Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science 265 (2010) 369–387
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

An Alternative Direct Simulation of Minsky Machines into Classical Bunched Logics via Group Semantics

Dominique Larchey-Wendling

LORIA – CNRS, UMR 7503
Vandœuvre-lès-Nancy, France

Abstract

Recently, Brotherston & Kanovich, and independently Larchey-Wendling & Galmiche, proved the undecidability of the bunched implication logic BBI. Moreover, Brotherston & Kanovich also proved the undecidability of the related logic CBI, as well as its neighbours. All of the above results are based on encodings of two-counter Minsky machines, but are derived using different techniques. Here, we show that the technique of Larchey-Wendling & Galmiche can also be extended, via group Kripke semantics, to prove the undecidability of CBI. Hence, we propose an alternative direct simulation of Minsky machines into both BBI and CBI. We identify a fragment called elementary Boolean BI (eBBI) which is common to the BBI/CBI families of logics and we show that the problem of Minsky machine acceptance can be encoded into eBBI. The soundness of the encoding is derived from the soundness of a goal directed sequent calculus designed for eBBI. The faithfulness of the encoding is obtained from a Kripke model based on the free commutative group $\mathbb{Z}^n$.

Keywords: Boolean/classical bunched logics, Kripke semantics, Minsky machines, decidability.

1 Introduction

The logic of bunched implications of Pym and O'Hearn [16] contains two important families of logics: Boolean BI (BBI) and Classical BI (CBI). BBI is the core logical framework of separation logic, and has been well studied for a number of years [2,7,13]. CBI was introduced more recently by Brotherston and Calcagno [3]. The undecidability of BBI, which was a long-standing open problem, was recently established independently by two groups of researchers [5,14]. Using different techniques, both Larchey-Wendling & Galmiche [14] and Brotherston & Kanovich [5] derived the undecidability of BBI from a (different) encoding of two counter Minsky machines into a fragment of BBI. Moreover, Brotherston and Kanovich's results also include the undecidability of CBI (and its neighbours), again via an encoding of Minsky machines [5]. The aim of the present paper is to show that the technique

1571-0661© 2010 Elsevier B.V. Open access under CC BY-NC-ND license.
doi:10.1016/j.entcs.2010.08.022

of [14] can also be adapted, via group Kripke semantics, to simultaneously prove the undecidability of both BBI and CBI.

Recall that the logic BI of bunched implications [16] 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 [17]. Later, Galmiche *et al.* [8] 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 with 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 as the first investigated variant of BI which contained a negation: BBI combines intuitionistic multiplicatives with Boolean additives. This focus on BBI is the consequence of the natural links between BBI and separation or spatial logics. Indeed, for instance, the pure part of separation logic is essentially obtained by considering a particular model of BBI, based on a (partial) monoid of heaps [11] (see [13] for a more general discussion on these links). The Hilbert proof-system of BBI was proved complete w.r.t. *relational (or non-deterministic) Kripke semantics* [7]. 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.

Then *Classical* BI (CBI) was introduced [3] as a bunched logic which contained both a multiplicative negation and an additive negation. It could be used as a basis for resource models which contain a dualizing operator. For this logic, Brotherston and Calcagno [4] provided a Display calculus *à la Belnap* and established its soundness and completeness both w.r.t. the Hilbert proof-system and (dualizing) relational Kripke semantics. They proved cut-elimination as a by product of their Display proof-system and described a substantial part of the model theory of CBI, including the proof of the incompleteness of CBI w.r.t. the (dualizing) *partial monoidal Kripke semantics.* However, no decidability result followed from these achievements.

Then, back to BBI, two main families of results emerged giving a contrasted view of its proof-theory. On the one hand, Brotherston [2] adapted the Display proof-system of CBI 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 [13] 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. To complete the picture, Larchey-Wendling and Galmiche [14] recently established that relational Kripke semantics and partial monoidal Kripke semantics define different notions of (universal) validity in BBI, as in CBI [4]. Nevertheless, all the logics defined by theses classes of models are undecidable, as explained in [5,14] and the present paper.

Indeed, our aim here is to show that it is possible to find an encoding of Minsky machines that is suitable for both BBI and CBI, even when restricted to simple subclasses of models like commutative groups. A different encoding of Minsky machines in CBI was already proposed in [5], with the consequence of the undecidability of CBI. However it corresponds to classes of separation models and would not apply to commutative groups because it requires that the models have *indivisible units.* [1] The faithfulness of our encoding is established by building a model of CBI based on the group $\mathbb{Z}^n$ where n is the number of counters of the Minsky machine. Thus, this model suits for both BBI and CBI whether one considers relational, partial monoidal, total monoidal, or even group Kripke semantics. As a consequence, both BBI and CBI are undecidable even when their Kripke semantics is restricted $\mathbb{Z} \times \mathbb{Z}$.

