, m, n) the computation of the machine eventually reaches the state $(0, 0, 0)$. We are now going to describe the main steps that allow the encoding of acceptance in the elementary fragment eILL.

Recall that a sequent of the elementary fragment eILL has the shape $!\,\Sigma, \Gamma \vdash c$ where Σ is a multiset of $(\multimap, \&)$-elementary formulae that we call *commands*, Γ is a multiset of variables and c is a variable. We call Γ the *variables part*, and *c the goal formula*. We say that a variable g is *in goal position* in an elementary formula when it is the rightmost variable, i.e. the formula is of one of the following forms: $\_ \multimap g$, $(\_ \multimap \_) \multimap g$, $\_ \multimap (\_ \multimap g)$ or $(\_ \,\&\, \_) \multimap g$. We say that g occurs in goal position in Σ when it is in goal position in at least one of the commands of Σ.

We remark that except for the axiom rule $\langle \mathrm{Ax} \rangle$, each other rule of G-eILL requires that the goal formula occurs in goal position in Σ. Hence, when a variable a does not occur in goal position in Σ, then no rule of G-eILL can be applied to obtain the sequent $!\,\Sigma, \Gamma \vdash \mathsf{a}$ except for the axiom rule $\langle \mathrm{Ax} \rangle$

$$\frac{}{!\,\Sigma, \Gamma \vdash \mathsf{a}}\ \langle \mathrm{Ax} \rangle$$

and in this case, Γ must be reduced to the singleton multiset $\Gamma = \lfloor \mathsf{a} \rfloor$. Hence, if the variable a does not occur in goal position in Σ, the sequent $!\,\Sigma, \Gamma \vdash \mathsf{a}$ has a proof in G-eILL if and only if $\Gamma = \lfloor \mathsf{a} \rfloor$. From this, we deduce an encoding of the emptiness test on Γ. Let $\mathsf{a} \neq \mathsf{q}_0$ be two variables that do not occur in goal position in Σ. We also suppose that q_0 does not occur in the variables part Γ. Then, if the sequent $!\,\Sigma, !(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0, \Gamma \vdash \mathsf{q}_0$ has a proof in G-eILL, it must end with the following rule instance

$$\frac{!\,\Sigma, !(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0, \Gamma, \mathsf{a} \vdash \mathsf{a}}{!\,\Sigma, !(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0, \Gamma \vdash \mathsf{q}_0}\ \langle (\multimap)\multimap \rangle$$

because no other rule is applicable.[10] Then, the sequent $!\,\Sigma, !(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0, \Gamma, \mathsf{a} \vdash \mathsf{a}$ has a proof in G-eILL if and only if $\lfloor \Gamma, \mathsf{a} \rfloor = \lfloor \mathsf{a} \rfloor$, hence if and only if $\Gamma = \lfloor \emptyset \rfloor$. As a conclusion, we see that the emptiness test on Γ can be implemented by q_0 in goal position in one and only one command of Σ: $(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0$.

Let us now describe how we are going to encode the states of Minsky machines in eILL sequents. Given a fixed Minsky machine, the elementary sequent $!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ is associated to the state (i, m, n) of this machine. The commands in Σ are computed from the list of instructions of the machine. In this sequent, q_i might occur in goal position in Σ and the corresponding commands are supposed to simulate the instruction at position i. On the contrary a, b do not occur in goal position in Σ. Since $m.\mathsf{a}$ denotes the multiset containing m occurrences of the variable a, we see that the values of the counters are encoded by the number of occurrences of a and b in the variables part of the elementary sequent. We will arrange so that no variable other than a and b occurs in the variables part of these elementary sequents. We wish to obtain the following equivalence which characterizes acceptance by provability:

$!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ *has a proof in* G-eILL *if and only if the state* (i, m, n) *is accepted by the machine*

[10] Remark that the axiom $\langle \mathrm{Ax} \rangle$ does not apply because q_0 does not occur in Γ.

Since there is no instruction at position 0, the only accepted state at position 0 is $(0, 0, 0)$, i.e. when $m = n = 0$. Hence we can encode this acceptance condition with the emptiness test, i.e. with the goal q_0 and the command $(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0$ in Σ.

For the increment instruction i: `a:=a+1 ; goto` j, we have to transform the acceptance of (i, m, n) into the acceptance of $(j, m + 1, n)$ which can be done using the goal q_i and the command $(\mathsf{a} \multimap \mathsf{q}_j) \multimap \mathsf{q}_i$. Indeed, the proof would then end with the rule

$$\frac{!\,\Sigma, \mathsf{a}, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_j}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i}\ (\mathsf{a} \multimap \mathsf{q}_j) \multimap \mathsf{q}_i \in \Sigma$$

If $(\mathsf{a} \multimap \mathsf{q}_j) \multimap \mathsf{q}_i$ is the only command in Σ where q_i occurs in goal position then any proof of the sequent $!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ must end with the previously displayed rule.

For the zero test/decrement instruction i: `if a=0 then goto` j `else a:=a-1 ; goto` k, we distinguish the two branches of the test. In the *else branch*, we have to transform the acceptance of $(i, m + 1, n)$ into the acceptance of (k, m, n). This can be done using the command $\mathsf{a} \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)$. Indeed, the proof would then end with the rules

$$\frac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\langle \mathrm{Ax} \rangle \qquad !\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_k}{!\,\Sigma, \mathsf{a}, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i}\ \mathsf{a} \multimap (\mathsf{q}_k \multimap \mathsf{q}_i) \in \Sigma$$

If $\mathsf{a} \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)$ is the only command in Σ where q_i occurs in goal position then any proof of the sequent $!\,\Sigma, (m + 1).\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ must end with the previously displayed rules instances: indeed, even if there are many ways to split the multiset $(m + 1).\mathsf{a}, n.\mathsf{b}$ in two parts, as a is not in goal position in Σ, the only way to split it so that the goal a can be proved in the left branch is to extract exactly one a from the multiset $(m + 1).\mathsf{a}, n.\mathsf{b}$. In the right branch, the computation would then continue from the state (k, m, n) as required.

For the *then branch*, we have to transform the acceptance of $(i, 0, n)$ into the acceptance of the $(j, 0, n)$. We could simply use the command $\mathsf{q}_j \multimap \mathsf{q}_i$ but this would also transform the acceptance of (i, m, n) into the acceptance of (j, m, n)

$$\frac{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_j}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i}\ \mathsf{q}_j \multimap \mathsf{q}_i \in \Sigma$$

and the condition $m = 0$ would not be mandatory in that case, which would lead to an unsound encoding. So we introduce a new goal $\underline{\mathsf{a}}$ which is supposed to perform zero test on the number of occurrences of a (see later for how this is done). Using an idea coming from [Kanovich 1995], we fork two branches using the command $(\underline{\mathsf{a}} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i$, one doing the zero test, the other transforming acceptance. In this case, the proof would end with the rules

$$\frac{\dfrac{\text{test } m = 0}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \underline{\mathsf{a}}} \qquad !\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_j}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i}\ (\underline{\mathsf{a}} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i \in \Sigma$$

and would succeed only if the test $m = 0$ is successful. In the right branch, the computation would then continue from the state $(j, 0, n)$ as required.

So we are left with the encoding of a zero test on the occurrences of a. This can be done with the goal $\underline{\mathsf{a}}$ provided it is only allowed to consume as many b's as it needs to or to substitute itself with the goal q_0 that succeeds if and only if $m = n = 0$. With the commands $\mathsf{b} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}})$ and $\mathsf{q}_0 \multimap \underline{\mathsf{a}}$, we would then obtain the following proofs:

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{b} \vdash \mathsf{b}}\langle \mathrm{Ax}\rangle \quad \dfrac{\text{repeat until } n = 0}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \underline{\mathsf{a}}}}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b}, \mathsf{b} \vdash \underline{\mathsf{a}}}\ \mathsf{b} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}}) \in \Sigma \qquad \dfrac{\dfrac{\text{succeeds iff } m = 0}{!\,\Sigma, m.\mathsf{a}, 0.\mathsf{b} \vdash \mathsf{q}_0}}{!\,\Sigma, m.\mathsf{a}, 0.\mathsf{b} \vdash \underline{\mathsf{a}}}\ \mathsf{q}_0 \multimap \underline{\mathsf{a}} \in \Sigma$$

the left proof being used repeatedly to exhaust all the b's, and then the right proof finishing the job with a test on emptiness, which in this case, would be reduced to a zero test on m.

So we have presented an overview of the main ideas that lead to an encoding of Minsky machines acceptance into the fragment eILL, at least for the soundness part. We organize these ideas in a formal proof in the coming sections. The completeness part could be obtained by reasoning on the shape of possible proofs using arguments based on goal positions, as sketched earlier. But, as we will see, it is much easier/quicker to obtain completeness through a (trivial) phase semantics interpretation as already remarked by Lafont [Lafont 1996; Lafont and Scedrov 1996].

5.2. Two counter Minsky machines

Let a and b be two distinct counter symbols. A (deterministic) two counter Minsky machine is a pair $\mathfrak{M} = (l, \psi)$ where $l > 0$ is a strictly positive natural *number of instructions* and

$$\psi : [1, l] \longrightarrow \{+\} \times \{\mathsf{a}, \mathsf{b}\} \times [0, l] \;\Big|\; \{-\} \times \{\mathsf{a}, \mathsf{b}\} \times [0, l] \times [0, l]$$

is a total map representing the *list of instructions*. Here, | represents the (disjoint) set sum. Minsky machine instructions (incrementation, zero test/decrementation) are encoded as illustrated in the following two examples:

$\psi(1) = (+, \mathsf{a}, 3) \leftrightsquigarrow$ `1: a:=a+1 ; goto 3`
$\psi(2) = (-, \mathsf{b}, 4, 5) \leftrightsquigarrow$ `2: if b=0 then goto 4 else b:=b-1 ; goto 5`

Given a two counter Minsky machine $\mathfrak{M} = (l, \psi)$, we define the set $\mathsf{S}(\mathfrak{M})$ of *states* of the machine by $\mathsf{S}(\mathfrak{M}) = [0, l] \times \mathbb{N} \times \mathbb{N}$ which collects the next instruction and the values of the counters a and b. With the following notations:

$$\overline{\mathsf{a}} = (1, 0) \qquad \overline{\mathsf{b}} = (0, 1) \qquad (m, n)_{\mathsf{a}} = m \qquad (m, n)_{\mathsf{b}} = n$$

we define a (binary) transition relation between states $\to_{\mathfrak{M}} \subseteq \mathsf{S}(\mathfrak{M}) \times \mathsf{S}(\mathfrak{M})$. For any two states (i, m, n) and (i', m', n'), the relation $(i, m, n) \to_{\mathfrak{M}} (i', m', n')$ holds if

$$\begin{aligned} & \psi(i) = (+, x, i') \text{ and } (m', n') = (m, n) + \overline{x} \\ \text{or } & \psi(i) = (-, x, i', k), (m, n)_x = 0 \text{ and } (m', n') = (m, n) \\ \text{or } & \psi(i) = (-, x, j, i'), (m, n)_x \neq 0 \text{ and } (m', n') + \overline{x} = (m, n) \end{aligned}$$

holds for some $x \in \{\mathsf{a}, \mathsf{b}\}$ and some $j, k \in [0, l]$. Notice that $(i, m, n) \to_{\mathfrak{M}} (i', m', n')$ does not hold if $i = 0$ because $\psi(0)$ is not defined. Let $\to^{\star}_{\mathfrak{M}}$ be the reflexive and transitive closure of the relation $\to_{\mathfrak{M}}$. We say that the machine $\mathfrak{M}$ *accepts* the input (m, n) if starting from the state $(1, m, n)$, there exists a sequence of transitions leading to the state $(0, 0, 0)$ and we define the set $\mathsf{A}(\mathfrak{M})$ of accepted inputs:

$$\mathsf{A}(\mathfrak{M}) = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid (1, m, n) \to^{\star}_{\mathfrak{M}} (0, 0, 0)\}$$

THEOREM 5.1 (MINSKY). *There exists a two counter Minsky machine $\mathfrak{M}$ for which the set $\mathsf{A}(\mathfrak{M})$ of accepted inputs is not recursive [Minsky 1961].*

5.3. The formal encoding of two counter Minsky machines

Let us consider the two counter symbols a and b as two (different) logical variables and let us choose two new variables $\underline{\mathsf{a}}$ and $\underline{\mathsf{b}}$ so that the set $\{\mathsf{a}, \mathsf{b}, \underline{\mathsf{a}}, \underline{\mathsf{b}}\} \subseteq \mathsf{Var}$ has cardinal four. Let us choose an infinite set[11] of new logical variables $\{\mathsf{q}_i \mid i \in \mathbb{N}\}$ such that $\mathsf{q}_i \neq \mathsf{q}_j$ unless $i = j$ and $\{\mathsf{a}, \mathsf{b}, \underline{\mathsf{a}}, \underline{\mathsf{b}}\} \cap \{\mathsf{q}_i \mid i \in$

[11] In fact, we only need as many q_i's as there are instructions in the Minsky machine obtained from Theorem 5.1.

$\mathbb{N}\} = \emptyset$. Let Σ_0 be the following multiset composed of five $(\multimap, \&)$-elementary formulae:

$$\Sigma_0 = \{(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0, \mathsf{b} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}}), \mathsf{q}_0 \multimap \underline{\mathsf{a}}, \mathsf{a} \multimap (\underline{\mathsf{b}} \multimap \underline{\mathsf{b}}), \mathsf{q}_0 \multimap \underline{\mathsf{b}}\}$$

Given a Minsky machine $\mathfrak{M} = (l, \psi)$, for $i \in [1, l]$, we define the multisets $\Sigma_1, \ldots, \Sigma_l$ of $(\multimap, \&)$-elementary formulae by:

$$\begin{array}{rll} & \Sigma_i = \{(x \multimap \mathsf{q}_j) \multimap \mathsf{q}_i\} & \text{when } \psi(i) = (+, x, j) \\ \text{and} & \Sigma_i = \{(\underline{x} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i, x \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)\} & \text{when } \psi(i) = (-, x, j, k) \end{array}$$

Let $\Sigma_{\mathfrak{M}}$ be the multiset $\Sigma_{\mathfrak{M}} = \Sigma_0, \Sigma_1, \ldots, \Sigma_l$. Given a natural number $n \in \mathbb{N}$ and a logical variable $x \in \{\mathsf{a}, \mathsf{b}\}$, we define $n.x = x, x, \ldots, x$ as the multiset composed of n occurrences of the variable x. For instance, the two identities $m.\mathsf{a}, n.\mathsf{a} = (m + n).\mathsf{a}$ and $1.\mathsf{a} = \mathsf{a}$ hold, and $0.\mathsf{a}$ (resp. $0.\mathsf{b}$) is equal to the empty multiset. Then, it is trivial to verify that for any natural numbers m, n and any $i \in [0, l]$, the sequent $!\,\Sigma_{\mathfrak{M}}, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ belongs to the fragment eILL.

Let us now consider a fixed Minsky machine $\mathfrak{M} = (l, \psi)$. Then we denote $\Sigma_{\mathfrak{M}}$ (resp. $\rightarrow_{\mathfrak{M}}$) simply by Σ (resp. $\rightarrow$). We prove four main intermediate results.

Proposition 5.2. *For any $m, n \in \mathbb{N}$, the sequents $!\,\Sigma, n.\mathsf{b} \vdash \underline{\mathsf{a}}$ and $!\,\Sigma, m.\mathsf{a} \vdash \underline{\mathsf{b}}$ have a proof in* G-eILL.

Proof. Here is a suitable proof tree for the case with $\mathsf{b}/\underline{\mathsf{a}}$, built by induction on n.

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{b} \vdash \mathsf{b}}\langle \mathrm{Ax}\rangle \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\langle \mathrm{Ax}\rangle}{!\,\Sigma \vdash \mathsf{q}_0}\,(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0 \in \Sigma}{!\,\Sigma \vdash \underline{\mathsf{a}}}\,\mathsf{q}_0 \multimap \underline{\mathsf{a}} \in \Sigma}{}}{}\,\mathsf{b} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}}) \in \Sigma$$

$$\vdots \;\; \text{applied } n - 1 \text{ times}$$

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{b} \vdash \mathsf{b}}\langle \mathrm{Ax}\rangle \qquad \dfrac{}{!\,\Sigma, (n-1).\mathsf{b} \vdash \underline{\mathsf{a}}}}{!\,\Sigma, n.\mathsf{b} \vdash \underline{\mathsf{a}}}\,\mathsf{b} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}}) \in \Sigma$$

The case of $\mathsf{a}/\underline{\mathsf{b}}$ is similar. Here is a suitable proof tree built by induction on m:

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\langle \mathrm{Ax}\rangle \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\langle \mathrm{Ax}\rangle}{!\,\Sigma \vdash \mathsf{q}_0}\,(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0 \in \Sigma}{!\,\Sigma \vdash \underline{\mathsf{b}}}\,\mathsf{q}_0 \multimap \underline{\mathsf{b}} \in \Sigma}{}}{}\,\mathsf{a} \multimap (\underline{\mathsf{b}} \multimap \underline{\mathsf{b}}) \in \Sigma$$

$$\vdots \;\; \text{applied } m - 1 \text{ times}$$

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\langle \mathrm{Ax}\rangle \qquad \dfrac{}{!\,\Sigma, (m-1).\mathsf{a} \vdash \underline{\mathsf{b}}}}{!\,\Sigma, m.\mathsf{a} \vdash \underline{\mathsf{b}}}\,\mathsf{a} \multimap (\underline{\mathsf{b}} \multimap \underline{\mathsf{b}}) \in \Sigma$$

In fact, these are the only possible proof trees but the demonstration of this uniqueness result is left to the reader. □

Lemma 5.3. *For any $r, m, n \in \mathbb{N}$ and any $i \in [0, l]$, if $(i, m, n) \rightarrow^r (0, 0, 0)$ then the sequent $!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ has a proof in* G-eILL.