The paper is structured as following: we first outline the Kripke model theory of BBI/CBI based on the notion of non-deterministic (or relational monoid) and recall different results w.r.t. the semantics of both logics on particular sub-classes of models. Then we introduce a fragment of BBI/CBI which we call elementary BBI (eBBI). This fragment is provided with a set of sound goal-directed sequent calculus rules called gBBI. Then, we present an encoding of Minsky machines acceptance into elementary BBI. For each input $\mathsf{m} \in \mathbb{N}^n$ of the machine, we compute a sequent S_m in eBBI. We prove the soundness of this encoding: if m is accepted by the Minsky machine then S_m has a proof tree in gBBI. This proof tree is extracted from the successful computation of the Minsky machine starting with m. The faithfulness of the encoding is established by building a model based on the group $\mathbb{Z}^n$. Hence, if S_m is semantically valid in Kripke semantics (even when the semantic interpretation is restricted to the group $\mathbb{Z}^n$) then the Minsky machine accepts the input m.

2 Non-Deterministic Monoids and Groupoids

In this section, we present the algebraic notions necessary for the definition of the relational Kripke semantics of BBI/CBI. Let us consider a set M. We denote by $\mathcal{P}(M)$ the powerset of M, i.e. its set of subsets. A binary function $\circ : M \times M \longrightarrow \mathcal{P}(M)$ is naturally extended to a binary operator on $\mathcal{P}(M)$ by

$$X \circ Y = \bigcup \{x \circ y \mid x \in X, y \in Y\} \tag{1}$$

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

Definition 2.1 A *non-deterministic (or relational) monoid* is a tuple $(M, \circ, \epsilon)$ where $\epsilon \in M$ and $\circ : M \times M \longrightarrow \mathcal{P}(M)$. We require the following conditions to hold:

[1] The unit ϵ is indivisible if the following property holds: $\forall x, y \;\; x \circ y = \epsilon \Rightarrow x = y = \epsilon$.

(i) $\forall a \in M, \epsilon \circ a = \{a\}$ (neutrality)

(ii) $\forall a, b \in M, a \circ b = b \circ a$ (commutativity)

(iii) $\forall a, b, c \in M, a \circ (b \circ c) = (a \circ b) \circ c$ (associativity)[2]

The term *non-deterministic* was introduced in [7] 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 $(M, \bullet, \mathsf{e})$ is a (usual) commutative monoid then, defining $a \circ b = \{a \bullet b\}$ and $\epsilon = \mathsf{e}$ induces a non-deterministic monoid $(M, \circ, \epsilon)$. Using the bijection $x \mapsto \{x\}$ mapping elements of M to singletons in $\mathcal{P}(M)$, 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.

The term *relational* is sometimes used because the map $\circ : M \times M \longrightarrow \mathcal{P}(M)$ can equivalently be understood as a ternary relation $- \circ - \ni - : M \times M \times M \longrightarrow \{0, 1\}$ through the Curry-Howard isomorphism and the axioms correspond to those of an internal monoid in the category of relations [9]. The two presentations are equivalent but we rather use the monoidal presentation in this paper.

Proposition 2.2 *The extension of $\circ$ to $\mathcal{P}(M)$ defined by (1) induces a commutative monoidal structure with unit element $\{\epsilon\}$ on $\mathcal{P}(M)$.*

The proof of this trivial proposition is left to the reader. As a consequence of Proposition 2.2, the denotation $a_1 \circ \cdots \circ a_k$ is unambiguous for any multiset $\{a_1, \ldots, a_k\}$ because it is identical to the product $\{a_1\} \circ \cdots \circ \{a_k\}$ in the commutative monoid $\mathcal{P}(M)$.

Proposition 2.3 *For any $m \in M$ and any $X, Y \in \mathcal{P}(M)$, if $m \in X \circ Y$ then there exists $x \in X$ such that $m \in x \circ Y$.*

This is a direct consequence of the defining equation (1) of the extension of $\circ$ to $\mathcal{P}(M)$. As a particular case, if $m \in a_1 \circ \cdots \circ a_k \circ b_1 \circ \cdots \circ b_p$ then there exists $\alpha \in a_1 \circ \cdots \circ a_k$ such that $m \in \alpha \circ b_1 \circ \cdots \circ b_p$.

Let $(M, \circ, \epsilon)$ be a non-deterministic monoid. It is a *partial deterministic monoid* if for any $x, y \in M$, the composition $x \circ y$ is either empty or a singleton. $(M, \circ, \epsilon)$ is a *total deterministic monoid* if for any $x, y \in M$, the composition $x \circ y$ is a singleton. If moreover for every $x \in M$ there exists y such that $\epsilon \in x \circ y$ then $(M, \circ, \epsilon)$ is a *total deterministic group*. Total deterministic monoids exactly correspond to those non-deterministic monoids derived from usual commutative monoid.

Definition 2.4 The class of non-deterministic (resp. partial deterministic, resp. total deterministic) monoids is denoted NDm (resp. Dm, resp. Tm). The class of total deterministic groups is denoted G.

Proposition 2.5 *The strict inclusions* $\mathrm{G} \subsetneq \mathrm{Tm} \subsetneq \mathrm{Dm} \subsetneq \mathrm{NDm}$ *hold.*

[2] Associativity should be understood using the extension (1) of $\circ$ to $\mathcal{P}(M)$.

Proof. The inclusion between those classes of non-deterministic monoids is obvious. We illustrate NDm $\nsubseteq$ Dm by the following structure: $(\{\epsilon, \mathtt{x}, \mathtt{y}\}, \circ, \epsilon)$ where $\mathtt{x} \circ \mathtt{x} = \{\epsilon, \mathtt{y}\}$ and $\mathtt{y} \circ \alpha = \{\mathtt{y}\}$ for any $\alpha \in \{\epsilon, \mathtt{x}, \mathtt{y}\}$. □

Definition 2.6 A *non-deterministic groupoid* is a tuple $(M, \circ, \epsilon, -, \infty)$ where $(M, \circ, \epsilon)$ is a non-deterministic monoid and $- : M \longrightarrow M$ and $\infty \in M$ satisfy:

(i) $\forall a \in M, \infty \in a \circ -a$

(ii) $\forall a, b \in M, \infty \in a \circ b \Rightarrow b = -a$

The *pseudo inverse* operator $-$ is extended point-wise to $\mathcal{P}(M) \longrightarrow \mathcal{P}(M)$ by $-X = \{-x \mid x \in X\}$. The identities $-\epsilon = \infty$ and $--x = x$ hold for any $x \in M$. The reader can find proofs of these identities in [3] as well as many examples of non-deterministic groupoids (called CBI-models there), though many of them are only partial deterministic.

Let $(M, \circ, \epsilon, -, \infty)$ be a non-deterministic groupoid. It is a *partial deterministic groupoid* if for any $x, y \in M$, the composition $x \circ y$ is either empty or a singleton. $(M, \circ, \epsilon, -, \infty)$ is a *total deterministic groupoid* if for any $x, y \in M$, the composition $x \circ y$ is a singleton. If moreover $\epsilon = \infty$ then $(M, \circ, \epsilon, -, \infty)$ is a *total deterministic group*.

Definition 2.7 The class of non-deterministic (resp. partial deterministic, resp. total deterministic) groupoids is denoted NDg (resp. Dg, resp. Tg). The class of total deterministic groups is denoted G.

Remark that there is no contradiction in the definition of total deterministic groups (class G) from Definition 2.4 and Definition 2.7 because in this case, the inverse and the pseudo inverse are identical operators.

Proposition 2.8 *The strict inclusions* G $\subsetneq$ Tg $\subsetneq$ Dg $\subsetneq$ NDg *hold.*

Proof. See [3,4] for a justification of the strictness of the inclusions. For instance, the *bit-arithmetic model* is a witness for Tg $\nsubseteq$ G. □

3 Kripke Semantics for BBI and CBI

We first present the syntax of BBI and CBI. In fact, the operators of BBI form a strict subset of the operator of CBI. The formulae of CBI are defined as following: starting from a set Var, they are freely build using the *logical variables* in Var, the *logical constants* in $\{\mathsf{O}, \mathsf{I}, \top, \bot\}$, the unary connectives in $\{\sim, \neg\}$ or the binary connectives in $\{*, -\!\!*, \wedge\}$. The formulae of BBI are those formulae of CBI that contain neither O nor $\sim$. Formally, the set of formulae of BBI/CBI is described by the following grammar:

$$\mathsf{BBI} \;:\; A ::= v \mid \mathsf{I} \mid \top \mid \bot \mid \neg A \mid A * A \mid A -\!\!* A \mid A \wedge A$$

$$\mathsf{CBI} \;:\; A ::= v \mid \mathsf{O} \mid \mathsf{I} \mid \top \mid \bot \mid \sim A \mid \neg A \mid A * A \mid A -\!\!* A \mid A \wedge A$$

with $v \in \mathsf{Var}$. Hence, BBI appears as a fragment of CBI.[3] If $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(M)$ is an interpretation of variables where $\mathcal{M} = (M, \circ, \epsilon)$ is a non-deterministic monoid, then we say that $(\mathcal{M}, \delta)$ is a *model of* BBI. On the other hand, if $(M, \circ, \epsilon, -, \infty)$ is a non-deterministic groupoid, we say that $(\mathcal{M}, \delta)$ is a *model of* CBI. We define the Kripke interpretation of the formulae of $\mathsf{BBI}/\mathsf{CBI}$ from a given model $(\mathcal{M}, \delta)$ of $\mathsf{BBI}/\mathsf{CBI}$, by induction on the structure of formulae:

$$\begin{array}{rcl@{\qquad}rcl}
m \Vdash v & \text{iff} & m \in \delta(v) & & & \\
m \Vdash \bot & \text{iff} & \text{never} & m \Vdash \mathsf{O} & \text{iff} & m \neq \infty \\
m \Vdash \top & \text{iff} & \text{always} & m \Vdash \mathsf{I} & \text{iff} & m = \epsilon \\
m \Vdash \neg A & \text{iff} & m \nVdash A & m \Vdash \sim A & \text{iff} & -m \nVdash A
\end{array}$$

$$\begin{array}{rcl}
m \Vdash A \wedge B & \text{iff} & m \Vdash A \text{ and } m \Vdash B \\
m \Vdash A * B & \text{iff} & \exists a, b,\ m \in a \circ b \text{ and } a \Vdash A \text{ and } b \Vdash B \\
m \Vdash A \mathrel{-\!\!*} B & \text{iff} & \forall a, b\ (b \in m \circ a \text{ and } a \Vdash A) \Rightarrow b \Vdash B
\end{array}$$

A formula F is *valid in the model* $((M, \circ, \ldots), \delta)$ if $m \Vdash F$ holds for any $m \in M$. A formulae F is *valid in a structure* $\mathcal{M} = (M, \circ, \ldots)$ if for any interpretation $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(M)$ of propositional variables, F is valid in the model $(\mathcal{M}, \delta)$. A *counter-model* of the formula F of BBI (resp. CBI) is given by a non-deterministic monoid (resp. groupoid) $(M, \circ, \ldots)$, an interpretation $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(M)$ and an element $m \in M$ such that $m \nVdash F$.