Proof. We proceed by induction on the length r of the transition sequence $(i, m, n) \rightarrow^r (0, 0, 0)$ leading to the accepting state.

If $r = 0$ then we have $(i, m, n) = (0, 0, 0)$. The sequent $!\,\Sigma \vdash \mathsf{q}_0$ has the following proof tree:

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\,\langle \text{Ax} \rangle}{!\,\Sigma \vdash \mathsf{q}_0}\,(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0 \in \Sigma$$

Let us now consider a transition sequence $(i, m, n) \to (i', m', n') \to^r (0, 0, 0)$ of length $r + 1$. By the induction hypothesis, let P be a proof tree for the sequent $!\,\Sigma, m'.\mathsf{a}, n'.\mathsf{b} \vdash \mathsf{q}_{i'}$. We consider the 3×2 possible cases for $(i, m, n) \to (i', m', n')$.

— if $\psi(i) = (+, \mathsf{a}, i')$ and $(m', n') = (m, n) + \overline{\mathsf{a}}$. Then $m' = m + 1$ and $n' = n$. We provide the following proof tree for $!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{P}{!\,\Sigma, \mathsf{a}, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_{i'}}}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i}\,(\mathsf{a} \multimap \mathsf{q}_{i'}) \multimap \mathsf{q}_i \in \Sigma$$

— if $\psi(i) = (+, \mathsf{b}, i')$ and $(m', n') = (m, n) + \overline{\mathsf{b}}$. Then $m' = m$ and $n' = n + 1$. Here is a proof tree for $!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{P}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b}, \mathsf{b} \vdash \mathsf{q}_{i'}}}{!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i}\,(\mathsf{b} \multimap \mathsf{q}_{i'}) \multimap \mathsf{q}_i \in \Sigma$$

— if $\psi(i) = (-, \mathsf{a}, i', k)$, $(m, n)_\mathsf{a} = 0$ and $(m', n') = (m, n)$. Then $m = m' = 0$ and $n = n'$. Let Q be a proof tree for $!\,\Sigma, n.\mathsf{b} \vdash \underline{\mathsf{a}}$ according to Proposition 5.2. We provide the following proof tree for $!\,\Sigma, n.\mathsf{b} \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{Q}{!\,\Sigma, n.\mathsf{b} \vdash \underline{\mathsf{a}}} \quad \dfrac{P}{!\,\Sigma, n.\mathsf{b} \vdash \mathsf{q}_{i'}}}{!\,\Sigma, n.\mathsf{b} \vdash \mathsf{q}_i}\,(\underline{\mathsf{a}} \,\&\, \mathsf{q}_{i'}) \multimap \mathsf{q}_i \in \Sigma$$

— if $\psi(i) = (-, \mathsf{b}, i', k)$, $(m, n)_\mathsf{b} = 0$ and $(m', n') = (m, n)$. Then $m = m'$ and $n = n' = 0$. Let Q be a proof tree for $!\,\Sigma, m.\mathsf{a} \vdash \underline{\mathsf{b}}$ according to Proposition 5.2. Here is a proof tree for $!\,\Sigma, m.\mathsf{a} \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{Q}{!\,\Sigma, m.\mathsf{a} \vdash \underline{\mathsf{b}}} \quad \dfrac{P}{!\,\Sigma, m.\mathsf{a} \vdash \mathsf{q}_{i'}}}{!\,\Sigma, m.\mathsf{a} \vdash \mathsf{q}_i}\,(\underline{\mathsf{b}} \,\&\, \mathsf{q}_{i'}) \multimap \mathsf{q}_i \in \Sigma$$

— if $\psi(i) = (-, \mathsf{a}, j, i')$, $(m, n)_\mathsf{a} \neq 0$ and $(m', n') + \overline{\mathsf{a}} = (m, n)$. Then $m = m' + 1$ and $n = n'$. We provide the following proof tree for $!\,\Sigma, (m' + 1).\mathsf{a}, n'.\mathsf{b} \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\,\langle \text{Ax} \rangle \quad \dfrac{P}{!\,\Sigma, m'.\mathsf{a}, n'.\mathsf{b} \vdash \mathsf{q}_{i'}}}{!\,\Sigma, \mathsf{a}, m'.\mathsf{a}, n'.\mathsf{b} \vdash \mathsf{q}_i}\,\mathsf{a} \multimap (\mathsf{q}_{i'} \multimap \mathsf{q}_i) \in \Sigma$$

— if $\psi(i) = (-, \mathsf{b}, j, i')$, $(m, n)_\mathsf{b} \neq 0$ and $(m', n') + \overline{\mathsf{b}} = (m, n)$. Then $m' = m$ and $n' + 1 = n$. Here is a proof tree for $!\,\Sigma, m'.\mathsf{a}, (n' + 1).\mathsf{b} \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{b} \vdash \mathsf{b}}\,\langle \text{Ax} \rangle \quad \dfrac{P}{!\,\Sigma, m'.\mathsf{a}, n'.\mathsf{b} \vdash \mathsf{q}_{i'}}}{!\,\Sigma, m'.\mathsf{a}, n'.\mathsf{b}, \mathsf{b} \vdash \mathsf{q}_i}\,\mathsf{b} \multimap (\mathsf{q}_{i'} \multimap \mathsf{q}_i) \in \Sigma$$

In any case we obtain a proof tree for $!\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ which fulfills the induction step. Again, but this is left to the reader, it can be demonstrated that the proof tree recursively built from the transition sequence $(i, m, n) \to^r (0, 0, 0)$ is the unique proof tree for the sequent $!\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$. □

Let us now consider the following trivial phase semantics interpretation. Consider the product monoid $(\mathbb{N}\times\mathbb{N}, +, (0, 0))$. We define $x \circ y = \{x + y\}$ and thus $(\mathbb{N}\times\mathbb{N}, \circ, (0, 0))$ is a total deterministic monoid. Every subset of $\mathbb{N}\times\mathbb{N}$ is closed in trivial phase semantics and we define

$$[\![\mathsf{a}]\!] = \{(1, 0) = \overline{\mathsf{a}}\} \quad [\![\underline{\mathsf{a}}]\!] = \{0\}\times\mathbb{N} \quad [\![\mathsf{q}_i]\!] = \{(m, n) \in \mathbb{N}\times\mathbb{N} \mid (i, m, n) \to^\star (0, 0, 0)\}$$
$$[\![\mathsf{b}]\!] = \{(0, 1) = \overline{\mathsf{b}}\} \quad [\![\underline{\mathsf{b}}]\!] = \mathbb{N}\times\{0\}$$

It is crucial that variables $\mathsf{a}, \mathsf{b}, \underline{\mathsf{a}}, \underline{\mathsf{b}}, \mathsf{q}_0, \mathsf{q}_1, \ldots, \mathsf{q}_l$ were chosen distinct from one another for this definition to be valid. Let us now consider the trivial phase semantics interpretation of the elementary formulae of Σ.

Proposition 5.4. *For any $\sigma \in \Sigma$, $[\![!\,\sigma]\!] = \{(0, 0)\}$ holds.*

Proof. First, we remark that since there is no instruction at position 0, we have $(0, m, n) \to^\star (0, 0, 0)$ iff $(0, m, n) \to^0 (0, 0, 0)$ iff $m = n = 0$ and thus the identity $[\![\mathsf{q}_0]\!] = \{(0, 0)\}$ holds. Also, from the definition of $[\![\underline{x}]\!]$, we deduce $(m, n) \in [\![\underline{x}]\!]$ if and only if $(m, n)_x = 0$ for any $x \in \{\mathsf{a}, \mathsf{b}\}$. As the identity $[\![!\,\sigma]\!] = \{(0, 0)\} \cap [\![\sigma]\!]$ holds in trivial phase semantics, it is necessary and sufficient to prove that $(0, 0) \in [\![\sigma]\!]$ holds for any $\sigma \in \Sigma$.

Let us consider the formulae of $\Sigma_0 = \{(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0, \mathsf{b} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}}), \mathsf{q}_0 \multimap \underline{\mathsf{a}}, \mathsf{a} \multimap (\underline{\mathsf{b}} \multimap \underline{\mathsf{b}}), \mathsf{q}_0 \multimap \underline{\mathsf{b}}\}$. First let us prove that $[\![\mathsf{a} \multimap \mathsf{a}]\!] = \{(0, 0)\}$. Indeed, $(m, n) \in [\![\mathsf{a} \multimap \mathsf{a}]\!]$ iff $(m, n) \circ [\![\mathsf{a}]\!] \subseteq [\![\mathsf{a}]\!]$ iff $(m, n) \circ \{(1, 0)\} \subseteq \{(1, 0)\}$ iff $\{(m + 1, n)\} \subseteq \{(1, 0)\}$ iff $(m, n) = (0, 0)$. Since $[\![\mathsf{q}_0]\!] = \{(0, 0)\}$ holds, we compute $[\![(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0]\!] = \{(0, 0)\} \multimap \{(0, 0)\} = \{(0, 0)\}$. From $[\![\mathsf{q}_0]\!] = \{(0, 0)\}$ again, we compute $[\![\mathsf{q}_0 \multimap \underline{\mathsf{a}}]\!] = \{(0, 0)\} \multimap [\![\underline{\mathsf{a}}]\!] = [\![\underline{\mathsf{a}}]\!] = \{0\}\times\mathbb{N}$. By a similar argument, we get $[\![\mathsf{q}_0 \multimap \underline{\mathsf{b}}]\!] = \mathbb{N}\times\{0\}$. Also $(m, n) \in [\![\mathsf{b} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}})]\!]$ iff $(m, n) \circ \{(0, 1)\} \circ \{0\}\times\mathbb{N} \subseteq \{0\}\times\mathbb{N}$ iff $m = 0$. Thus $[\![\mathsf{b} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}})]\!] = \{0\}\times\mathbb{N}$. By a similar argument, we get $[\![\mathsf{a} \multimap (\underline{\mathsf{b}} \multimap \underline{\mathsf{b}})]\!] = \mathbb{N}\times\{0\}$. So for any formula $\sigma \in \Sigma_0$, we have the inclusion $(0, 0) \in [\![\sigma]\!]$.

Let us now consider the formulae in Σ_i for $i \in [1, l]$. Let us prove that the inclusion $(0, 0) \in [\![\sigma]\!]$ holds for any $\sigma \in \Sigma_i$ by case analysis:

— if $\psi(i) = (+, x, j)$ then $\Sigma_i = \{(x \multimap \mathsf{q}_j) \multimap \mathsf{q}_i\}$. Let us show $(0, 0) \in [\![(x \multimap \mathsf{q}_j) \multimap \mathsf{q}_i]\!]$, i.e. $[\![x \multimap \mathsf{q}_j]\!] \subseteq [\![\mathsf{q}_i]\!]$. Let us consider $(m, n) \in [\![x \multimap \mathsf{q}_j]\!]$. Then $\{(m, n) + \overline{x}\} = \{(m, n)\} \circ [\![x]\!] \subseteq [\![\mathsf{q}_j]\!]$ and thus $(m', n') = (m, n) + \overline{x} \in [\![\mathsf{q}_j]\!]$. Thus we have $(i, m, n) \to (j, m', n') \to^\star (0, 0, 0)$ and we conclude $(m, n) \in [\![\mathsf{q}_i]\!]$;
— if $\psi(i) = (-, x, j, k)$ then $\Sigma_i = \{(\underline{x} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i, x \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)\}$. Let us first show that $(0, 0) \in [\![(\underline{x} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i]\!]$, i.e. $[\![\underline{x}]\!] \cap [\![\mathsf{q}_j]\!] \subseteq [\![\mathsf{q}_i]\!]$. Let us consider $(m, n) \in [\![\underline{x}]\!] \cap [\![\mathsf{q}_j]\!]$. Then $(m, n)_x = 0$ and $(j, m, n) \to^\star (0, 0, 0)$. Thus $(i, m, n) \to (j, m, n) \to^\star (0, 0, 0)$ and the inclusion $(m, n) \in [\![\mathsf{q}_i]\!]$ holds. Hence $[\![\underline{x}]\!] \cap [\![\mathsf{q}_j]\!] \subseteq [\![\mathsf{q}_i]\!]$ holds.
Let us finally show that $(0, 0) \in [\![x \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)]\!]$, i.e. $[\![x]\!] \circ [\![\mathsf{q}_k]\!] \subseteq [\![\mathsf{q}_i]\!]$. As $[\![x]\!] = \{\overline{x}\}$, let us choose an arbitrary pair $(m', n') \in [\![\mathsf{q}_k]\!]$ and define $(m, n) = (m', n') + \overline{x}$. Then $(m, n)_x = (m', n')_x + 1 \neq 0$ and $(i, m, n) \to (k, m', n') \to^\star (0, 0, 0)$. We obtain $(m, n) \in [\![\mathsf{q}_i]\!]$ and thus conclude $\overline{x} + (m', n') = (m, n) \in [\![\mathsf{q}_i]\!]$. Hence, for any $(m', n') \in [\![\mathsf{q}_k]\!]$ we get $[\![x]\!] \circ (m', n') \subseteq [\![\mathsf{q}_i]\!]$. Thus $[\![x]\!] \circ [\![\mathsf{q}_k]\!] \subseteq [\![\mathsf{q}_i]\!]$ holds.

As a consequence, for any $\sigma \in \Sigma$, we obtain the inclusion $(0, 0) \in [\![\sigma]\!]$. The identity $[\![!\,\sigma]\!] = \{(0, 0)\}$ holds for any $\sigma \in \Sigma$. □

Lemma 5.5. *For any $i \in [0, l]$ and any $m, n \in \mathbb{N}$, if the sequent $!\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ has a proof in* G-eILL *then the relation $(i, m, n) \to^\star (0, 0, 0)$ holds.*

Proof. Let $\Sigma = \{\sigma_1, \ldots, \sigma_k\}$. We suppose that the sequent $!\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$ has a proof in G-eILL. By the soundness part of Theorem 4.4, in our particular total deterministic trivial phase semantics interpretation, we have

$$[\![!\,\sigma_1]\!] \circ \cdots \circ [\![!\,\sigma_k]\!] \circ [\![\mathsf{a}]\!] \circ \cdots \circ [\![\mathsf{a}]\!] \circ [\![\mathsf{b}]\!] \circ \cdots \circ [\![\mathsf{b}]\!] \subseteq [\![\mathsf{q}_i]\!]$$

where a occurs m times and b occurs n times. From the inclusions $(0,0) \in [\![!\,\sigma_j]\!]$ (Proposition 5.4), $(1,0) \in [\![\mathsf{a}]\!]$ and $(0,1) \in [\![\mathsf{b}]\!]$, we derive $(m,n) = k.(0,0) + m.(1,0) + n.(0,1) \in [\![\mathsf{q}_i]\!]$ and thus the relation $(i,m,n) \to^\star (0,0,0)$ holds. □

From Lemma 5.3 and Lemma 5.5, we obtain as a direct consequence the following theorem which characterizes Minsky machine acceptance in terms of provability in G-eILL.

Theorem 5.6. *For any two counter Minsky machine* $\mathfrak{M}$ *and for any pair* $m,n \in \mathbb{N}$*, we have* $(m,n) \in \mathsf{A}(\mathfrak{M})$ *if and only if the sequent* $!\,\Sigma_{\mathfrak{M}}, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_1$ *is provable in* G-eILL.

We point out that the form $(\&)\multimap$ is used here to encode *forking* in a way similar to how Kanovich does with $\oplus$ (see [Kanovich 1995]). The reader may have noticed that more than the simple encoding of computability with provability, we can even show that computations and proofs match one to one. Even though this result is not necessary to our argumentation, this suggests that the system G-eILL is a natural choice to illustrate the relations between Minsky machines and linear logic, and may be more straightforward than the $(!, \oplus)$-Horn fragment [Kanovich 1995].

5.4. The undecidability of eILL

Whereas the decidability of $\mathsf{s\text{-}IMELL}_0^{\multimap}$ is still unclear (but nevertheless known to be equivalent to the open and very difficult question of decidability of MELL [de Groote et al. 2004]), we have proved that the simple addition of the form $(\&)\multimap$ to $\mathsf{s\text{-}IMELL}_0^{\multimap}$ is sufficient to encode forking and thus computations of Minsky machines.

Theorem 5.7. *Validity is undecidable in the elementary fragment of* ILL.

Proof. By Theorem 5.1, there is a two counter Minsky machine $\mathfrak{M}$ such that $\mathsf{A}(\mathfrak{M})$ is not recursive. Let us compute $\Sigma_{\mathfrak{M}}$. If there is an algorithm that discriminates between provable and unprovable sequents of eILL, we use it to decide

$$\mathsf{A}(\mathfrak{M}) = \{(m,n) \in \mathbb{N} \times \mathbb{N} \mid !\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_1 \text{ is provable in G-eILL}\}$$

This identity is a direct consequence of Theorem 5.6. Thus $\mathsf{A}(\mathfrak{M})$ would be recursive. We obtain a contradiction. □

We point out that the model through which the faithfulness of the encoding is obtained (see Lemma 5.5) is based on the free monoid $\mathbb{N} \times \mathbb{N}$. With $\mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$ denoting the set of sequents which are valid in every trivial phase semantic interpretation over the free monoid $(\mathbb{N} \times \mathbb{N}, +, (0,0))$, we obtain the following "stronger" result:

Theorem 5.8. $\mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$ *is not a recursive set of sequents.*

Proof. It is sufficient to prove the following equivalence:

$$(m,n) \in \mathsf{A}(\mathfrak{M}) \quad \text{iff} \quad !\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_1 \text{ belongs to } \mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$$

For the *if part*, if $!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_1$ belongs to $\mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$ then we deduce that $(m,n) \in \mathsf{A}(\mathfrak{M})$, using the *same proof* as in Lemma 5.5. For the *only if part*, if $(m,n) \in \mathsf{A}(\mathfrak{M})$, then by Lemma 5.3, we obtain that $!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_1$ is provable in G-eILL. Thus, by definition, it belongs to eILL_p, and as a consequence of Theorem 4.4, the sequent $!\,\Sigma, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_1$ belongs to $\mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$. □

Remark: we leave the question of the strictness of the inclusion $\mathsf{eILL}_p \subseteq \mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$ as a remaining open problem.

5.5. Comparison with other encodings of Minsky machines

In this section, we discuss the similarities and the differences that exist between our own encoding of Minsky machines in the eILL fragment and some other encodings of Minsky machines either in (fragments of) linear logic like those of Kanovich [Kanovich 1994; 1995] and Lafont [Lafont 1996], but more specifically, between our encoding and the one of Brotherston and Kanovich [Brotherston and Kanovich 2010] in the minimal fragment of Boolean BI and separation logic.

All the previously cited encodings relate acceptance of a state (i,m,n) of a (say) two counter Minsky machine to the provability of a sequent/formula in a given logic. We remark that the initial work of Kanovich [Kanovich 1995] was strongly influenced by the encoding of Petri nets [Reisig 1985] in linear logic [Martí-Oliet and Meseguer 1991]. In a Petri net N, the state is represented by the number of tokens on each place, i.e. by a multiset m of places. Basically, the list of transitions of the Petri net N is associated to a sequence Σ_N of formulae and the state $\mathsf{m} = m_1.\mathsf{p}_1 + \cdots + m_k.\mathsf{p}_k$ is associated to the formula $\mathsf{p}_1^{m_1} \otimes \cdots \otimes \mathsf{p}_k^{m_k}$. The following equivalence holds: the state n is reachable from the state m in the Petri net N (denoted $\mathsf{m} \to_N^\star \mathsf{n}$) if and only if the sequent

$$!\,\Sigma_N, \mathsf{p}_1^{m_1} \otimes \cdots \otimes \mathsf{p}_k^{m_k} \vdash \mathsf{p}_1^{n_1} \otimes \cdots \otimes \mathsf{p}_k^{n_k}$$

has a proof in (some fragment of) linear logic.

In his encoding [Kanovich 1995], Kanovich chooses to encode the state (i,m,n) of (two counter) Minsky machines by the formula $\mathsf{q}_i \otimes \mathsf{a}^m \otimes \mathsf{b}^n$ where q_i represents a formula of linear logic uniquely associated to the position i in the Minsky machine. The list of instructions of a Minsky machine $\mathfrak{M}$ is associated to a sequence $\Sigma_{\mathfrak{M}}$ of formulae in the $(!,\oplus)$-Horn fragment of linear logic, and Kanovich obtains the following characterization: the state (i,m,n) is accepted by $\mathfrak{M}$ (i.e. the relation $(i,m,n) \to_{\mathfrak{M}}^\star (0,0,0)$ holds) if and only if the sequent

$$!\,\Sigma_{\mathfrak{M}}, \mathsf{q}_i \otimes \mathsf{a}^m \otimes \mathsf{b}^n \vdash \mathsf{q}_0 \otimes \mathsf{a}^0 \otimes \mathsf{b}^0$$

has a proof in linear logic. We point out that only acceptance is encoded (as opposed to the more general notion of reachability). However, the formulation is similar to the characterization of reachability for Petri nets. We also point out that the completeness of the encoding is obtained through some specific kind of proof normalization: proofs can be normalized and each normal proof contains the trace of a computation of the machine $\mathfrak{M}$.

The encoding of Lafont [Lafont 1996] is based on the encoding of Kanovich but the linear exponential $!\,X$ is replaced by $1 \,\&\, X$. Moreover, the completeness of the encoding was obtained through a phase semantic argument instead of proof normalization because at that time, normalization of second order linear logic was an open problem.[12] Our own phase semantics argument was inspired by the one of Lafont except that it is done in the restricted framework of trivial phase semantics, remarking that in trivial phase semantics, the exponential $!\,X$ behaves exactly as $1 \,\&\, X$ (see Equation (3) in Section 3.2). The fact that $\mathsf{I} \wedge X$ behaves as an exponential in Boolean BI is also pointed out in [Brotherston and Kanovich 2010] (see Lemma 2.2). We remark that this property does not hold in the case of (intuitionistic) BI which is one of the reasons why our own encoding or the encoding of Brotherston and Kanovich cannot be adapted to the intuitionistic version of BI.

In the case of the encoding of [Brotherston and Kanovich 2010], we would say that it is similar to the original one of [Kanovich 1995] except that it is done in a fragment of Boolean BI instead of linear logic. Double "magic wand" negation $(A \mathrel{-\!\!*} b) \mathrel{-\!\!*} b$ is used to simulate the $\oplus$ connective of the $(!,\oplus)$-Horn fragment linear logic using the $\vee$ connective of Boolean BI. This corresponds to the phase semantic equation

$$[\![A \oplus B]\!] = \big([\![A]\!] \cup [\![B]\!]\big)^{\perp\perp} = \big([\![A \vee B]\!] \multimap [\![b]\!]\big) \multimap [\![b]\!]$$

[12] Okada [Okada 2002] later proved that cut-elimination/normalization itself can be obtained through a phase semantics argument (see Appendix B).

whenever $[\![b]\!]$ is chosen equal to $[\![\bot]\!]$. The real difference between [Kanovich 1995] and [Brotherston and Kanovich 2010] lies much more in the completeness argument for the encoding which, in the later case, is a semantic one. It is based on a model which suits for Boolean BI but also and mainly for separation logic: the RAM-domain model $\mathbb{P}_f(\mathbb{N})$. We believe and argue in Sections 7.3 and 7.4 that the completeness proof of [Brotherston and Kanovich 2010] would be much simpler if it were based on the model $\mathbb{N} \times \mathbb{N}$ like in our own completeness proof. However, $\mathbb{N} \times \mathbb{N}$ is a model of BBI but not a model of separation logic, which justifies their focus on the RAM-domain model.

To make a syntactic comparison of our own encoding with the one of [Brotherston and Kanovich 2010], we remark that we were less influenced by the encoding of Petri nets reachability inherited from [Kanovich 1995]. Specifically, we do not encode the state (i, m, n) with the formula $\mathsf{q}_i \otimes \mathsf{a}^m \otimes \mathsf{b}^n$. On the contrary, we separate the encoding of the position i which occurs in the right of the $\vdash$ sign from the encoding of the counters which occurs on the left of the $\vdash$ sign in the sequent

$$! \, \Sigma_{\mathfrak{M}}, m.\mathsf{a}, n.\mathsf{b} \vdash \mathsf{q}_i$$

But since only acceptance (as opposed to reachability) is needed to derive undecidability, this change turned out not to be a big problem. The idea to separate q_i and $\mathsf{a}^m \otimes \mathsf{b}^n$ was suggested by the encoding of vector addition tree automata in the fragment $\mathsf{s\text{-}IMELL}_0^{\multimap}$ of ILL [de Groote et al. 2004]. As a result, we defined the elementary fragment eILL of ILL which extends $\mathsf{s\text{-}IMELL}_0^{\multimap}$ with the form $(\&)\multimap$. We believe that the elementary fragment together with trivial phase semantics is, so far, among the simplest logical frameworks in which an encoding of Minsky machines acceptance has be formulated.

6. THE SEMANTICS OF BOOLEAN BI

Boolean BI (denoted BBI) is the variant of intuitionistic BI [O'Hearn and Pym 1999] where the additive connectives are interpreted as Boolean connectives, contrary to (intuitionistic) BI where the additive connectives are interpreted as in propositional intuitionistic logic. The linear connectives are interpreted as those of multiplicative intuitionistic linear logic, i.e. the multiplicative fragment of ILL. When the connectives of BBI are given a Kripke semantics (see Section 6.1) and the model belongs to the class of heap monoids HM or the class of separation algebras SA, then we recover the logic that serves as the assertion language of (propositional) separation logic [Ishtiaq and O'Hearn 2001].

Informally, Boolean BI is an extension of classical propositional logic (hence the prefix Boolean) which should not be confused with Classical BI [Brotherston and Calcagno 2009]. Boolean BI has only an additive negation whereas Classical BI has both an additive and a multiplicative negation. Classical propositional logic consists of the additive fragment $\wedge$, $\vee$, $\rightarrow$ and $\neg$ of BBI. We insist on the fact that the additive implication $A \rightarrow B$ is equivalent to $\neg A \vee B$, contrary to what happens in (intuitionistic) BI and intuitionistic logic. The multiplicative fragment $*$ and $-\!\!*$ of BBI is composed of connectives similar to those of intuitionistic linear logic. The Kripke interpretation of the multiplicative conjunction is given by

$$m \Vdash A * B \quad \text{iff} \quad \text{there exist } a, b \text{ such that } a \circ b \triangleright m \text{ and } a \Vdash A \text{ and } b \Vdash B$$

where ternary relation $- \circ - \triangleright -$ has different interpretations depending on various semantic frameworks: $a \circ b \triangleright m$ reads either as m is a result of the composition of a and b, or as m can be decomposed into a and b. We show in [Galmiche and Larchey-Wendling 2006] that the interpretation $m \in a \circ b$ in a non-deterministic monoid provides a complete semantics for the Hilbert proof-system corresponding to BBI, which is that of (intuitionistic) BI augmented with the axiom $\neg\neg A \rightarrow A$. This semantics is also complete for the Display style proof-system of [Brotherston 2010]. When BBI is used as a language to express properties of models of memory heaps (i.e. separation logic models), the relation $a \circ b \triangleright m$ is interpreted by $m = a \circ b$ in a particular partial (deterministic) monoid of class HM, hence a restriction of the non-deterministic interpretation. As shown in Section 6.2, the non-deterministic interpretation and the restricted partial deterministic interpretation do not define the same set of (universally) valid formulae.

Formally, the syntax of BBI is exactly the syntax of BI augmented with negation, although negation could be defined by $\neg A = A \rightarrow \bot$ like in classical logic. Thus, the formulae of BBI are defined as follows. Starting from a set Var, they are freely built using the *logical variables* in Var, the *logical constants* in $\{\mathsf{I}, \top, \bot\}$, the unary connective $\neg$ or the binary connectives in $\{*, -\!\!*, \wedge, \vee, \rightarrow\}$. Formally, the set of formulae is denoted Form and described by the following grammar:

$$\mathsf{Form}: \quad A ::= v \mid c \mid \neg A \mid A \circledast A \quad \text{with } v \in \mathsf{Var}, c \in \{\mathsf{I}, \top, \bot\} \text{ and } \circledast \in \{*, -\!\!*, \wedge, \vee, \rightarrow\}$$

Validity in BBI has not always been unequivocally defined. Indeed, the initial proposition of Pym [Pym 2002] was simply to add a double negation principle to the cut-free bunched proof system of BI. But of course, this does not lead to a proof-theoretically well behaved proof-system for BBI: it does not enjoy cut-elimination, sub-formula property, etc. Then, the syntax of BBI has been used as a foundation for numerous variants of separation logic with the common property that the additive operator $\rightarrow$ is interpreted point-wise/classically whereas it is interpreted intuitionistically in BI [Ishtiaq and O'Hearn 2001; Calcagno et al. 2005]. The removal of the pre-order in the Kripke semantics is moreover necessary for the interpretation of classical negation $\neg$.

6.1. Kripke Semantics for BBI

In this paper, we choose to present BBI as a family of logics defined by their Kripke semantics rather than proof-systems. Given a non-deterministic monoid $(\mathsf{M}, \circ, \epsilon)$ and an interpretation of propositional variables $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$, we define the binary Kripke forcing relation $\Vdash_\delta \subseteq \mathsf{M} \times \mathsf{Form}$ by induction on the structure of BBI-formulae:

$$\begin{array}{rcl@{\qquad}rcl}
m \Vdash_\delta \bot & \text{iff} & \text{never} & m \Vdash_\delta A \vee B & \text{iff} & m \Vdash_\delta A \text{ or } m \Vdash_\delta B \\
m \Vdash_\delta \top & \text{iff} & \text{always} & m \Vdash_\delta A \wedge B & \text{iff} & m \Vdash_\delta A \text{ and } m \Vdash_\delta B \\
m \Vdash_\delta \neg A & \text{iff} & m \nVdash_\delta A & m \Vdash_\delta A \rightarrow B & \text{iff} & m \nVdash_\delta A \text{ or } m \Vdash_\delta B \\
m \Vdash_\delta \mathsf{I} & \text{iff} & m = \epsilon & m \Vdash_\delta A * B & \text{iff} & \exists a, b,\ m \in a \circ b \text{ and } a \Vdash_\delta A \text{ and } b \Vdash_\delta B \\
m \Vdash_\delta v & \text{iff} & m \in \delta(v) & m \Vdash_\delta A -\!\!* B & \text{iff} & \forall a, b\ (b \in a \circ m \text{ and } a \Vdash_\delta A) \Rightarrow b \Vdash_\delta B
\end{array}$$

This formulation of the Kripke semantics of BBI may seem unnatural to the reader but this really is a generalization of the standard partial monoidal Kripke semantics (of say separation logic) to the case of non-deterministic monoids. Indeed, if the monoid $(\mathsf{M}, \circ, \epsilon)$ belongs to the class PD of partial deterministic monoids, then the relation $m \in a \circ b$ is equivalent to $a \circ b = \{m\}$ which reads as "the composition of a and b is defined and equal to m." This non-deterministic semantics has already been used in [Galmiche and Larchey-Wendling 2006] for BBI and in [Brotherston and Calcagno 2009] for Classical BI. Beware also that the Kripke semantics of the (additive) implication is point-wise/Boolean which contrast with the case of (intuitionistic) BI where the interpretation of the (additive) implication requires a pre-order as in the Kripke semantics of intuitionistic logic. We invite the reader to consult [Larchey-Wendling and Galmiche 2009] for an in-depth study of the relations between (intuitionistic) BI and Boolean BI.

Definition 6.1. A formula F is *valid* in a non-deterministic monoid $(\mathsf{M}, \circ, \epsilon)$ if for any interpretation $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$ of propositional variables, the relation $m \Vdash_\delta F$ holds for any $m \in \mathsf{M}$. A *counter-model* of the formula F is given by a non-deterministic monoid $(\mathsf{M}, \circ, \epsilon)$, an interpretation $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$ and an element $m \in \mathsf{M}$ such that $m \nVdash_\delta F$.

When the interpretation of variables is obvious from the context, we may simply omit the δ subscript and write $\Vdash$ instead of $\Vdash_\delta$. In some papers, BBI is defined by non-deterministic monoidal Kripke semantics [Brotherston 2010; Galmiche and Larchey-Wendling 2006]; in other papers it is defined by partial but deterministic monoidal Kripke semantics [Larchey-Wendling and Galmiche 2009] and generally (abstract) separation logic models are particular instances of partial (deterministic) monoids.

Definition 6.2. We denote by BBI_X the set of formulae of BBI which are valid in every (non-deterministic) monoid of the class X.

On the proof-theoretic side, we briefly recall that $\mathsf{BBI}_{\mathrm{ND}}$ has been proved sound and complete w.r.t. a Hilbert proof-system [Galmiche and Larchey-Wendling 2006] and also, more recently w.r.t. a Display logic based proof-system [Brotherston 2010] enjoying cut-elimination. $\mathsf{BBI}_{\mathrm{PD}}$ can be proved sound and complete w.r.t. the semantic constraints based tableaux proof-system presented in [Larchey-Wendling and Galmiche 2009] (although only the soundness proof is presented in that particular paper) and the adaptation of this tableaux system to $\mathsf{BBI}_{\mathrm{TD}}$ should be straightforward (contrary to $\mathsf{BBI}_{\mathrm{ND}}$). We view the problem of designing sound and complete proof-systems for $\mathsf{BBI}_{\mathrm{HM}}$ or $\mathsf{BBI}_{\mathrm{SA}}$ to be a difficult one.

6.2. Different versions of BBI

As it turns out, the three different classes of models ND, PD and TD define three different logics, i.e. universally valid formulae differ from one class of models to another. The relation of *strict inclusion* between $\mathsf{BBI}_{\mathrm{ND}}$ and $\mathsf{BBI}_{\mathrm{PD}}$ was, to our knowledge, an undecided proposition.

THEOREM 6.3. $\mathsf{BBI}_{\mathrm{ND}} \subsetneq \mathsf{BBI}_{\mathrm{PD}} \subsetneq \mathsf{BBI}_{\mathrm{TD}}$

PROOF. The inclusion relations TD $\subseteq$ PD $\subseteq$ ND hold between the classes of models which respectively define those three logics. Hence, only the strictness of the inclusion of validities is not obvious. This strictness is established by upcoming Theorem 6.4 and Proposition 6.5. □

Consider the formula $\mathcal{I} = \neg(\top \twoheadrightarrow \neg \mathsf{I})$ and a non-deterministic monoid $(M, \circ, \epsilon)$. Since $\mathcal{I}$ does not contain any variable, its Kripke interpretation does not depend on the choice of δ. One can check that for any $x \in M$, $x \Vdash \mathcal{I}$ iff there exists $x' \in M$ s.t. $\epsilon \in x \circ x'$. So $\mathcal{I}$ expresses "invertibility" in Kripke semantics. The formula $(\mathcal{I} * \mathcal{I}) \to \mathcal{I}$ expresses stability of invertibility by monoidal composition.