Definition 3.1 We denote by $\mathsf{BBI}_{\mathrm{ND}}$ (resp. $\mathsf{BBI}_{\mathrm{D}}$, $\mathsf{BBI}_{\mathrm{T}}$, $\mathsf{BBI}_{\mathrm{G}}$, $\mathsf{CBI}_{\mathrm{ND}}$, $\mathsf{CBI}_{\mathrm{D}}$, $\mathsf{CBI}_{\mathrm{T}}$, $\mathsf{CBI}_{\mathrm{G}}$) the set of formulae of BBI (resp. CBI) which are valid in every structure belonging to the class NDm (resp. Dm, Tm, G, NDg, Dg, Tg, G).

The following theorem collects some previously known results (see below) with a new one, namely $\mathsf{CBI}_{\mathrm{T}} \not\subseteq \mathsf{CBI}_{\mathrm{D}}$, to give an overview of the relations between the different flavors of BBI and CBI.

Theorem 3.2 *The two following inclusions sequences hold:*

$$(i)\ \ \mathsf{BBI}_{\mathrm{ND}} \subsetneq \mathsf{BBI}_{\mathrm{D}} \subsetneq \mathsf{BBI}_{\mathrm{T}} \subsetneq \mathsf{BBI}_{\mathrm{G}} \qquad (ii)\ \ \mathsf{CBI}_{\mathrm{ND}} \subsetneq \mathsf{CBI}_{\mathrm{D}} \subsetneq \mathsf{CBI}_{\mathrm{T}} \subsetneq \mathsf{CBI}_{\mathrm{G}}$$

Proof. For a given $\mathsf{BBI}/\mathsf{CBI}$-model $\mathcal{M} = (M, \circ, \epsilon, \ldots)$, the following table lists the

[3] We did not include the two other additive connectives $\vee$ and $\rightarrow$ or the other multiplicative connective $\mathbin{\vee\!\!\!*}$ which we consider definable in $\mathsf{BBI}/\mathsf{CBI}$ by the De Morgan equations $A \vee B = \neg(\neg A \wedge \neg B)$, $A \rightarrow B = \neg(A \wedge \neg B)$ and $A \mathbin{\vee\!\!\!*} B = \sim(\sim A * \sim B)$.

Kripke interpretations of some $\mathsf{BBI}/\mathsf{CBI}$ formulae in the model $\mathcal{M}$:

Name	Formula F	$m \Vdash F$	BBI	CBI
	$\neg\,\mathsf{O}$	$m = \infty$		✓
$\mathcal{I}$	$\neg(\top \mathrel{-\!\!*} \neg\,\mathsf{I})$	$\epsilon \in m \circ M$	✓	✓
$\mathcal{T}$	$(\neg\,\mathsf{I} \mathrel{-\!\!*} \bot) \rightarrow \mathsf{I}$	$m \circ (M \backslash \{\epsilon\}) = \emptyset \Rightarrow m = \epsilon$	✓	✓
$\mathcal{K}$	$\neg(\neg\,\mathsf{O} \mathrel{-\!\!*} \neg\,\mathsf{I})$	$\epsilon \in m \circ \infty$		✓
$\mathcal{L}$	$\neg\,\mathsf{O} \mathrel{-\!\!*} \mathsf{I}$	$m \circ \infty \subseteq \{\epsilon\}$		✓
$\mathcal{O}$	$\mathsf{O} \vee \mathsf{I}$	$\infty = \epsilon$		✓
$\mathcal{O}'$	$(\neg\,\mathsf{O} * \neg\,\mathsf{O}) \rightarrow \neg\,\mathsf{O}$	$m \in \infty \circ \infty \Rightarrow m = \infty$		✓
$\square\, A$	$\top * (\mathsf{I} \wedge (\top \mathrel{-\!\!*} A))$	$\forall x \in M,\, x \Vdash A$	✓	✓

For $\mathsf{BBI}_{\mathrm{D}} \not\subseteq \mathsf{BBI}_{\mathrm{ND}}$ (resp. $\mathsf{BBI}_{\mathrm{T}} \not\subseteq \mathsf{BBI}_{\mathrm{D}}$), the witness formula $(\mathcal{I} * \mathcal{I}) \rightarrow \mathcal{I}$ (resp. $\mathcal{T}$) was given in [14]. The formula $\mathcal{I}$ encodes invertibility in $\mathsf{BBI}/\mathsf{CBI}$, thus $\mathcal{I}$ belongs to $\mathsf{BBI}_{\mathrm{G}}$ but not to $\mathsf{BBI}_{\mathrm{T}}$. Hence $\mathsf{BBI}_{\mathrm{G}} \not\subseteq \mathsf{BBI}_{\mathrm{T}}$.