THEOREM 6.4. *With $\mathcal{I} = \neg(\top \twoheadrightarrow \neg \mathsf{I})$, the formula $(\mathcal{I} * \mathcal{I}) \to \mathcal{I}$ is valid in every partial deterministic monoid. There exists a non-deterministic monoid which is a counter-model to $(\mathcal{I} * \mathcal{I}) \to \mathcal{I}$.*

PROOF. First the counter-model. Consider the non-deterministic monoid $(\{\epsilon, \mathtt{x}, \mathtt{y}\}, \circ, \epsilon)$ uniquely defined by $\mathtt{x} \circ \mathtt{x} = \{\epsilon, \mathtt{y}\}$, $\mathtt{y} \circ \alpha = \{\mathtt{y}\}$ for any $\alpha \in \{\epsilon, \mathtt{x}, \mathtt{y}\}$ and the axioms 1 & 2 of Definition 2.1.[13] Then $\mathtt{x} \Vdash \mathcal{I}$ because there exists α ($\alpha = \mathtt{x}$) such that $\epsilon \in \mathtt{x} \circ \alpha$. On the other hand, $\mathtt{y} \nVdash \mathcal{I}$ because there is no α such that $\epsilon \in \mathtt{y} \circ \alpha$ holds. So, as $\mathtt{y} \in \mathtt{x} \circ \mathtt{x}$, we have $\mathtt{y} \Vdash \mathcal{I} * \mathcal{I}$. Thus $\mathtt{y} \nVdash (\mathcal{I} * \mathcal{I}) \to \mathcal{I}$.

Now let us prove that $(\mathcal{I} * \mathcal{I}) \to \mathcal{I}$ is valid in every partial deterministic monoid. Let $(\mathsf{M}, \circ, \epsilon)$ be a partial deterministic monoid. Let us choose $a \in \mathsf{M}$ and let us prove that $a \Vdash (\mathcal{I} * \mathcal{I}) \to \mathcal{I}$. So we suppose $a \Vdash \mathcal{I} * \mathcal{I}$ holds and we have to prove $a \Vdash \mathcal{I}$. As $a \Vdash \mathcal{I} * \mathcal{I}$, there exist $b, c \in \mathsf{M}$ such that $a \in b \circ c$, $b \Vdash \mathcal{I}$ and $c \Vdash \mathcal{I}$. Thus there exist $b', c' \in \mathsf{M}$ such that $\epsilon \in b \circ b'$ and $\epsilon \in c \circ c'$. As M is (partial) deterministic, we have $b \circ b' = \{\epsilon\}$, $c \circ c' = \{\epsilon\}$ and $b \circ c = \{a\}$. Thus we have $(b \circ b') \circ (c \circ c') = \{\epsilon\} \circ \{\epsilon\} = \{\epsilon\}$.

If $b' \circ c' = \emptyset$ then we would have $(b \circ c) \circ (b' \circ c') = \{a\} \circ \emptyset = \emptyset$ but also $(b \circ b') \circ (c \circ c') = \{\epsilon\}$ and thus $\emptyset = \{\epsilon\}$ by associativity/commutativity, which is absurd. Thus $b' \circ c' = \{a'\}$ and we obtain $(b \circ c) \circ (b' \circ c') = \{a\} \circ \{a'\} = a \circ a'$ and then $a \circ a' = \{\epsilon\}$ by associativity/commutativity. Hence, $\epsilon \in a \circ a'$ and $a \Vdash \mathcal{I}$. □

The formula $(\neg \mathsf{I} \twoheadrightarrow \bot) \to \mathsf{I}$ is inspired by the example given to establish the incompleteness of (total) monoidal Kripke semantics w.r.t. (intuitionistic) BI (see [Pym 2002] page 63).

PROPOSITION 6.5. *The formula $(\neg \mathsf{I} \twoheadrightarrow \bot) \to \mathsf{I}$ is valid in every total deterministic monoid. There exists a partial deterministic monoid which is a counter-model to $(\neg \mathsf{I} \twoheadrightarrow \bot) \to \mathsf{I}$.*

PROOF. First the counter-model. Consider the following partial deterministic monoid $(\{\epsilon, \mathtt{x}\}, \circ, \epsilon)$ where $\mathtt{x} \circ \mathtt{x} = \emptyset$ and $\epsilon \circ \alpha = \alpha \circ \epsilon = \{\alpha\}$ for any $\alpha \in \{\epsilon, \mathtt{x}\}$. Then $\mathtt{x} \neq \epsilon$ and thus $\mathtt{x} \nVdash \mathsf{I}$. Let us prove that $\mathtt{x} \Vdash \neg \mathsf{I} \twoheadrightarrow \bot$. Let a, b such that $b \in \mathtt{x} \circ a$ and $a \Vdash \neg \mathsf{I}$. Then $a \neq \epsilon$ and thus $a = \mathtt{x}$. Then $\mathtt{x} \circ a = \mathtt{x} \circ \mathtt{x} = \emptyset$. We get a contradiction with $b \in \mathtt{x} \circ a$. From this contradiction, we deduce $b \Vdash \bot$. Hence, $\mathtt{x} \Vdash \neg \mathsf{I} \twoheadrightarrow \bot$ and we conclude $\mathtt{x} \nVdash (\neg \mathsf{I} \twoheadrightarrow \bot) \to \mathsf{I}$ and we have the counter-model.

[13] This non-deterministic monoid was presented in Section 2.2 as a witness that the class ND is strictly larger than PD.

Now let us prove that $(\neg \mathsf{I} \twoheadrightarrow \bot) \to \mathsf{I}$ is valid in every total deterministic monoid. Let $(\mathsf{M}, \circ, \epsilon)$ be a total deterministic monoid. Let us choose $a \in \mathsf{M}$. There are two cases. Either $a = \epsilon$ or $a \neq \epsilon$. In the case $a = \epsilon$, we obviously have $a \Vdash (\neg \mathsf{I} \twoheadrightarrow \bot) \to \mathsf{I}$. In the case $a \neq \epsilon$, let us prove $a \nVdash \neg \mathsf{I} \twoheadrightarrow \bot$. Suppose $a \Vdash \neg \mathsf{I} \twoheadrightarrow \bot$. As $a \neq \epsilon$ we have $a \Vdash \neg \mathsf{I}$. Also $a \circ a$ is not empty because $\circ$ is total. Let $b \in a \circ a$. As $a \Vdash \neg \mathsf{I} \twoheadrightarrow \bot$, $b \in a \circ a$ and $a \Vdash \neg \mathsf{I}$, we must have $b \Vdash \bot$ which is impossible. Hence $a \nVdash \neg \mathsf{I} \twoheadrightarrow \bot$ and we conclude that $a \Vdash (\neg \mathsf{I} \twoheadrightarrow \bot) \to \mathsf{I}$ holds also in the case $a \neq \epsilon$. $\square$

Remark: the counter-examples of Theorem 6.4 and Proposition 6.5 have no impact on the inclusion sequence $\mathsf{ILL}^t_{\mathrm{ND}} \subseteq \mathsf{ILL}^t_{\mathrm{PD}} \subseteq \mathsf{ILL}^t_{\mathrm{TD}}$ of which the strictness or not remains an open question: indeed, the formulae $(\mathcal{I} * \mathcal{I}) \to \mathcal{I}$ and $(\neg \mathsf{I} \twoheadrightarrow \bot) \to \mathsf{I}$ cannot be transposed to ILL because both contain Boolean negations.

7. THE UNDECIDABILITY OF BOOLEAN BI

Having defined the Kripke semantics of BBI within the framework of non-deterministic monoids, let us establish precisely its relations with non-deterministic trivial phase semantics for ILL.

7.1. Trivial Phase vs. Kripke Semantics

Let us compare the trivial phase semantic interpretation of ILL connectives and the Kripke interpretation of BBI connectives. Given a non-deterministic monoid $\mathcal{M} = (\mathsf{M}, \circ, \epsilon)$, a trivial phase semantic interpretation $[\![\cdot]\!]^t : \mathsf{Var} \longrightarrow \mathcal{M}^\diamond$ and an interpretation of variables in Kripke semantics $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$, we compare the trivial phase semantic interpretation of ILL-formulae and the Kripke interpretation of BBI-formulae. Recall that in trivial phase semantics all subsets of M are closed and thus $\mathcal{M}^\diamond = \mathbb{P}(\mathsf{M})$. To better compare the two semantics, we use the notation

$$[\![F]\!]^k = \{m \mid m \Vdash F\}$$

Then, using the equations defining Kripke semantics (see Section 6.1), we easily obtain the following correspondence between the interpretations of ILL and BBI connectives:

		$[\![!\,A]\!]^t = \{\epsilon\} \cap [\![A]\!]^t$	$[\![\mathsf{I} \wedge A]\!]^k = \{\epsilon\} \cap [\![A]\!]^k$
$[\![\bot]\!]^t = \emptyset$	$[\![\bot]\!]^k = \emptyset$	$[\![A \oplus B]\!]^t = [\![A]\!]^t \cup [\![B]\!]^t$	$[\![A \vee B]\!]^k = [\![A]\!]^k \cup [\![B]\!]^k$
$[\![\top]\!]^t = \mathsf{M}$	$[\![\top]\!]^k = \mathsf{M}$	$[\![A \,\&\, B]\!]^t = [\![A]\!]^t \cap [\![B]\!]^t$	$[\![A \wedge B]\!]^k = [\![A]\!]^k \cap [\![B]\!]^k$
$[\![1]\!]^t = \{\epsilon\}$	$[\![\mathsf{I}]\!]^k = \{\epsilon\}$	$[\![A \otimes B]\!]^t = [\![A]\!]^t \circ [\![B]\!]^t$	$[\![A * B]\!]^k = [\![A]\!]^k \circ [\![B]\!]^k$
		$[\![A \multimap B]\!]^t = [\![A]\!]^t \multimap [\![B]\!]^t$	$[\![A \twoheadrightarrow B]\!]^k = [\![A]\!]^k \multimap [\![B]\!]^k$

Thus, there is an obvious embedding of the connectives of ILL into BBI, which can be formalized with the following inductively defined map $(\cdot)^\circledast : \mathsf{ILL} \longrightarrow \mathsf{BBI}$:

$$\begin{array}{rlrl}
v^\circledast &= v \quad \text{for } v \in \mathsf{Var} & & \\
\bot^\circledast &= \bot & (A \oplus B)^\circledast &= A^\circledast \vee B^\circledast \\
\top^\circledast &= \top & (A \,\&\, B)^\circledast &= A^\circledast \wedge B^\circledast \\
1^\circledast &= \mathsf{I} & (A \otimes B)^\circledast &= A^\circledast * B^\circledast \\
(!\,A)^\circledast &= \mathsf{I} \wedge A^\circledast & (A \multimap B)^\circledast &= A^\circledast \twoheadrightarrow B^\circledast
\end{array}$$

LEMMA 7.1. *If the trivial phase semantics interpretation* $[\![\cdot]\!] : \mathsf{Var} \longrightarrow \mathcal{M}^\diamond$ *and the Kripke interpretation* $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$ *are identical maps then the trivial phase semantics and the Kripke semantics are in the following relation for any* ILL*-formula* F *and any* $m \in \mathsf{M}$*:*

$$m \in [\![F]\!] \quad \textit{iff} \quad m \Vdash_\delta F^\circledast \tag{4}$$

PROOF. Using the previous notations $[\![\cdot]\!]^t$ and $[\![\cdot]\!]^k$, we show that $[\![F]\!]^t = [\![F^\circledast]\!]^k$ by induction on the structure of F. We consider the case $F = A \otimes B$ as a typical example. Using the inductions hypotheses $[\![A]\!]^t = [\![A^\circledast]\!]^k$ and $[\![B]\!]^t = [\![B^\circledast]\!]^k$, we compute $[\![A \otimes B]\!]^t = [\![A]\!]^t \circ [\![B]\!]^t = [\![A^\circledast]\!]^k \circ [\![B^\circledast]\!]^k = [\![A^\circledast * B^\circledast]\!]^k = [\![(A \otimes B)^\circledast]\!]^k$. $\square$

So if the interpretation of logical variables coincide, trivial phase semantics and Kripke semantics correspond to each other through the map $(\cdot)^{\circledast}$. Given a *sequence* $A_1, \ldots, A_k$ of formulae of ILL, we define $(A_1, \ldots, A_k)^{\circledast}$ by structural induction:

$$()^{\circledast} = \mathsf{I} \qquad (A_1, \ldots, A_{k+1})^{\circledast} = A_1^{\circledast} * (A_2, \ldots, A_{k+1})^{\circledast}$$

When $[\![\cdot]\!]$ and δ are identical maps on propositional variables, it is then straightforward to prove this equivalence by induction on k:

$$m \in [\![A_1]\!] \circ \cdots \circ [\![A_k]\!] \quad \text{iff} \quad m \Vdash (A_1, \ldots, A_k)^{\circledast} \tag{5}$$

7.2. Faithfully embedding (trivial) ILL into BBI

We define a reverse map from multisets of formulae of ILL into lists of formulae by choosing an arbitrary *decidable total order* among the formulae of ILL (e.g. lexicographic ordering). For any multiset Γ of formulae of ILL, there exists a unique and computable ordered sequence of formulae $A_1, \ldots, A_k$ such that $\Gamma = \{A_1, \ldots, A_k\}$ and we define $\Gamma^{\circledast} = (A_1, \ldots, A_k)^{\circledast}$.

Proposition 7.2. *The function* $(\cdot)^{\circledast} : \mathsf{ILL} \longrightarrow \mathsf{BBI}$ *mapping the* ILL*-sequent* $\Gamma \vdash C$ *to the* BBI*-formula* $\Gamma^{\circledast} \to C^{\circledast}$ *is a computable map from sequents of* ILL *to formulae of* BBI*.*

Proof. The only thing to prove here is that the map is computable and this is done using any sorting algorithm based on the decidable total order previously chosen. □

Proposition 7.3. *Let* $\mathcal{M} = (\mathsf{M}, \circ, \epsilon)$ *be a non-deterministic monoid. Let* $\Gamma \vdash C$ *be a sequent of* ILL*. Then the sequent* $\Gamma \vdash C$ *is valid in every trivial phase semantics interpretation based on* $\mathcal{M}$ *if and only if the formula* $\Gamma^{\circledast} \to C^{\circledast}$ *is valid in every Kripke interpretation based on* $\mathcal{M}$*.*

Proof. Let us pick the ordered sequence $A_1, \ldots, A_k$ such that the identity $\Gamma = \lfloor A_1, \ldots, A_k \rfloor$ holds as a multiset equation. Let us first suppose that $A_1, \ldots, A_k \vdash C$ is valid in every trivial phase semantics interpretation based on $\mathcal{M}$. Let $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$ be a Kripke interpretation of variables in the model $\mathcal{M}$. We choose the trivial phase semantics interpretation $[\![\cdot]\!] : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$ defined by $[\![v]\!] = \delta(v)$ for any variable $v \in \mathsf{Var}$. By hypothesis, $A_1, \ldots, A_k \vdash C$ is valid in the interpretation $[\![\cdot]\!]$ and we deduce $[\![A_1]\!] \circ \cdots \circ [\![A_k]\!] \subseteq [\![C]\!]$. Then, by Equations (4) and (5), for any $m \in \mathsf{M}$ we have $m \Vdash (A_1, \ldots, A_k)^{\circledast} \to C^{\circledast}$. Thus the formula $(A_1, \ldots, A_k)^{\circledast} \to C^{\circledast}$ is valid in the model $(\mathsf{M}, \circ, \epsilon, \delta)$.

Now, let us suppose that $(A_1, \ldots, A_k)^{\circledast} \to C^{\circledast}$ is valid in every Kripke interpretation based on $\mathcal{M}$. Let $[\![\cdot]\!] : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$ be a trivial phase semantic interpretation of variables in the model $\mathcal{M}$. We choose the Kripke interpretation $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathsf{M})$ defined by $\delta(v) = [\![v]\!]$ for any variable $v \in \mathsf{Var}$. By hypothesis, the formula $(A_1, \ldots, A_k)^{\circledast} \to C^{\circledast}$ is valid in the interpretation δ and we deduce that for any $m \in \mathsf{M}$ we have $m \Vdash (A_1, \ldots, A_k)^{\circledast} \to C^{\circledast}$. As a consequence of Equations (4) and (5), we obtain $[\![A_1]\!] \circ \cdots \circ [\![A_k]\!] \subseteq [\![C]\!]$. Hence, the sequent $A_1, \ldots, A_k \vdash C$ is valid in the trivial phase model $(\mathsf{M}, \circ, \epsilon, [\![\cdot]\!])$. □

Theorem 7.4 (Embedding). *For any class* X *of non-deterministic monoids and any sequent* $\Gamma \vdash C$ *of* ILL*, the following equivalence holds:*

$$\Gamma \vdash C \in \mathsf{ILL}^t_{\mathrm{X}} \quad \textit{if and only if} \quad \Gamma^{\circledast} \to C^{\circledast} \in \mathsf{BBI}_{\mathrm{X}}$$

Proof. Obvious consequence of Proposition 7.3. □

Corollary 7.5. *Let* X *and* Y *be two classes of non deterministic monoids such that the inclusion* $\mathsf{BBI}_{\mathrm{X}} \subseteq \mathsf{BBI}_{\mathrm{Y}}$ *holds. Then the inclusions* $\mathsf{ILL}^t_{\mathrm{X}} \subseteq \mathsf{ILL}^t_{\mathrm{Y}}$ *and* $\mathsf{eILL}^t_{\mathrm{X}} \subseteq \mathsf{eILL}^t_{\mathrm{Y}}$ *hold.*

Proof. It is obviously sufficient to prove the inclusion $\mathsf{ILL}^t_{\mathrm{X}} \subseteq \mathsf{ILL}^t_{\mathrm{Y}}$ because eILL is a fragment of ILL. But the inclusion $\mathsf{ILL}^t_{\mathrm{X}} \subseteq \mathsf{ILL}^t_{\mathrm{Y}}$ is trivially derived from the inclusion $\mathsf{BBI}_{\mathrm{X}} \subseteq \mathsf{BBI}_{\mathrm{Y}}$ using the embedding Theorem 7.4. □

7.3. Finitely generated free monoidal models vs. the RAM-domain model

In this section, we briefly explain how free monoidal models are less general than heap models, and in particular, less general than the RAM-domain model. The core of the argument is based on the bisimulation of multisets by heaps, a technique that was already (implicitly) used in [Brotherston and Kanovich 2010]. In Appendix C, we explicitly show how the bisimulation argument works.

LEMMA 7.6. *Let* X *be a set. For* $\mathsf{L} = \mathsf{X} \times \mathbb{N}$ *and* $\mathsf{V} = \{*\}$*, there exists a surjective map* $\varphi : \mathbb{H}_{\mathsf{L},\mathsf{V}} \longrightarrow \mathbb{M}_f(\mathsf{X})$ *such that for any Kripke interpretation* $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathbb{M}_f(\mathsf{X}))$ *in the free monoid* $(\mathbb{M}_f(\mathsf{X}), \star, \pi)$*, the Kripke interpretation* $\delta' : \mathsf{Var} \longrightarrow \mathbb{P}(\mathbb{H}_{\mathsf{L},\mathsf{V}})$ *in the heap monoid* $(\mathbb{H}_{\mathsf{L},\mathsf{V}}, \uplus, \emptyset)$ *defined by* $\delta' = v \mapsto \varphi^{-1}(\delta(v))$ *satisfies the following property:*

$$h \Vdash_{\delta'} F \quad \textit{if and only if} \quad \varphi(h) \Vdash_{\delta} F \qquad \textit{for any } F \in \mathsf{Form}$$

PROOF. The proof of this technical lemma is postponed to Appendix C. □

Let us consider two particular models of BBI. First, the simplest heap model $(\mathbb{H}_{\mathbb{N},\{*\}}, \uplus, \emptyset)$ which is isomorphic to the partial monoid of finite subsets of $\mathbb{N}$, i.e. RAM-domain monoid $(\mathbb{P}_f(\mathbb{N}), \uplus, \emptyset)$. Then the finitely generated free monoid over two elements $(\mathbb{M}_f(\{0,1\}), \star, \pi)$ which is isomorphic to the total deterministic monoid $(\mathbb{N} \times \mathbb{N}, +, (0,0))$. We denote by $\mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})}$ (resp. $\mathsf{BBI}_{\mathbb{N}\times\mathbb{N}}$) the set of BBI formulae which are valid in every Kripke interpretation over the heap model $(\mathbb{P}_f(\mathbb{N}), \uplus, \emptyset)$ (resp. free monoid $(\mathbb{N} \times \mathbb{N}, +, (0,0))$).

THEOREM 7.7. *The following sequence of inclusions holds:*

$$\mathsf{BBI}_{\mathrm{PD}} \subseteq \mathsf{BBI}_{\mathrm{SA}} \subseteq \mathsf{BBI}_{\mathrm{HM}} \subseteq \mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})} \subseteq \mathsf{BBI}_{\mathrm{FMf}} \subseteq \mathsf{BBI}_{\mathbb{N}\times\mathbb{N}}$$

PROOF. Since the inclusions $\mathbb{P}_f(\mathbb{N}) \simeq \mathbb{H}_{\mathbb{N},\{*\}} \in \mathrm{HM} \subseteq \mathrm{SA} \subseteq \mathrm{PD}$ and $\mathbb{N} \times \mathbb{N} \simeq \mathbb{M}_f(\{0,1\}) \in \mathrm{FMf}$ hold, the only inclusion left to prove is $\mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})} \subseteq \mathsf{BBI}_{\mathrm{FMf}}$. We prove this inclusion by contraposition. Let $F \notin \mathsf{BBI}_{\mathrm{FMf}}$ be a BBI-formula which has a counter-model in the form of a free monoid $(\mathbb{M}_f(\mathsf{X}), \star, \pi, \delta, m)$ for some non-empty finite set X. Hence we have $m \in \mathbb{M}_f(\mathsf{X})$ and $m \nVdash_{\delta} F$.

Let $\mathsf{L} = \mathsf{X} \times \mathbb{N}$. We build a counter-model for F based on $\mathbb{H}_{\mathsf{L},\{*\}}$. Let $\varphi : \mathbb{H}_{\mathsf{L},\{*\}} \longrightarrow \mathbb{M}_f(\mathsf{X})$ be the surjective map obtained by Lemma 7.6. Let us pick $h \in \mathbb{H}_{\mathsf{L},\{*\}}$ such that $\varphi(h) = m$ (φ is surjective). By Lemma 7.6, we have $h \nVdash'_{\delta} F$. Hence $(\mathbb{H}_{\mathsf{L},\{*\}}, \uplus, \emptyset, \delta', h)$ is a counter-model of F in the class HM.[14]

But since X is non-empty and finite, we deduce that $\mathsf{L} = \mathsf{X} \times \mathbb{N}$ is countably infinite, hence in one-to-one correspondence with $\mathbb{N}$. Thus the heap monoid $(\mathbb{H}_{\mathsf{L},\{*\}}, \uplus, \emptyset)$, the heap monoid $(\mathbb{H}_{\mathbb{N},\{*\}}, \uplus, \emptyset)$ and the RAM-domain monoid $(\mathbb{P}_f(\mathbb{N}), \uplus, \emptyset)$ are isomorphic. As a consequence, it is trivial to transform the counter-model based on $\mathbb{H}_{\mathsf{L},\{*\}}$ into a counter-model based on $\mathbb{P}_f(\mathbb{N})$. We deduce $F \notin \mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})}$. □

Remark: the strictness of the inclusions remains an open question, potentially difficult to answer.

THEOREM 7.8. *Trivial phase semantics restricted to the RAM-domain monoid (resp. heap monoids, resp. separation algebras) is complete for the elementary fragment of* ILL.

PROOF. Combining Corollary 7.5 and Theorem 7.7, we derive the following inclusions:

$$\mathsf{eILL}^t_{\mathrm{PD}} \subseteq \mathsf{eILL}^t_{\mathrm{SA}} \subseteq \mathsf{eILL}^t_{\mathrm{HM}} \subseteq \mathsf{eILL}^t_{\mathbb{P}_f(\mathbb{N})} \subseteq \mathsf{eILL}^t_{\mathrm{FMf}}$$

By Theorem 4.4, we have $\mathsf{eILL}_g = \mathsf{eILL}^t_{\mathrm{PD}} = \mathsf{eILL}^t_{\mathrm{FMf}}$, hence we deduce the result. □

7.4. The Undecidability Results

From the preceding developments, we establish the undecidability of BBI w.r.t. Kripke semantics in any class belonging to $\{\mathrm{ND}, \mathrm{PD}, \mathrm{TD}, \mathrm{HM}, \mathrm{SA}, \mathrm{FM}, \mathrm{FMf}\}$. Indeed, we have a faithful embedding from $\mathsf{ILL}^t_{\mathrm{X}}$ into $\mathsf{BBI}_{\mathrm{X}}$. But $\mathsf{ILL}^t_{\mathrm{X}}$ contains eILL as a complete and undecidable fragment. Thus the embedding transfers the undecidability to $\mathsf{BBI}_{\mathrm{X}}$.

[14]Remark that the transfer of the counter-model is done through (the graph of) φ which is a bisimulation between $\mathbb{H}_{\mathsf{L},\{*\}}$ and $\mathbb{M}_f(\mathsf{X})$; see Appendix C for details.

THEOREM 7.9 (UNDECIDABILITY OF BBI). *For any class* X ∈ {ND, PD, TD, HM, SA, FM, FMf}*, the set of (universally valid) formulae* BBI_X *is not recursive.*

PROOF. Suppose that there is an algorithm which decides membership in BBI_X. We propose the following algorithm which would then decide validity in the fragment eILL.

For a given elementary sequent $\Gamma \vdash C$ of eILL, compute the BBI formula $\Gamma^{\circledast} \to C^{\circledast}$. Decide if $\Gamma^{\circledast} \to C^{\circledast}$ belong to BBI_X. If true, then by Theorem 7.4, the sequent $\Gamma \vdash C$ belongs to ILL^t_X. By Theorems 4.4 and 7.8, the fragment eILL is complete w.r.t. trivial phase semantics in class X, $\Gamma \vdash C$ is a valid sequent of eILL. On the contrary, if the formula $\Gamma^{\circledast} \to C^{\circledast}$ does not belong to BBI_X, then by Theorem 7.4 the sequent $\Gamma \vdash C$ has a trivial phase semantics counter-model of class X. Hence, it is an invalid sequent of eILL.

By Theorem 5.7, there is no algorithm which decides the validity of sequents of the fragment eILL. We obtain a contradiction and thus no algorithm decides membership in BBI_X. □

THEOREM 7.10. *The sets of formulae* $\mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})}$ *and* $\mathsf{BBI}_{\mathbb{N}\times\mathbb{N}}$ *are not recursive.*

PROOF. By Theorem 5.8, $\mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$ is not a recursive set of sequents. By Theorems 5.7 and 7.8, $\mathsf{eILL}_p = \mathsf{eILL}_{\mathbb{P}_f(\mathbb{N})}$ is not a recursive set of sequents. Using Proposition 7.3, we replay the preceding proof. □

COROLLARY 7.11. *Propositional separation logic is undecidable.*

This result of [Brotherston and Kanovich 2010] depends on how you define propositional separation logic which can be BBI_{HM} (or BBI_{SA}) for instance. Other sub-classes of BBI_{HM} are considered in their paper. In fact, to obtain undecidability, it is sufficient for the class of models X to verify the relations $\mathbb{P}_f(\mathbb{N}) \in X \subseteq PD$. The result that $\mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})}$ is not recursive is the central result of [Brotherston and Kanovich 2010]. The use of the model $\mathbb{P}_f(\mathbb{N})$ is of chief importance to them because it is the simplest model of separation logic. Even though we understand the reasons for this choice, we claim that the implicit use of bisimulation in their model introduces an overhead that might complicate the understanding of their arguments. They would probably have obtained a simpler proof if they focused on the undecidability of BBI_{FM} (or $\mathsf{BBI}_{\mathbb{N}\times\mathbb{N}}$) instead of the undecidability of $\mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})}$. From our point of view, the indirect proof we provide here makes explicit the use of bisimulation to transform a model based on $\mathbb{M}_f(\mathsf{X})$ into a model based on $\mathbb{P}_f(\mathbb{N})$.

8. CONCLUSION AND RELATED WORKS

In this paper, we give a full proof that Boolean BI is undecidable by identifying a fragment of BBI on which the semantics defined by different classes of models collapse to one. This fragment is the direct image by a faithful embedding of the elementary fragment of ILL. By studying the phase and trivial phase semantics of eILL, we establish its completeness with respect to trivial phase semantics, whichever class of models is chosen amongst ND, PD, TD, HM, SA, FM and FMf. Undecidability follows from an encoding of two counter Minsky machine computations. The faithfulness of the encoding is obtained using a trivial phase model built on the free monoid $\mathbb{N}\times\mathbb{N}$, hence we can even derive the undecidability of eILL (and later BBI) restricted to the interpretations in the model $\mathbb{N}\times\mathbb{N}$.

We also bisimulate free monoids with heap monoids and thus prove that eILL is complete (and thus undecidable) for heap and separation algebra semantics. The bisimulation between $\mathbb{M}_f(\mathsf{X})$ and $\mathbb{P}_f(\mathbb{N})$ allows us to deduce the undecidability of eILL (and thus BBI) restricted to the interpretations in the model $\mathbb{P}_f(\mathbb{N})$, which is the simplest heap model conceivable. The result of the undecidability of $\mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})}$ is probably the most direct way to compare our work to that of [Brotherston and Kanovich 2010]. In their paper, the authors focus on heap models (i.e. models of separation logic), in particular the RAM-domain model $\mathbb{P}_f(\mathbb{N})$ for which they obtain the core result of the undecidability of $\mathsf{BBI}_{\mathbb{P}_f(\mathbb{N})}$ and then derive other undecidability results. However, they use another fragment of BBI and another encoding of Minsky machines which requires the monoidal models to have indivisible units.

The question of the decidability for interpretations restricted to $\mathbb{N}$ remains open because one counter Minsky machines are a special case of push-down automata for which accessibility is a decidable problem [Bouajjani et al. 1997].

In [Brotherston and Kanovich 2010], the authors show that undecidability also holds for Classical BI [Brotherston and Calcagno 2009] which is another variant of BI containing both an additive and a multiplicative negation. The encoding presented in [Larchey-Wendling and Galmiche 2010] which we keep in this paper would not fit for Classical BI. But in [Larchey-Wendling 2010], the author proposes a modified version of our encoding which is suitable for both Boolean BI and Classical BI with a faithfulness argument based on an interpretation in the free abelian group $\mathbb{Z} \times \mathbb{Z}$. Hence he obtains another proof of undecidability suitable for both Boolean and Classical BI.

We left remaining open problems. In particular, the classification of ILL^t and BBI with respect to validity in particular classes of models, or in particular models is unfinished. Solving this requires finding ILL^t or BBI formulae which distinguish the classes of models. This may be a difficult task which might need a better understanding of the expressive power of those two logics.

A. SOUNDNESS OF NON-DETERMINISTIC PHASE SEMANTICS FOR ILL

We recall Theorem 3.3. The proof we provide is really just an adaptation of a standard proof in linear logic semantics to the more general context of non-deterministic monoids.

THEOREM 3.3. *Let* $\mathcal{M} = (\mathsf{M}, \circ, \epsilon, (\cdot)^\diamond, \mathsf{K})$ *be a non-deterministic intuitionistic phase space and* $[\![\cdot]\!] : \mathsf{Var} \longrightarrow \mathcal{M}^\diamond$ *be an interpretation of logical variables. If the sequent* $A_1, \ldots, A_k \vdash B$ *has a proof in* S-ILL*, then the inclusion* $[\![A_1]\!] \circ \cdots \circ [\![A_k]\!] \subseteq [\![B]\!]$ *holds.*

PROOF. It could be done by induction on ILL proof trees but we rather use the algebraic semantic characterization of ILL of [Troelstra 1992]. We prove that

$$(\mathcal{M}^\diamond, \cap, (\cdot \cup \cdot)^\diamond, \emptyset^\diamond, \multimap, (\cdot \circ \cdot)^\diamond, \{\epsilon\}^\diamond, (\mathsf{K} \cap \cdot)^\diamond)$$

is *an IL-algebra with storage operator* (where $\multimap$ is defined by $\mathsf{X} \multimap \mathsf{Y} = \{k \in \mathsf{M} \mid k \circ \mathsf{X} \subseteq \mathsf{Y}\}$).

First, it is obvious that $(\mathsf{M}^\diamond, \cap, (\cdot \cup \cdot)^\diamond, \emptyset^\diamond)$ is a complete lattice with bottom $\emptyset^\diamond$. This is the *same proof* as in the usual (monoidal) case because the (non-deterministic) monoidal structure does not play any role in this part of the proof. The principal argument is that $(\cdot)^\diamond$ is a closure operator on $\mathbb{P}(\mathsf{M})$.

Let us prove that $(\mathcal{M}^\diamond, (\cdot \circ \cdot)^\diamond, \{\epsilon\}^\diamond)$ is a commutative monoid. Obviously the set $\mathcal{M}^\diamond$ is stable under the operator $(\cdot \circ \cdot)^\diamond$ which thus induces a binary operation on $\mathcal{M}^\diamond$. By stability, we obtain the inclusion $\{\epsilon\}^\diamond \circ \mathsf{X}^\diamond \subseteq (\{\epsilon\} \circ \mathsf{X})^\diamond = \mathsf{X}^\diamond$ and we deduce that for any closed subset X (i.e. $\mathsf{X} = \mathsf{X}^\diamond$), we have $(\{\epsilon\}^\diamond \circ \mathsf{X})^\diamond \subseteq \mathsf{X}$. Also $\mathsf{X} = \{\epsilon\} \circ \mathsf{X} \subseteq \{\epsilon\}^\diamond \circ \mathsf{X} \subseteq (\{\epsilon\}^\diamond \circ \mathsf{X})^\diamond$ by monotonicity of $\circ$ and $(\cdot)^\diamond$. Thus $(\{\epsilon\}^\diamond \circ \mathsf{X})^\diamond = \mathsf{X}$ for any closed subset $\mathsf{X} \in \mathcal{M}^\diamond$ and thus $\{\epsilon\}^\diamond$ is a (left) unit for $(\cdot \circ \cdot)^\diamond$. Then, it is obvious that $(\cdot \circ \cdot)^\diamond$ is a commutative operation because $\circ$ is itself commutative. We deduce that $\{\epsilon\}^\diamond$ is a unit for $(\cdot \circ \cdot)^\diamond$.