For $\mathsf{CBI}_{\mathrm{D}} \not\subseteq \mathsf{CBI}_{\mathrm{ND}}$, the witness formula $\mathcal{K} \rightarrow \mathcal{L}$ was given in [4]. The formula $\mathcal{O}$ encodes the equation $\infty = \epsilon$ and is thus a witness for $\mathsf{CBI}_{\mathrm{G}} \not\subseteq \mathsf{CBI}_{\mathrm{T}}$.

Let us provide a witness for $\mathsf{CBI}_{\mathrm{T}} \not\subseteq \mathsf{CBI}_{\mathrm{D}}$. The formula $\mathcal{O}'$ is valid in a structure of the class Tg if and only if $\infty = \epsilon$ and thus the structure must also be of the class G and hence, the formula $\mathcal{O}$ must also be valid in that structure. Hence the formula $\square\, \mathcal{O}' \rightarrow \mathcal{O}$ belongs to $\mathsf{CBI}_{\mathrm{T}}$.

Let us show that $\square\, \mathcal{O}' \rightarrow \mathcal{O}$ does not belong to $\mathsf{CBI}_{\mathrm{D}}$. Consider the partial deterministic groupoid $\mathcal{M} = (\{\epsilon, \mathtt{x}, \mathtt{y}, \infty\}, \circ, \epsilon, -, \infty)$ defined by the following tables:

$\circ$	ϵ	$\mathtt{x}$	$\mathtt{y}$	∞
ϵ	$\{\epsilon\}$	$\{\mathtt{x}\}$	$\{\mathtt{y}\}$	$\{\infty\}$
$\mathtt{x}$	$\{\mathtt{x}\}$	$\emptyset$	$\{\infty\}$	$\emptyset$
$\mathtt{y}$	$\{\mathtt{y}\}$	$\{\infty\}$	$\emptyset$	$\emptyset$
∞	$\{\infty\}$	$\emptyset$	$\emptyset$	$\emptyset$

	$-$
ϵ	∞
$\mathtt{x}$	$\mathtt{y}$
$\mathtt{y}$	$\mathtt{x}$
∞	ϵ

There is no need to provide δ because no logical variable appear in the formulae we consider. We let the reader check that the structure $\mathcal{M}$ verifies the axioms of non-deterministic groupoids. Thus, $\mathcal{M} \in \mathrm{Dg}$ holds. The formula $\mathcal{O}'$ is valid in this structure because $\infty \circ \infty = \emptyset$. Hence, $\square\, \mathcal{O}'$ is valid in $\mathcal{M}$. Obviously $\infty \neq \epsilon$ holds in $\mathcal{M}$ and thus $\mathcal{M}$ is a counter-model to the formula $\square\, \mathcal{O}' \rightarrow \mathcal{O}$. Moreover, $\mathcal{M}$ belongs to the class Dg. □

We do not discuss the relations between the different sub-classes of $\mathsf{BBI}/\mathsf{CBI}$ models further. See [3,5,13,14] for a more detailed presentation.

$$\frac{}{A \vdash A}\,\langle\text{id}\rangle \qquad \frac{\Gamma \vdash B}{\Gamma, \mathsf{I} \wedge A \vdash B}\,\langle\text{w}\rangle \qquad \frac{\Gamma, \mathsf{I} \wedge A, \mathsf{I} \wedge A \vdash B}{\Gamma, \mathsf{I} \wedge A \vdash B}\,\langle\text{c}\rangle \qquad \frac{\Gamma, A \vdash B}{\Gamma, \mathsf{I} \wedge A \vdash B}\,\langle \mathsf{I}_L \rangle$$

$$\frac{\Gamma \vdash A \qquad \Delta, B \vdash C}{\Gamma, \Delta, A \mathrel{-\!\!*} B \vdash C}\,\langle \mathrel{-\!\!*}_L \rangle \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \mathrel{-\!\!*} B}\,\langle \mathrel{-\!\!*}_R \rangle \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,\langle \wedge_R \rangle$$

Fig. 1. Sequent calculus rules for BBI/CBI

4 Sequents for BBI/CBI

Contrary to (intuitionistic) BI or Linear Logic [10,18], bunched logics with classical additives like BBI and CBI are usually not described by sequent calculi. There is no known sequent calculus enjoying decent proof-theoretical properties like cut-elimination or the sub-formula property. Only Display style proof-systems exist for BBI/CBI [2,3]. Nevertheless, we present a set of sound sequent calculus rules with are suitable for many bunched logics with classical additives, because they preserve validity in a particular model.

Let us consider a fixed BBI or CBI model $(\mathcal{M}, \delta)$ with $\delta : \mathsf{Var} \longrightarrow \mathcal{M}$, depending on whether we only want to interpret the fragment BBI or full CBI.

Definition 4.1 A *sequent* is a pair denoted $\Gamma \vdash B$ where Γ is a multiset of formulae and B is a single formula. The sequent $A_1, \ldots, A_p \vdash B$ is *valid* in the model $(\mathcal{M}, \delta)$ and we write $(\mathcal{M}, \delta) \Vdash A_1, \ldots, A_p \vdash B$ if

$$\forall m, m_1, \ldots, m_p \in \mathcal{M}, (m \in m_1 \circ \ldots \circ m_p \text{ and } \forall i, m_i \Vdash A_i) \text{ implies } m \Vdash B \qquad (2)$$

When $\Gamma \vdash B$ is valid in the model $(\mathcal{M}, \delta)$, we also say that $(\mathcal{M}, \delta)$ is a *model of the sequent* $\Gamma \vdash B$.

Because of the associativity and commutativity of $\circ$, property (2) is stable by permutation of the A_i's and thus, validity is a well-defined notion for sequents. *Universal validity* w.r.t. a sub-class of non-deterministic monoids (resp. groupoids) means validity in all the models belonging to that particular sub-class. With Definition 4.1, we derive the following obvious result:

Proposition 4.2 *The sequent $A_1, \ldots, A_p \vdash B$ is valid in $(\mathcal{M}, \delta)$ if and only if the formula $\neg((A_1 * \cdots * A_p) \wedge \neg B)$ is valid in $(\mathcal{M}, \delta)$.*

4.1 Sequent Calculi for BBI/CBI

In general, a proof rule is *sound* if it preserves universal validity from the premises to the conclusion. A proof rule is *strongly sound* if it preserves models from the premises to the conclusion. Hence strong soundness implies soundness. The next result establishes the strong soundness of the sequent calculus rules of Figure 1. Remark that these sequent rules can be viewed as a subset of the rules of intuitionistic linear logic where the exponential $!A$ has been replaced by $\mathsf{I} \wedge A$.

Proposition 4.3 *The rules of Figure 1 preserve validity in the model $(\mathcal{M}, \delta)$.*

$$\frac{}{\Sigma^{\mathsf{I}}, A \vdash A}\ \langle\mathrm{Ax}\rangle \qquad\qquad \frac{\Sigma^{\mathsf{I}}, \Gamma \vdash A \qquad \Sigma^{\mathsf{I}}, \Delta \vdash B}{\Sigma^{\mathsf{I}}, \Gamma, \Delta \vdash C}\ A \mathrel{-\!\!\ast} (B \mathrel{-\!\!\ast} C) \in \Sigma$$

$$\frac{\Sigma^{\mathsf{I}}, \Gamma, A \vdash B}{\Sigma^{\mathsf{I}}, \Gamma \vdash C}\ (A \mathrel{-\!\!\ast} B) \mathrel{-\!\!\ast} C \in \Sigma \qquad\qquad \frac{\Sigma^{\mathsf{I}}, \Gamma \vdash A \qquad \Sigma^{\mathsf{I}}, \Gamma \vdash B}{\Sigma^{\mathsf{I}}, \Gamma \vdash C}\ (A \wedge B) \mathrel{-\!\!\ast} C \in \Sigma$$

Fig. 2. gBBI: a set of goal-directed sequent calculus rules for BBI/CBI

The proof of this result is standard and is reproduced in Appendix A. In this paper, we will not use the rules of Figure 1 directly. We rather use a set gBBI of *goal-directed* sequent rules which better correspond to the computation steps of Minsky machines. In the set gBBI of goal-directed rules described in Figure 2, we denote Σ^{I} for the multiset $\Sigma^{\mathsf{I}} = \mathsf{I} \wedge A_1, \ldots, \mathsf{I} \wedge A_k$ when Σ is the multiset $\Sigma = A_1, \ldots, A_k$. Moreover, we name the rules of gBBI according to the form of their corresponding side condition, i.e. $\langle\mathrm{Ax}\rangle$, $\langle(\mathrel{-\!\!\ast})\mathrel{-\!\!\ast}\rangle$, $\langle\mathrel{-\!\!\ast}(\mathrel{-\!\!\ast})\rangle$ and $\langle(\wedge)\mathrel{-\!\!\ast}\rangle$.

Theorem 4.4 *For any* BBI *(resp.* CBI*) model* $(\mathcal{M}, \delta)$*, if a* BBI*-sequent (resp.* CBI*-sequent) has a proof in* gBBI *then it is valid in* $(\mathcal{M}, \delta)$*.*

Proof. First, we show that each rule of gBBI can be obtained as a combination of the rules of Figure 1.

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

$$\dfrac{\begin{array}{c}\dfrac{\dfrac{}{A \vdash A}\ \langle\mathrm{id}\rangle}{}\ \langle\mathrm{w}\rangle \\ \vdots\ \ \text{applied } n \text{ times}\end{array}}{\Sigma^{\mathsf{I}}, A \vdash A}\ \langle\mathrm{w}\rangle$$

case of rule $\langle\mathrel{-\!\!\ast}(\mathrel{-\!\!\ast})\rangle$

$$\dfrac{\begin{array}{c}\dfrac{\dfrac{\Sigma^{\mathsf{I}}, \Gamma \vdash A \qquad \dfrac{\Sigma^{\mathsf{I}}, \Delta \vdash B \qquad \dfrac{}{C \vdash C}\ \langle\mathrm{id}\rangle}{\Sigma^{\mathsf{I}}, \Delta, B \mathrel{-\!\!\ast} C \vdash C}\ \langle\mathrel{-\!\!\ast}_L\rangle}{\Sigma^{\mathsf{I}}, \Gamma, \Sigma^{\mathsf{I}}, \Delta, A \mathrel{-\!\!\ast} (B \mathrel{-\!\!\ast} C) \vdash C}\ \langle\mathrel{-\!\!\ast}_L\rangle}{\dfrac{\Sigma^{\mathsf{I}}, \Gamma, \Sigma^{\mathsf{I}}, \Delta, \mathsf{I} \wedge (A \mathrel{-\!\!\ast} (B \mathrel{-\!\!\ast} C)) \vdash C}{}\ \langle\mathrm{c}\rangle}\ \langle\mathsf{I}_L\rangle \\ \vdots\ \ \text{applied } n+1 \text{ times}\end{array}}{\Sigma^{\mathsf{I}}, \Gamma, \Delta \vdash C}\ \langle\mathrm{c}\rangle$$