Let us prove that $(\cdot \circ \cdot)^\diamond$ is associative. Let $\mathsf{A}, \mathsf{B}, \mathsf{C} \in \mathcal{M}^\diamond$. Then, by stability of $(\cdot)^\diamond$, we have $\mathsf{A} \circ (\mathsf{B} \circ \mathsf{C})^\diamond \subseteq \mathsf{A}^\diamond \circ (\mathsf{B} \circ \mathsf{C})^\diamond \subseteq (\mathsf{A} \circ (\mathsf{B} \circ \mathsf{C}))^\diamond = (\mathsf{A} \circ \mathsf{B} \circ \mathsf{C})^\diamond$. Thus $(\mathsf{A} \circ (\mathsf{B} \circ \mathsf{C})^\diamond)^\diamond \subseteq (\mathsf{A} \circ \mathsf{B} \circ \mathsf{C})^\diamond$ holds. As $\mathsf{A} \circ \mathsf{B} \circ \mathsf{C} = \mathsf{A} \circ (\mathsf{B} \circ \mathsf{C}) \subseteq \mathsf{A} \circ (\mathsf{B} \circ \mathsf{C})^\diamond \subseteq (\mathsf{A} \circ (\mathsf{B} \circ \mathsf{C})^\diamond)^\diamond$, we deduce $(\mathsf{A} \circ \mathsf{B} \circ \mathsf{C})^\diamond \subseteq (\mathsf{A} \circ (\mathsf{B} \circ \mathsf{C})^\diamond)^\diamond$. By double inclusion, we conclude that $(\mathsf{A} \circ \mathsf{B} \circ \mathsf{C})^\diamond = (\mathsf{A} \circ (\mathsf{B} \circ \mathsf{C})^\diamond)^\diamond$. Associativity of $(\cdot \circ \cdot)^\diamond$ follows from this last identity and associativity/commutativity of $\circ$ on $\mathbb{P}(\mathsf{M})$.

It is obvious that $(\cdot \circ \cdot)^\diamond$ is monotonic in both parameters because it is obtained by composition of two monotonic operators, namely $\circ$ and $(\cdot)^\diamond$. Let us now prove that $\multimap$ is a right-adjoint $(\cdot \circ \cdot)^\diamond$. First, $\mathsf{X} \multimap \mathsf{Y}$ is closed as soon as Y is closed and $\mathsf{X} \multimap \mathsf{Y}^\diamond = \mathsf{X}^\diamond \multimap \mathsf{Y}^\diamond$ holds for any $\mathsf{X}, \mathsf{Y} \in \mathbb{P}(\mathsf{M})$ just as in the usual (monoidal) case. Now let $\mathsf{A}, \mathsf{B}, \mathsf{C} \in \mathcal{M}^\diamond$. We have $(\mathsf{A} \circ \mathsf{B})^\diamond \subseteq \mathsf{C}$ iff $\mathsf{A} \circ \mathsf{B} \subseteq \mathsf{C}$ iff $\mathsf{A} \subseteq \mathsf{B} \multimap \mathsf{C}$. Thus $\multimap$ is indeed right-adjoint to $(\cdot \circ \cdot)^\diamond$. The fact that $\multimap$ is contra-variant w.r.t. its first operand and co-variant w.r.t. its second operand is deducible from the monotonicity of $\circ$ and the fact that $\multimap$ is right adjoint to $\circ$.

We finish by proving that $\mathsf{X} \mapsto (\mathsf{K} \cap \mathsf{X})^\diamond$ is a *modality*. First, for any $\mathsf{X} \in \mathcal{M}^\diamond$, as $\mathsf{K} \cap \mathsf{X} \subseteq \mathsf{X} = \mathsf{X}^\diamond$, we obtain $(\mathsf{K} \cap \mathsf{X})^\diamond \subseteq \mathsf{X}$. Then for $\mathsf{X}, \mathsf{Y} \in \mathcal{M}^\diamond$, if we suppose that $(\mathsf{K} \cap \mathsf{Y})^\diamond \subseteq \mathsf{X}$ holds, we deduce

$\mathsf{K}\cap\mathsf{Y}\subseteq\mathsf{X}$ and thus $\mathsf{K}\cap\mathsf{Y}\subseteq\mathsf{K}\cap\mathsf{X}$. So we obtain $(\mathsf{K}\cap\mathsf{Y})^\diamond\subseteq(\mathsf{K}\cap\mathsf{X})^\diamond$. Then, from $\epsilon\in\mathsf{K}$, we deduce $\{\epsilon\}^\diamond\subseteq\mathsf{K}^\diamond=(\mathsf{K}\cap\mathsf{M})^\diamond$.[15] The last condition to check is $((\mathsf{K}\cap\mathsf{X})^\diamond\circ(\mathsf{K}\cap\mathsf{Y})^\diamond)^\diamond=(\mathsf{K}\cap\mathsf{X}\cap\mathsf{Y})^\diamond$ for any $\mathsf{X},\mathsf{Y}\in\mathcal{M}^\diamond$. First we have $(\mathsf{K}\cap\mathsf{X})^\diamond\circ(\mathsf{K}\cap\mathsf{Y})^\diamond\subseteq((\mathsf{K}\cap\mathsf{X})\circ(\mathsf{K}\cap\mathsf{Y}))^\diamond$. As $\mathsf{K}\subseteq\mathsf{J}\subseteq\{\epsilon\}^\diamond$, we have $(\mathsf{K}\cap\mathsf{X})\circ(\mathsf{K}\cap\mathsf{Y})\subseteq\{\epsilon\}^\diamond\circ\mathsf{Y}\subseteq\mathsf{Y}^\diamond=\mathsf{Y}$. We also have $(\mathsf{K}\cap\mathsf{X})\circ(\mathsf{K}\cap\mathsf{Y})\subseteq\mathsf{X}$. As $\mathsf{K}\circ\mathsf{K}\subseteq\mathsf{K}$ we have $(\mathsf{K}\cap\mathsf{X})\circ(\mathsf{K}\cap\mathsf{Y})\subseteq\mathsf{K}$ and hence, we deduce $(\mathsf{K}\cap\mathsf{X})\circ(\mathsf{K}\cap\mathsf{Y})\subseteq\mathsf{K}\cap\mathsf{X}\cap\mathsf{Y}$. Using stability, we compute $(\mathsf{K}\cap\mathsf{X})^\diamond\circ(\mathsf{K}\cap\mathsf{Y})^\diamond\subseteq((\mathsf{K}\cap\mathsf{X})\circ(\mathsf{K}\cap\mathsf{Y}))^\diamond\subseteq(\mathsf{K}\cap\mathsf{X}\cap\mathsf{Y})^\diamond$ and thus $((\mathsf{K}\cap\mathsf{X})^\diamond\circ(\mathsf{K}\cap\mathsf{Y})^\diamond)^\diamond\subseteq(\mathsf{K}\cap\mathsf{X}\cap\mathsf{Y})^\diamond$. Now let us prove the reverse inclusion. Let $z\in\mathsf{K}\cap\mathsf{X}\cap\mathsf{Y}$. As $z\in\mathsf{K}$ then $z\in\mathsf{J}$ and we have $z\in(z\circ z)^\diamond\subseteq((\mathsf{K}\cap\mathsf{X})\circ(\mathsf{K}\cap\mathsf{Y}))^\diamond\subseteq((\mathsf{K}\cap\mathsf{X})^\diamond\circ(\mathsf{K}\cap\mathsf{Y})^\diamond)^\diamond$. Hence, $\mathsf{K}\cap\mathsf{X}\cap\mathsf{Y}\subseteq((\mathsf{K}\cap\mathsf{X})^\diamond\circ(\mathsf{K}\cap\mathsf{Y})^\diamond)^\diamond$ and we deduce $(\mathsf{K}\cap\mathsf{X}\cap\mathsf{Y})^\diamond\subseteq((\mathsf{K}\cap\mathsf{X})^\diamond\circ(\mathsf{K}\cap\mathsf{Y})^\diamond)^\diamond$.

We can then apply Theorem 8.21 (page 80) from [Troelstra 1992]. If $A_1,\ldots,A_k\vdash B$ has a proof in ILL, then the inclusion $[\![A_1,\ldots,A_k]\!]\subseteq[\![B]\!]$ holds. It is obvious to prove that $[\![A_1]\!]\circ\cdots\circ[\![A_k]\!]\subseteq[\![A_1,\ldots,A_k]\!]$ by induction on k for example. So we deduce $[\![A_1]\!]\circ\cdots\circ[\![A_k]\!]\subseteq[\![B]\!]$. □

B. COMPLETENESS OF NON-DETERMINISTIC PHASE SEMANTICS FOR ILL

In this section, Form denotes the set of formulae of ILL build from Var as set of logical variables, as defined in Section 3. Let $\mathsf{Ctx}=\mathbb{M}_\mathrm{f}(\mathsf{Form})$ denotes the set of *contexts* build from the formulae of ILL, i.e. the set of finite multisets of ILL-formulae. Recall that a sequent is a pair $(\Gamma,C)\in\mathsf{Ctx}\times\mathsf{Form}$ denoted $\Gamma\vdash C$ and that ILL_p denotes the set of sequents for which there exists a proof in the S-ILL.

Given a set of contexts $\mathsf{X}\subseteq\mathsf{Ctx}$, a context $\Delta\in\mathsf{Ctx}$ and a formula $C\in\mathsf{Form}$, we denote by $\Delta,\mathsf{X}\vdash C$ the following set of sequents:

$$\Delta,\mathsf{X}\vdash C=\{\Delta,\Gamma\vdash C\mid\Gamma\in\mathsf{X}\}$$

We consider the following free (commutative) monoid $(\mathsf{Ctx},\star,\pi)$ where the composition $\star$ is defined by $\Gamma\star\Delta=\{\lfloor\Gamma,\Delta\rfloor\}$[16] for any $\Gamma,\Delta\in\mathsf{Ctx}$ and $\pi=\lfloor\emptyset\rfloor$ is the empty context. This non-deterministic monoid $(\mathsf{Ctx},\star,\pi)$ obviously belongs to the class FM. The adjoint of $\star$ is denoted $-\!\!\star$. We define the closure operator $(\cdot)^\diamond$ on $\mathbb{P}(\mathsf{Ctx})$ and the set $\mathsf{K}\subseteq\mathsf{Ctx}$ by

$$\begin{aligned}\mathsf{X}^\diamond&=\{\Gamma\in\mathsf{Ctx}\mid\forall\Delta\in\mathsf{Ctx},\forall C\in\mathsf{Form}\ \ \Delta,\mathsf{X}\vdash C\subseteq\mathsf{ILL}_p\Rightarrow\Delta,\Gamma\vdash C\in\mathsf{ILL}_p\}\\ \mathsf{K}&=\{!\,\Gamma\in\mathsf{Ctx}\mid\Gamma\in\mathsf{Ctx}\}\end{aligned}$$

Proposition B.1. $(\mathsf{Ctx},\star,\pi,(\cdot)^\diamond,\mathsf{K})$ *is a non-deterministic phase space of class* FM.

Proof. As mentioned earlier, $(\mathsf{Ctx},\star,\pi)$ is a non-deterministic monoid of class FM. We first prove that $(\cdot)^\diamond$ is a stable closure, then we show that K verifies $\pi\in\mathsf{K}\subseteq\{\Gamma\in\mathsf{Ctx}\mid\Gamma\in\{\pi\}^\diamond\cap(\Gamma\star\Gamma)^\diamond\}$ and $\mathsf{K}\star\mathsf{K}\subseteq\mathsf{K}$.

Let X and Y be two subsets of Ctx. Let us prove $\mathsf{X}\subseteq\mathsf{X}^\diamond$. Let $\Gamma\in\mathsf{X}$. Then for any Δ,C we have $\{\Delta,\Gamma\vdash C\}\subseteq\Delta,\mathsf{X}\vdash C$. Hence, if $\Delta,\mathsf{X}\vdash C\subseteq\mathsf{ILL}_p$ holds, the property $\Delta,\Gamma\vdash C\in\mathsf{ILL}_p$ also holds. Thus, $\Gamma\in\mathsf{X}^\diamond$ holds. We have proved $\mathsf{X}\subseteq\mathsf{X}^\diamond$. From the definition of $(\cdot)^\diamond$, $\mathsf{X}\subseteq\mathsf{Y}$ obviously entails $\mathsf{X}^\diamond\subseteq\mathsf{Y}^\diamond$. Let us now prove that $\mathsf{X}^{\diamond\diamond}\subseteq\mathsf{X}^\diamond$. Let $\Gamma\in\mathsf{X}^{\diamond\diamond}$ and let us prove $\Gamma\in\mathsf{X}^\diamond$. We consider Δ,C such that the property $\Delta,\mathsf{X}\vdash C\subseteq\mathsf{ILL}_p$ holds. By definition of $(\cdot)^\diamond$, we deduce that $\Delta,\mathsf{X}^\diamond\vdash C\subseteq\mathsf{ILL}_p$ holds. Since $\Gamma\in\mathsf{X}^{\diamond\diamond}$, we deduce that $\Delta,\Gamma\vdash C\in\mathsf{ILL}_p$ holds. From $\Delta,\mathsf{X}\vdash C\subseteq\mathsf{ILL}_p$ we derived $\Delta,\Gamma\vdash C\in\mathsf{ILL}_p$, so we have proved that $\Gamma\in\mathsf{X}^\diamond$. Hence, $\mathsf{X}^{\diamond\diamond}\subseteq\mathsf{X}^\diamond$ and then $(\cdot)^\diamond$ is a closure operator on $\mathbb{P}(\mathsf{Ctx})$.

Let us now prove that the closure $(\cdot)^\diamond$ is stable, i.e. satisfies the axiom $\mathsf{X}^\diamond\star\mathsf{Y}^\diamond\subseteq(\mathsf{X}\star\mathsf{Y})^\diamond$ for any two subsets X, Y of Ctx. Since $\star$ is commutative and $(\cdot)^\diamond$ is a closure, it is sufficient to prove the property $\mathsf{X}\star\mathsf{Y}^\diamond\subseteq(\mathsf{X}\star\mathsf{Y})^\diamond$ for any two subsets X, Y of Ctx (the proof of this simplification is left to the reader). Now let us consider $\Gamma_1\in\mathsf{X}$ and $\Gamma_2\in\mathsf{Y}^\diamond$ and let us prove that $\lfloor\Gamma_1,\Gamma_2\rfloor\in(\mathsf{X}\star\mathsf{Y})^\diamond$. So let us introduce Δ,C such that $\Delta,\mathsf{X}\star\mathsf{Y}\vdash C\subseteq\mathsf{ILL}_p$. Since $\Gamma_1\in\mathsf{X}$ holds, we deduce $\{\Gamma_1\}\star\mathsf{Y}\subseteq\mathsf{X}\star\mathsf{Y}$ and thus $\lfloor\Delta,\Gamma_1\rfloor,\mathsf{Y}\vdash C\subseteq\mathsf{ILL}_p$ holds. Since $\Gamma_2\in\mathsf{Y}^\diamond$ holds, we deduce $\lfloor\Delta,\Gamma_1\rfloor,\Gamma_2\vdash C\in\mathsf{ILL}_p$. Hence, $\Delta,\lfloor\Gamma_1,\Gamma_2\rfloor\vdash C\in\mathsf{ILL}_p$ holds. We conclude $\lfloor\Gamma_1,\Gamma_2\rfloor\in(\mathsf{X}\star\mathsf{Y})^\diamond$. We have proved that $\mathsf{X}\star\mathsf{Y}^\diamond\subseteq(\mathsf{X}\star\mathsf{Y})^\diamond$ holds for any $\mathsf{X},\mathsf{Y}\subseteq\mathsf{Ctx}$. As a consequence, the closure $(\cdot)^\diamond$ is stable.

[15] Recall the identity $\emptyset^\diamond\multimap\emptyset^\diamond=\emptyset\multimap\emptyset^\diamond=\mathsf{M}$.

[16] Recall that $\Gamma\mapsto\lfloor\Gamma\rfloor$ is the identity map on Ctx but the extra notation $\lfloor\cdot\rfloor$ in $\{\lfloor\Gamma,\Delta\rfloor\}$ is used to here to remove the ambiguity on the denotation of the comma: here it denotes the composition of multisets, not the addition of elements in a set.

Now let us finish by checking the axioms corresponding to K. Since $\pi = \lfloor\emptyset\rfloor = \lfloor !\,\emptyset\rfloor$, it is obvious that $\pi \in \mathsf{K}$. Let us prove that $\mathsf{K} \subseteq \{\Gamma \in \mathsf{Ctx} \mid \Gamma \in \{\pi\}^\diamond \cap (\Gamma \star \Gamma)^\diamond\}$. Let $\Gamma \in \mathsf{K}$. There exists Γ_0 such that $\Gamma = !\,\Gamma_0$. Let us prove that $!\,\Gamma_0 \in \{\pi\}^\diamond$. We consider Δ, C such that $\Delta, \{\pi\} \vdash C \subseteq \mathsf{ILL}_p$, which reduces to $\Delta \vdash C \in \mathsf{ILL}_p$. Hence $\Delta \vdash C$ has a proof in S-ILL and by multiple applications of rule $\langle \mathrm{w}\rangle$, we obtain a proof of $\Delta, !\,\Gamma_0 \vdash C$ in S-ILL. Hence $\Delta, !\,\Gamma_0 \vdash C \in \mathsf{ILL}_p$. We conclude that $\Gamma = !\,\Gamma_0$ belongs to $\{\pi\}^\diamond$. Since $\Gamma \star \Gamma = \{\lfloor !\,\Gamma_0, !\,\Gamma_0\rfloor\}$, we prove that $!\,\Gamma_0 \in \{\lfloor !\,\Gamma_0, !\,\Gamma_0\rfloor\}^\diamond$ using a similar argument, replacing rule $\langle \mathrm{w}\rangle$ by rule $\langle \mathrm{c}\rangle$. We finish with a proof of $\mathsf{K} \star \mathsf{K} \subseteq \mathsf{K}$. Let $\Gamma \in \mathsf{K} \star \mathsf{K}$. By Definition (1) of the extension of $\star$ on $\mathbb{P}(\mathsf{Ctx})$, there exists $!\,\Gamma_0 \in \mathsf{K}$ and $!\,\Gamma_1 \in \mathsf{K}$ such that $\Gamma \in \Gamma_0 \star \Gamma_1$. We deduce $\Gamma = \lfloor !\,\Gamma_0, !\,\Gamma_1\rfloor$ and, as a consequence $\Gamma \in \mathsf{K}$ holds. □

For any formula F of ILL, we denote by $\downarrow F$ the *section below F* defined by

$$\downarrow F = \{\Gamma \in \mathsf{Ctx} \mid \Gamma \vdash F \in \mathsf{ILL}_p\}$$

It is easy to prove that sections are closed subsets of $\mathbb{P}(\mathsf{Ctx})$.