case of rule $\langle(\mathrel{-\!\!\ast})\mathrel{-\!\!\ast}\rangle$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Sigma^{\mathsf{I}}, \Gamma, A \vdash B}{\Sigma^{\mathsf{I}}, \Gamma \vdash A \mathrel{-\!\!\ast} B}\ \langle\mathrel{-\!\!\ast}_R\rangle \qquad \dfrac{}{C \vdash C}\ \langle\mathrm{id}\rangle}{\Sigma^{\mathsf{I}}, \Gamma, (A \mathrel{-\!\!\ast} B) \mathrel{-\!\!\ast} C \vdash C}\ \langle\mathrel{-\!\!\ast}_L\rangle}{\Sigma^{\mathsf{I}}, \Gamma, \mathsf{I} \wedge ((A \mathrel{-\!\!\ast} B) \mathrel{-\!\!\ast} C) \vdash C}\ \langle\mathsf{I}_L\rangle}{\Sigma^{\mathsf{I}}, \Gamma \vdash C}\ \langle\mathrm{c}\rangle$$

case of rule $\langle(\wedge)\mathrel{-\!\!\ast}\rangle$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Sigma^{\mathsf{I}}, \Gamma \vdash A \qquad \Sigma^{\mathsf{I}}, \Gamma \vdash B}{\Sigma^{\mathsf{I}}, \Gamma \vdash A \wedge B}\ \langle\wedge_R\rangle \qquad \dfrac{}{C \vdash C}\ \langle\mathrm{id}\rangle}{\Sigma^{\mathsf{I}}, \Gamma, (A \wedge B) \mathrel{-\!\!\ast} C \vdash C}\ \langle\mathrel{-\!\!\ast}_L\rangle}{\Sigma^{\mathsf{I}}, \Gamma, \mathsf{I} \wedge ((A \wedge B) \mathrel{-\!\!\ast} C) \vdash C}\ \langle\mathsf{I}_L\rangle}{\Sigma^{\mathsf{I}}, \Gamma \vdash C}\ \langle\mathrm{c}\rangle$$

Remark that in the cases of rules $\langle\mathrm{Ax}\rangle$ and $\langle\mathrel{-\!\!\ast}(\mathrel{-\!\!\ast})\rangle$, n represents the size of the multiset Σ (counting all the occurrences of the formulae that appear in Σ). Since the rules of rules of Figure 1 preserve validity in $(\mathcal{M}, \delta)$ (see Proposition 4.3), thus the rules of gBBI preserve validity in $(\mathcal{M}, \delta)$. Hence, the root of a proof tree must be a sequent which is valid in $(\mathcal{M}, \delta)$. □

Neither the set of rules of Figure 1 nor the set of rules of Figure 2 constitute a complete proof-system for either $\mathsf{BBI}_{\mathrm{ND}}$ or $\mathsf{CBI}_{\mathrm{ND}}$. However, there exists some completeness results w.r.t. gBBI and fragments of BBI/CBI discussed in Section 4.3. The important property of gBBI in the context of this paper is that gBBI is sufficient to be able to simulate Minsky machines computations and it is the simplest system we could design for such a goal.

4.2 The elementary fragment of BBI

We define a fragment called elementary BBI (eBBI) which is common to BBI and CBI. eBBI will be used to encode Minsky machines and corresponds to an extension of the fragment $\mathsf{s\text{-}IMELL}_0^{\multimap}$ of multiplicative exponential linear logic [6,14].

Definition 4.5 A formula of BBI/CBI is $(\mathrel{-\!\!*}, \wedge)$-*elementary* if it is of the form $(u \mathrel{-\!\!*} v) \mathrel{-\!\!*} w$, $u \mathrel{-\!\!*} (v \mathrel{-\!\!*} w)$ or $(u \wedge v) \mathrel{-\!\!*} w$ where u, v and w are logical variables. *The sequents of the fragment* eBBI 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 $(\mathrel{-\!\!*}, \wedge)$-elementary formulae.

One can view eBBI as a fragment of BBI/CBI through Proposition 4.2 and in this sense, it seems to be a bit simpler than *minimal* BBI as defined in [5]. Validity in eBBI is the restriction of validity in BBI/CBI. Hence (see Theorem 3.2), this notion may depend on the class of models chosen among NDm, Dm, Tm, NDg, Dg, Tg and G. However, by Theorem 4.4, gBBI is sound w.r.t. any of those classes of models. Hence, we are safe as long as we use gBBI to establish validity of eBBI sequents. It is obvious that eBBI is stable by backward application of the rules of gBBI, hence any gBBI proof of a sequent of eBBI contains only sequents of eBBI.