Proposition B.2. *For any formula F of ILL, the inclusion $(\downarrow F)^\diamond \subseteq \downarrow F$ holds.*

Proof. For the following values of $\Delta = \lfloor\emptyset\rfloor$ and $C = F$, we obtain $\Delta, \downarrow F \vdash C \subseteq \mathsf{ILL}_p$. Hence, if we pick $\Gamma \in (\downarrow F)^\diamond$, we deduce $\Delta, \Gamma \vdash C \in \mathsf{ILL}_p$ by definition of $(\cdot)^\diamond$. We conclude $\Gamma \vdash F \in \mathsf{ILL}_p$ and thus $\Gamma \in \downarrow F$. Hence the inclusion $(\downarrow F)^\diamond \subseteq \downarrow F$ holds. □

As sections are closed, it is legitimate to interpret logical variables by their section, i.e. we define the interpretation $[\![v]\!] = \downarrow v$ for every variable $v \in \mathsf{Var}$. The following lemma which is the core of the completeness argument was first explicited by Okada [Okada 2002] (but not for exactly the same closure operator we use here).

Lemma B.3 (Okada). *For any formula F of ILL, the relation $\lfloor F\rfloor \in [\![F]\!] \subseteq \downarrow F$ holds.*

Proof. The proof is done by (mutual) induction of the formula F. The beauty of the argument is that the semantic properties $\lfloor F\rfloor \in [\![F]\!]$ and $[\![F]\!] \subseteq \downarrow F$ correspond one to one with the rules of the $\langle \mathrm{cut}\rangle$-free S-ILL calculus.

— for a variable $v \in \mathsf{Var}$, the property $\lfloor v\rfloor \in [\![v]\!]$ reduces to $\lfloor v\rfloor \in \downarrow v$ which is an instance of the identity axiom $\langle \mathrm{id}\rangle$. The property $[\![v]\!] \subseteq \downarrow v$ reduces to $\downarrow v \subseteq \downarrow v$ which is trivial;

— if F is a formula of type $F = A \otimes B$, then we observe that rule $\langle \otimes_L\rangle$ corresponds to the relation $\lfloor A \otimes B\rfloor \in \{\lfloor A, B\rfloor\}^\diamond$ and rule $\langle \otimes_R\rangle$ corresponds to the relation $\downarrow A \star \downarrow B \subseteq \downarrow A \otimes B$. Thus, using the induction hypotheses $\lfloor A\rfloor \in [\![A]\!] \subseteq \downarrow A$ and $\lfloor B\rfloor \in [\![B]\!] \subseteq \downarrow B$, we compute $\lfloor A \otimes B\rfloor \in \{\lfloor A, B\rfloor\}^\diamond \subseteq (\lfloor A\rfloor \star \lfloor B\rfloor)^\diamond \subseteq ([\![A]\!] \star [\![B]\!])^\diamond \subseteq [\![A \otimes B]\!]$ and $[\![A \otimes B]\!] \subseteq ([\![A]\!] \star [\![B]\!])^\diamond \subseteq (\downarrow A \star \downarrow B)^\diamond \subseteq (\downarrow A \otimes B)^\diamond \subseteq \downarrow A \otimes B$;

— if $F = A \multimap B$, then we use the relations $\lfloor A \multimap B\rfloor \in (\downarrow A) \mathrel{-\!\!\star} \{\lfloor B\rfloor\}^\diamond$ and $\{\lfloor A\rfloor\} \mathrel{-\!\!\star} \downarrow B \subseteq \downarrow A \multimap B$ corresponding to rules $\langle \multimap_L\rangle$ and $\langle \multimap_R\rangle$ respectively. We compute $\lfloor A \multimap B\rfloor \in (\downarrow A) \mathrel{-\!\!\star} \{\lfloor B\rfloor\}^\diamond \subseteq [\![A]\!] \mathrel{-\!\!\star} [\![B]\!]^\diamond = [\![A \multimap B]\!]$ and $[\![A \multimap B]\!] = [\![A]\!] \mathrel{-\!\!\star} [\![B]\!] \subseteq \{\lfloor A\rfloor\} \mathrel{-\!\!\star} \downarrow B \subseteq \downarrow A \multimap B$;

— if $F = 1$, we obtain the relations $\lfloor 1\rfloor \in \{\lfloor\emptyset\rfloor\}^\diamond$ and $\lfloor\emptyset\rfloor \in \downarrow 1$ for rules $\langle 1_L\rangle$ and $\langle 1_R\rangle$ respectively. Thus $\lfloor 1\rfloor \in \{\lfloor\emptyset\rfloor\}^\diamond = \{\pi\}^\diamond = [\![1]\!]$ and $[\![1]\!] = \{\lfloor\emptyset\rfloor\}^\diamond \subseteq (\downarrow 1)^\diamond \subseteq \downarrow 1$;

— if $F = A \,\&\, B$, we obtain the relations $\lfloor A \,\&\, B\rfloor \in \{\lfloor A\rfloor\}^\diamond$, $\lfloor A \,\&\, B\rfloor \in \{\lfloor B\rfloor\}^\diamond$ and $\downarrow A \cap \downarrow B \subseteq \downarrow A \,\&\, B$ for rules $\langle \&^1_L\rangle$, $\langle \&^2_L\rangle$ and $\langle \&_R\rangle$respectively. Thus $\lfloor A \,\&\, B\rfloor \in \{\lfloor A\rfloor\}^\diamond \cap \{\lfloor B\rfloor\}^\diamond \subseteq [\![A]\!]^\diamond \cap [\![B]\!]^\diamond \subseteq [\![A]\!] \cap [\![B]\!] = [\![A \,\&\, B]\!]$ and $[\![A \,\&\, B]\!] = [\![A]\!] \cap [\![B]\!] \subseteq \downarrow A \cap \downarrow B \subseteq \downarrow A \,\&\, B$;

— if $F = \top$, we obtain the relation $\mathsf{Ctx} \subseteq \downarrow \top$ for rule $\langle \top_R\rangle$. Thus $\lfloor \top\rfloor \in \mathsf{Ctx} = [\![\top]\!]$ and $[\![\top]\!] = \mathsf{Ctx} \subseteq \downarrow \top$;

— if $F = A \oplus B$, we obtain the relations $\lfloor A \oplus B\rfloor \in \{\lfloor A\rfloor, \lfloor B\rfloor\}^\diamond$, $\downarrow A \subseteq \downarrow A \oplus B$ and $\downarrow B \subseteq \downarrow A \oplus B$ for rules $\langle \oplus_L\rangle$, $\langle \oplus^1_R\rangle$ and $\langle \oplus^2_R\rangle$ respectively. Thus $\lfloor A \oplus B\rfloor \in \{\lfloor A\rfloor, \lfloor B\rfloor\}^\diamond = (\{\lfloor A\rfloor\} \cup \{\lfloor B\rfloor\})^\diamond \subseteq ([\![A]\!] \cup [\![B]\!])^\diamond = [\![A \oplus B]\!]$ and $[\![A \oplus B]\!] = ([\![A]\!] \cup [\![B]\!])^\diamond \subseteq (\downarrow A \cup \downarrow B)^\diamond \subseteq (\downarrow A \oplus B)^\diamond \subseteq \downarrow A \oplus B$;

— if $F = \bot$, we obtain the relation $\lfloor \bot\rfloor \in \emptyset^\diamond$ for rule $\langle \bot_L\rangle$. Thus $\lfloor \bot\rfloor \in \emptyset^\diamond = [\![\bot]\!]$ and $[\![\bot]\!] = \emptyset^\diamond \subseteq (\downarrow \bot)^\diamond \subseteq \downarrow \bot$;

— if $F = \,!A$, we obtain the relations $\lfloor !A \rfloor \in \{\lfloor A \rfloor\}^\diamond$ and $\mathsf{K} \cap \downarrow A \subseteq \downarrow(!A)$ for rules $\langle !_L \rangle$ and $\langle !_R \rangle$ respectively. Since $\lfloor !A \rfloor \in \mathsf{K}$ by definition of K, we deduce $\lfloor !A \rfloor \in \mathsf{K} \cap \{\lfloor A \rfloor\}^\diamond \subseteq \mathsf{K} \cap [\![A]\!] \subseteq [\![!A]\!]$ and $[\![!A]\!] = (\mathsf{K} \cap [\![A]\!])^\diamond \subseteq (\mathsf{K} \cap \downarrow A)^\diamond \subseteq (\downarrow(!A))^\diamond \subseteq \downarrow(!A)$.

□

THEOREM 3.5. *If the sequent $\Gamma \vdash A$ is valid in every free monoidal phase semantic interpretation $(M, \circ, \epsilon, (\cdot)^\diamond, K, [\![\cdot]\!])$ (i.e. with $(M, \circ, \epsilon)$ of the class* FM*), then $\Gamma \vdash A$ has a proof in* S-ILL.

PROOF. Let $A_1, \ldots, A_k \vdash B$ be a sequent which is valid in every free monoidal phase semantic interpretation. In particular, it is valid in our current interpretation $(\mathsf{Ctx}, \star, \pi)$ and we deduce that the inclusion $[\![A_1]\!] \star \cdots \star [\![A_k]\!] \subseteq [\![B]\!]$ holds. By Okada's lemma B.3, we obtain

$$\lfloor A_1, \ldots, A_k \rfloor \in \lfloor A_1 \rfloor \star \cdots \star \lfloor A_k \rfloor \subseteq [\![A_1]\!] \star \cdots \star [\![A_k]\!] \subseteq [\![B]\!] \subseteq \downarrow B$$

and we conclude $A_1, \ldots, A_k \vdash B \in \mathsf{ILL}_p$. Hence, the sequent $A_1, \ldots, A_k \vdash B$ has a proof in S-ILL. □

Remark: this proof does not use the cut rule ⟨cut⟩ so it can also be used as an argument for *strong completeness* from which it is easy to derive a semantic proof of cut-elimination for S-ILL.

C. BISIMULATING FREE MONOIDS WITH THE RAM-DOMAIN MODEL

In this section, we give a detailed proof of Lemma 7.6. Let us fix a set X. We denote by $(\mathbb{M}_f(\mathsf{X}), +, 0)$ the (usual) free commutative monoid generated by X, i.e. $\mathbb{M}_f(\mathsf{X})$ is the set of finite multisets of elements of X. Multiset composition is denoted additively, so for example we denote by $m = \sum_{x \in \mathsf{X}} m_x.x$ the multiset which contains exactly $m_x \in \mathbb{N}$ occurrences of the variable x for each $x \in \mathsf{X}$. In case X is infinite, it is assumed that the value of m_x is non-zero for only a finite subset of X. Recall that there is an associated (total deterministic) free monoid of class FM which is denoted $(\mathbb{M}_f(\mathsf{X}), \star, \pi)$ with the identities $m \star n = \{m + n\}$ and $\pi = 0$.

We define the following set of locations $\mathsf{L} = \mathsf{X} \times \mathbb{N}$, and $\mathsf{L}_x = \{x\} \times \mathbb{N}$ is a section of L for each $x \in \mathsf{X}$. We also define $l_x^i = (x, i) \in \mathsf{L}$ and thus we obtain the following identities:

$$\mathsf{L} = \biguplus_{x \in \mathsf{X}} \mathsf{L}_x \qquad \text{and} \qquad \mathsf{L}_x = \{l_x^0, l_x^1, l_x^2, \ldots\} \quad \text{for } x \in \mathsf{X}$$

We define the set of values $\mathsf{V} = \{*\}$ as a singleton set. Considering the heap monoid $(\mathbb{H}_{\mathsf{L},\mathsf{V}}, \uplus, \varnothing)$, we define a map $\varphi : \mathbb{H}_{\mathsf{L},\mathsf{V}} \longrightarrow \mathbb{M}_f(\mathsf{X})$ by

$$\varphi(h) = \sum_{x \in \mathsf{X}} \mathrm{card}(\mathrm{def}(h) \cap \mathsf{L}_x).x$$

PROPOSITION C.1. *The map $\varphi : \mathbb{H}_{\mathsf{L},\mathsf{V}} \longrightarrow \mathbb{M}_f(\mathsf{X})$ satisfies the following properties:*

(*1*) *φ is a surjective map;*
(*2*) *if $m_1, m_2 \in \mathbb{M}_f(\mathsf{X})$ and $h \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ satisfy $\varphi(h) = m_1 + m_2$ then there exists $h_1, h_2 \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ such that $\varphi(h_1) = m_1$, $\varphi(h_2) = m_2$ and $h_1 \uplus h_2 = \{h\}$;*
(*3*) *for any $m_1 \in \mathbb{M}_f(\mathsf{X})$ and any $h_2 \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ there exists $h_1 \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ such that $\mathrm{def}(h_1) \cap \mathrm{def}(h_2) = \emptyset$ and $\varphi(h_1) = m_1$;*
(*4*) *$\varphi(h_1 \uplus h_2) = \varphi(h_1) \star \varphi(h_2)$ when $\mathrm{def}(h_1) \cap \mathrm{def}(h_2) = \emptyset$;*
(*5*) *$\varphi(h) = 0$ if and only if $h = \varnothing$ for any $h \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$;*
(*6*) *$\varphi^{-1}(\mathsf{A}) \uplus \varphi^{-1}(\mathsf{B}) = \varphi^{-1}(\mathsf{A} \star \mathsf{B})$ for any $\mathsf{A}, \mathsf{B} \subseteq \mathbb{M}_f(\mathsf{X})$.*

PROOF. Let us prove Property (1) and show that φ is a surjective map. Let $m = \sum_{x \in \mathsf{X}} m_x.x$ be a finite multiset. Then the set $\{(l_x^i, *) \mid 0 \leqslant i < m_x\}$ is the graph of a partial function and we denote this function by h_m. It can be easily be checked that $\mathrm{def}(h_m)$ is a finite subset of L and that

$$\varphi(h_m) = \sum_{x \in \mathsf{X}} \mathrm{card}\{l_x^i \mid 0 \leqslant i < m_x\}.x = \sum_{x \in \mathsf{X}} m_x.x = m$$

Let use prove Property (2). Let $m, n \in \mathbb{M}_f(\mathsf{X})$ and $h \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ be such that $\varphi(h) = m + n$. For each $x \in \mathsf{X}$, we have $\mathrm{card}(\mathrm{def}(h) \cap \mathsf{L}_x) = m_x + n_x$. Let us partition $\mathrm{def}(h) \cap \mathsf{L}_x$ in $\mathrm{def}(h) \cap \mathsf{L}_x = \mathsf{L}_x^1 \cup \mathsf{L}_x^2$ such that $\mathrm{card}(\mathsf{L}_x^1) = m_x$ and $\mathrm{card}(\mathsf{L}_x^2) = n_x$. Then let h_1 (resp. h_2) be the partial function with graph $\{(l_x^i, *) \mid l_x^i \in \mathsf{L}_x^1\}$ (resp. $\{(l_x^i, *) \mid l_x^i \in \mathsf{L}_x^2\}$). The reader can check that $\varphi(h_1) = m_1$, $\varphi(h_2) = m_2$ and $h_1 \uplus h_2 = \{h\}$ hold.

Let us prove Property (3). Let us write $m_1 = \sum_{x \in \mathsf{X}} m_x^1.x$. For $x \in \mathsf{Var}$, since $\mathsf{L}_x \backslash \mathrm{def}(h_2)$ is an infinite set, let us choose L_x^1 such that $\mathsf{L}_x^1 \subseteq \mathsf{L}_x \backslash \mathrm{def}(h_2)$ and $\mathrm{card}(\mathsf{L}_x^1) = m_x^1$. Now let us consider the partial function h_1 defined by the graph $\{(l_x^i, *) \mid l_x^i \in \mathsf{L}_x^1\}$. It is obvious that $\mathrm{def}(h_1)$ is finite, $\mathrm{def}(h_1) \cap \mathrm{def}(h_2) = \emptyset$ and $\varphi(h_1) = m_1$.

Let us prove Property (4). Let $h_1, h_2 \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ such that $\mathrm{def}(h_1) \cap \mathrm{def}(h_2) = \emptyset$. Let h be the result of the composition of h_1 and h_2, i.e. $h_1 \uplus h_2 = \{h\}$. Then $\mathrm{card}(\mathrm{def}(h) \cap \mathsf{L}_x) = \mathrm{card}(\mathrm{def}(h_1) \cap \mathsf{L}_x) + \mathrm{card}(\mathrm{def}(h_1) \cap \mathsf{L}_x)$ and we deduce $\varphi(h) = \varphi(h_1) + \varphi(h_2)$, hence $\varphi(h_1 \uplus h_2) = \{\varphi(h_1) + \varphi(h_2)\}$.

Let us prove Property (5). For the *only if part*, let us suppose that $\varphi(h) = 0$. Then for any $x \in \mathsf{X}$, we have $\mathrm{card}(\mathrm{def}(h) \cap \mathsf{L}_x) = 0$ and thus $\mathrm{def}(h) \cap \mathsf{L}_x = \emptyset$. Hence we compute $\mathrm{def}(h) \cap \mathsf{L} = \mathrm{def}(h) \cap (\bigcup_{x \in \mathsf{X}} \mathsf{L}_x) = \bigcup_{x \in \mathsf{X}} \mathrm{def}(h) \cap \mathsf{L}_x = \emptyset$. We deduce $\mathrm{def}(h) = \emptyset$ and, as a consequence, the identity $h = \varnothing$ holds. For the *if part*, let us suppose that $h = \varnothing$. Then $\mathrm{def}(h) = \emptyset$ holds and thus we obtain $\mathrm{card}(\mathrm{def}(h) \cap \mathsf{L}_x) = 0$ for any $x \in \mathsf{X}$. So, we derive the identity $\varphi(h) = 0$.

Let us prove Property (6). First let us consider the inclusion $\varphi^{-1}(\mathsf{A} \star \mathsf{B}) \subseteq \varphi^{-1}(\mathsf{A}) \uplus \varphi^{-1}(\mathsf{B})$. Let us pick $h \in \varphi^{-1}(\mathsf{A} \star \mathsf{B})$. Then $\varphi(h) \in \mathsf{A} \star \mathsf{B}$ so there exists $m_1 \in \mathsf{A}$ and $m_2 \in \mathsf{B}$ such that $\varphi(h) = m_1 + m_2$. By Property (2), there exists h_1, h_2 such that $\varphi(h_1) = m_1$, $\varphi(h_2) = m_2$ and $h_1 \uplus h_2 = \{h\}$. Hence $h_1 \in \varphi^{-1}(\mathsf{A})$ and $h_2 \in \varphi^{-1}(\mathsf{B})$. As $h_1 \uplus h_2 = \{h\}$, we get $h \in \varphi^{-1}(\mathsf{A}) \uplus \varphi^{-1}(\mathsf{B})$. Let us consider the reverse inclusion $\varphi^{-1}(\mathsf{A}) \uplus \varphi^{-1}(\mathsf{B}) \subseteq \varphi^{-1}(\mathsf{A} \star \mathsf{B})$. Let $h \in \varphi^{-1}(\mathsf{A}) \uplus \varphi^{-1}(\mathsf{B})$. Then there exists $h_1 \in \varphi^{-1}(\mathsf{A})$ and $h_2 \in \varphi^{-1}(\mathsf{B})$ such that $h \in h_1 \uplus h_2$. Then we have $\mathrm{def}(h_1) \cap \mathrm{def}(h_2) = \emptyset$ (otherwise $h_1 \uplus h_2 = \emptyset$) and by Property (4), we deduce $\varphi(h) = \varphi(h_1) + \varphi(h_2) \in \mathsf{A} \star \mathsf{B}$. Hence $h \in \varphi^{-1}(\mathsf{A} \star \mathsf{B})$. □

LEMMA C.2 (BISIMULATION). *Let $R_\varphi \subseteq \mathbb{H}_{\mathsf{L},\mathsf{V}} \times \mathbb{M}_f(\mathsf{X})$ be the binary relation defined by the graph of φ, i.e. $h\ R_\varphi\ m$ iff $\varphi(h) = m$. Then R_φ is a bisimulation between non-deterministic monoids, i.e. it satisfies the following property for any $h \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ and any $m \in \mathbb{M}_f(\mathsf{X})$*

$$h\ R_\varphi\ m \Rightarrow \begin{cases} h = \varnothing \text{ iff } m = \pi \\ \forall h_1, h_2\ \ h \in h_1 \uplus h_2 \Rightarrow \exists m_1, m_2\ \ m \in m_1 \star m_2 \text{ and } h_1\ R_\varphi\ m_1 \text{ and } h_2\ R_\varphi\ m_2 \\ \forall m_1, m_2\ \ m \in m_1 \star m_2 \Rightarrow \exists h_1, h_2\ \ h \in h_1 \uplus h_2 \text{ and } h_1\ R_\varphi\ m_1 \text{ and } h_2\ R_\varphi\ m_2 \\ \forall h_1, h_2\ \ h_2 \in h_1 \uplus h \Rightarrow \exists m_1, m_2\ \ m_2 \in m_1 \star m \text{ and } h_1\ R_\varphi\ m_1 \text{ and } h_2\ R_\varphi\ m_2 \\ \forall m_1, m_2\ \ m_2 \in m_1 \star m \Rightarrow \exists h_1, h_2\ \ h_2 \in h_1 \uplus h \text{ and } h_1\ R_\varphi\ m_1 \text{ and } h_2\ R_\varphi\ m_2 \end{cases}$$

PROOF. Let us first prove that $h\ R_\varphi\ m \Rightarrow (h = \varnothing \text{ iff } m = \pi)$. Let h and m such that $h\ R_\varphi\ m$ holds. Then by definition, we obtain $\varphi(h) = m$. If $m = \pi (= 0)$, then by Property (5) of Proposition C.1, we obtain $h = \varnothing$ and thus $(h, m) \in \{(\varnothing, \pi)\}$. If $m \neq 0$ then by Property (5) of Proposition C.1, we obtain $h \neq \varnothing$ and thus $(h, m) \in \mathbb{M}_f(\mathsf{X}) \backslash \{\pi\}$.

Let us now prove the four co-induction properties. Let h and m such that $h\ R_\varphi\ m$ holds. Then $\varphi(h) = m$ holds.

— Let $h_1, h_2 \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ such that $h \in h_1 \uplus h_2$. Let $m_1 = \varphi(h_1)$ and $m_2 = \varphi(h_2)$. By Property (4) of Proposition C.1, we obtain $m = \varphi(h) \in \varphi(h_1) \star \varphi(h_2) = m_1 \star m_2$, $h_1\ R_\varphi\ m_1$ and $h_2\ R_\varphi\ m_2$;

— Let $m_1, m_2 \in \mathbb{M}_f(\mathsf{X})$ such that $m = m_1 + m_2$. Property (2) of Proposition C.1, there exists $h_1, h_2 \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ such that $\varphi(h_1) = m_1$, $\varphi(h_2) = m_2$ and $h_1 \uplus h_2 = \{h\}$. Hence, $h \in h_1 \uplus h_2$, $h_1\ R_\varphi\ m_1$ and $h_2\ R_\varphi\ m_2$;

— Let $h_1, h_2 \in \mathbb{H}_{\mathsf{L},\mathsf{V}}$ such that $h_2 \in h_1 \uplus h$. Let $m_1 = \varphi(h_1)$ and $m_2 = \varphi(h_2)$. By Property (4) of Proposition C.1, we obtain $m_2 = \varphi(h_2) \in \varphi(h_1) \star \varphi(h) = m_1 \star m$, $h_1\ R_\varphi\ m_1$ and $h_2\ R_\varphi\ m_2$;

— Let $m_1, m_2 \in \mathbb{M}_f(\mathsf{X})$ such that $m_2 = m_1 + m$. By Property (3) of Proposition C.1, let us choose h_1 such that $\mathrm{def}(h_1) \cap \mathrm{def}(h) = \emptyset$ and $\varphi(h_1) = m_1$. Hence, $h_1\ R_\varphi\ m_1$ holds. Since $\mathrm{def}(h_1) \cap \mathrm{def}(h) = \emptyset$, let h_2 be the unique heap such that $h_2 \in h_1 \uplus h$. By Property (4) of Proposition C.1, we obtain $\varphi(h_2) = \varphi(h_1) + \varphi(h) = m_1 + m = m_2$. Hence $h_2\ R_\varphi\ m_2$ holds.

□

LEMMA 7.6. *Let* X *be a set. For* $\mathsf{L} = \mathsf{X} \times \mathbb{N}$ *and* $\mathsf{V} = \{*\}$*, there exists a surjective map* $\varphi : \mathbb{H}_{\mathsf{L},\mathsf{V}} \longrightarrow \mathbb{M}_f(\mathsf{X})$ *such that for any Kripke interpretation* $\delta : \mathsf{Var} \longrightarrow \mathbb{P}(\mathbb{M}_f(\mathsf{X}))$ *in the free monoid* $(\mathbb{M}_f(\mathsf{X}), \star, \pi)$*, the Kripke interpretation* $\delta' : \mathsf{Var} \longrightarrow \mathbb{P}(\mathbb{H}_{\mathsf{L},\mathsf{V}})$ *in the heap monoid* $(\mathbb{H}_{\mathsf{L},\mathsf{V}}, \uplus, \emptyset)$ *defined by* $\delta' = v \mapsto \varphi^{-1}(\delta(v))$ *satisfies the following property:*

$$h \Vdash_{\delta'} F \quad \text{if and only if} \quad \varphi(h) \Vdash_{\delta} F \qquad \text{for any } F \in \mathsf{Form}$$

PROOF. By induction on the structure of F, we prove the following property:

$$\forall h, m \quad h\, R_\varphi\, m \Rightarrow (h \Vdash_{\delta'} F \text{ iff } m \Vdash_\delta F)$$

Let us proceed by case analysis on the structure of F:

— if F is reduced to a logical variable $v \in \mathsf{Var}$, then $h\, R_\varphi\, m$ implies $\varphi(h) = m$ and thus we compute: $h \Vdash_{\delta'} v$ iff $h \in \delta'(v)$ iff $h \in \varphi^{-1}(\delta(v))$ iff $\varphi(h) \in \delta(v)$ iff $m \in \delta(v)$ iff $m \Vdash_\delta v$;

— if F is the multiplicative unit I then the relation reduces to $h\, R_\varphi\, m \Rightarrow (h = \emptyset \text{ iff } m = \pi)$ which is a consequence of Lemma C.2;

— if $F = A * B$, let us suppose $h \Vdash_{\delta'} A * B$ and let us prove $m \Vdash_\delta A * B$. By definition of Kripke semantics, there exists h_1, h_2 such that $h \in h_1 \uplus h_2$, $h_1 \Vdash_{\delta'} A$ and $h_2 \Vdash_{\delta'} B$. Since $h\, R_\varphi\, m$, by Lemma C.2, we obtain m_1, m_2 such that $m \in m_1 \star m_2$, $h_1\, R_\varphi\, m_1$ and $h_2\, R_\varphi\, m_2$. By induction, we get $m_1 \Vdash_\delta A$ and $m_2 \Vdash_\delta B$. Hence, by definition of Kripke semantics, we deduce $m \Vdash_\delta A * B$. We proceed in a perfectly symmetric way for $m \Vdash_\delta A * B \Rightarrow h \Vdash_{\delta'} A * B$;

— if $F = A \mathrel{-\!\!*} B$, let us suppose $h \Vdash_{\delta'} A \mathrel{-\!\!*} B$ and let us prove $m \Vdash_\delta A \mathrel{-\!\!*} B$. So let us m_1, m_2 consider such that $m_2 \in m_1 \star m$ and $m_1 \Vdash_\delta A$ and let us prove that $m_2 \Vdash_\delta B$. Since $h\, R_\varphi\, m$, by Lemma C.2, we obtain h_1, h_2 such that $h_2 \in h_1 \uplus h$, $h_1\, R_\varphi\, m_1$ and $h_2\, R_\varphi\, m_2$. By induction, we get $h_1 \Vdash_{\delta'} A$. Hence, by definition of Kripke semantics for $\mathrel{-\!\!*}$, we deduce $h_2 \Vdash_{\delta'} B$. By induction again, we derive $m_2 \Vdash_\delta B$. Symmetrically we obtain $m \Vdash_\delta A \mathrel{-\!\!*} B \Rightarrow h \Vdash_{\delta'} A \mathrel{-\!\!*} B$;

— if the outermost connective of F is not multiplicative, i.e. belongs to $\{\bot, \top, \neg, \vee, \wedge, \rightarrow\}$, then the equivalence is trivially obtained from the induction hypothesis because of the point-wise definition of the Kripke semantics of non-linear connectives.

□

REFERENCES

BOUAJJANI, A., ESPARZA, J., AND MALER, O. 1997. Reachability Analysis of Pushdown Automata: Application to Model-Checking. In *CONCUR'97: Concurrency Theory, 8th International Conference, Warsaw, Poland*. Lecture Notes in Computer Science Series, vol. 1243. Springer, 135–150.

BROTHERSTON, J. 2010. A Unified Display Proof Theory for Bunched Logic. *Electronic Notes in Theoretical Computer Science 265*, 197–211.

BROTHERSTON, J. AND CALCAGNO, C. 2009. Classical BI: a logic for reasoning about dualising resources. In *Proceedings of the 36th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, Savannah, GA, USA*. ACM, 328–339.

BROTHERSTON, J. AND KANOVICH, M. I. 2010. Undecidability of Propositional Separation Logic and Its Neighbours. In *Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science, Edinburgh, United Kingdom*. IEEE Computer Society, 130–139.

CALCAGNO, C., CARDELLI, L., AND GORDON, A. 2005. Deciding Validity in a Spatial Logic for Trees. *Journal of Functional Programming 15,* 4, 543–572.

CALCAGNO, C., O'HEARN, P. W., AND YANG, H. 2007. Local Action and Abstract Separation Logic. In *22nd IEEE Symposium on Logic in Computer Science, Wroclaw, Poland*. IEEE Computer Society, 366–378.

DE GROOTE, P., GUILLAUME, B., AND SALVATI, S. 2004. Vector addition tree automata. In *Proceedings of the 19th IEEE Symposium on Logic in Computer Science, Turku, Finland*. IEEE Computer Society, 64–73.

GALMICHE, D. AND LARCHEY-WENDLING, D. 2006. Expressivity properties of Boolean BI through relational models. In *FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science, 26th International Conference, Kolkata, India*. Lecture Notes in Computer Science Series, vol. 4337. Springer, 357–368.

Galmiche, D., Méry, D., and Pym, D. 2005. The semantics of BI and resource tableaux. *Mathematical Structures in Computer Science 15,* 6, 1033–1088.

Ghilardi, S. and Meloni, G. 1990. Modal logics with n-ary connectives. *Zeitschr. f. math. Logik und Grundlagen d. Math 36*, 193–215.

Girard, J.-Y. 1987. Linear logic. *Theoretical Computer Science 50,* 1, 1–102.

Ishtiaq, S. and O'Hearn, P. 2001. BI as an Assertion Language for Mutable Data Structures. In *Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming languages, London, England*. ACM, 14–26.

Kanovich, M. 1994. Linear Logic as a Logic of Computations. *Annals of Pure and Applied Logic 67,* 1–3, 183–212.

Kanovich, M. 1995. The direct simulation of Minsky machines in linear logic. In *Advances in Linear Logic*, J.-Y. Girard, Y. Lafont, and L. Regnier, Eds. London Mathematical Society Lecture Note Series, vol. 222. Cambridge University Press, Chapter 2, 123–145.

Lafont, Y. 1996. The undecidability of second order linear logic without exponentials. *Journal of Symbolic Logic 61,* 2, 541–548.

Lafont, Y. and Scedrov, A. 1996. The undecidability of second order multiplicative linear logic. *Information and Computation 125,* 1, 46–51.

Larchey-Wendling, D. 2010. An Alternative Direct Simulation of Minsky Machines into Classical Bunched Logics via Group Semantics. *Electronic Notes in Theoretical Computer Science 265*, 369–387.

Larchey-Wendling, D. and Galmiche, D. 2009. Exploring the relation between Intuitionistic BI and Boolean BI: an unexpected embedding. *Mathematical Structures in Computer Science 19,* 3, 435–500.

Larchey-Wendling, D. and Galmiche, D. 2010. The Undecidability of Boolean BI through Phase Semantics. In *Proceedings of the 25th Annual IEEE Symposium on Logic in Computer Science, Edinburgh, United Kingdom*. IEEE Computer Society, 140–149.

Martí-Oliet, N. and Meseguer, J. 1991. From Petri nets to linear logic. *Mathematical Structures in Computer Science 1,* 1, 69–101.

Minsky, M. 1961. Recursive unsolvability of Post's problem of 'tag' and other topics in the theory of Turing machines. *Annals of Mathematics 74,* 3, 437–455.

O'Hearn, P. and Pym, D. 1999. The Logic of Bunched Implications. *Bulletin of Symbolic Logic 5,* 2, 215–244.

Okada, M. 2002. A uniform semantic proof for cut-elimination and completeness of various first and higher order logics. *Theoretical Computer Science 281,* 1–2, 471–498.

Pym, D. 2002. *The Semantics and Proof Theory of the Logic of Bunched Implications*. Applied Logic Series Series, vol. 26. Kluwer Academic Publishers. Errata available at `http://www.cs.ac.uk/~pym/pym-tofts-fac-errata.pdf`.

Reisig, W. 1985. *Petri Nets, An Introduction*. EATCS, Monographs on Theoretical Computer Science. Springer Verlag.

Troelstra, A. 1992. *Lectures on Linear Logic*. Lecture Notes Series, vol. 29. CSLI, Stanford, California.

Yetter, D. 1990. Quantales and (Noncommutative) Linear Logic. *Journal of Symbolic Logic 55,* 1, 41–64.

Received May 2011; revised October 2011; accepted February 2012