4.3 Completeness issues for gBBI *on the fragment* eBBI

On the fragment eBBI, the question of the completeness of gBBI w.r.t. the different classes of models considered in this paper is still partially open. In [14], the reader can find a proof that gBBI is sound and complete w.r.t. the classes of models NDm, Dm and Tm. We have a proof that gBBI is sound and complete w.r.t. the class Dg. Hence, gBBI is also sound and complete w.r.t. the class NDg. But none of these two proofs would fit for the classes Tg and G. To our knowledge, the question of the completeness of gBBI on the fragment eBBI for the classes Tg and G is open. In general, the question of completeness of fragments w.r.t. subclasses of models can be difficult to solve, as illustrated by the examples of the incompleteness of BBI [14] and CBI [4] w.r.t. partial monoidal Kripke semantics.

5 Encoding Minsky machines in BBI/CBI

We propose an encoding of Minsky machines [15] in BBI/CBI. As in [14], the encoding differs from Kanovich's encoding of Minsky machines in the $(!, \oplus)$-Horn fragment of intuitionistic linear logic [12]. Compared to the encoding proposed in [14], the one we give here is a bit more complex for two reasons. First reason: it is suitable for many counter Minsky machines. Second reason: it is designed such that its faithfulness can be derived from a model taken in the sub-class of groups, more precisely $(\mathbb{Z}^n, +, \mathsf{0})$.[4]

5.1 Many counters Minsky machines

In the following discussion, $n > 0$ represents the *number of counters* of the Minsky machine and $l > 0$ the *number of instructions* of the Minsky machine. The names p, q range over the interval $[1, n]$ and the names $i, j, k, \ldots$ range over the interval $[0, l]$. Hence, the variables n, l, p, q, i, j, k all represent positive integers. The values of the counters of the Minsky machine can be represented by a vector in $\mathbb{N}^n$, that is a n-uplet of the form $\mathsf{m} = (m_1, \ldots, m_n)$. Given the values of counters $\mathsf{m} \in \mathbb{N}^n$ and $p \in [1, n]$, we denote by m_p the value of the p-th counter, that is the p-th component of the vector m. Let us denote by $\mathsf{e}_p = (0, \ldots, 0, 1, 0, \ldots, 0)$ the vector of $\mathbb{N}^n$ with all components to 0 except the p-th which as value 1. Hence, $(\mathsf{e}_1, \ldots, \mathsf{e}_n)$ is the canonical base of $\mathbb{N}^n$ and we have the canonical decomposition: $\mathsf{m} = m_1\mathsf{e}_1 + \cdots + m_n\mathsf{e}_n$. We denote by $\mathsf{0}$ the vector $(0, \ldots, 0)$ where all components are null.

A n-counter Minsky machine with l instructions is given by a total function

$$\psi : [1, l] \longrightarrow \{+\} \times [1, n] \times [0, l] \ \uplus \ \{-\} \times [1, n] \times [0, l] \times [0, l]$$

where, $\uplus$ represents disjoint set union. Minsky machines instructions (incrementation, zero test/decrementation) are encoded as illustrated in the two following examples:

$\psi(1) = (+, 2, 3) \quad \rightsquigarrow$ `1: c[2]:=c[2]+1 ; goto 3`

$\psi(2) = (-, 6, 4, 5) \quad \rightsquigarrow$ `2: if c[6]=0 then goto 4 else c[6]:=c[6]-1 ; goto 5`

where `c[]` contains the array of counters of the Minsky machine.

Given a Minsky machine $\mathcal{M} = (n, l, \psi)$, its *state* is given by the index of the next instruction and the value of the counters. We represent the set $\mathcal{S}(\mathcal{M})$ of states by $\mathcal{S}(\mathcal{M}) = [0, l] \times \mathbb{N}^n$. The computation steps of the machine are represented by a (binary) transition relation between states $\rightarrow_{\mathcal{M}} \subseteq \mathcal{S}(\mathcal{M}) \times \mathcal{S}(\mathcal{M})$. For any two states (i, m) and (i', m'), the relation $(i, \mathsf{m}) \rightarrow_{\mathcal{M}} (i', \mathsf{m}')$ holds if there exists some $p \in [1, n]$ and some $j, k \in [0, l]$ such that one of the following conditions holds:

$$\begin{array}{rl} & \psi(i) = (+, p, i') \text{ and } \mathsf{m}' = \mathsf{m} + \mathsf{e}_p \\ \text{or} & \psi(i) = (-, p, i', k), m_p = 0 \text{ and } \mathsf{m}' = \mathsf{m} \\ \text{or} & \psi(i) = (-, p, j, i'), \mathsf{m}' + \mathsf{e}_p = \mathsf{m} \text{ (and } m_p \neq 0) \end{array}$$

[4] whereas it was the total monoid $(\mathbb{N} \times \mathbb{N}, +, \mathsf{0})$ in [14].

Remark that $(i, \mathsf{m}) \to_{\mathcal{M}} (i', \mathsf{m}')$ does not hold if $i = 0$ because $\psi(0)$ is not defined. Let $\to^\star_{\mathcal{M}}$ be the reflexive and transitive closure of the relation $\to_{\mathcal{M}}$.

We say that the machine $\mathcal{M} = (n, l, \psi)$ accepts the input m if starting from the state $(1, \mathsf{m})$, there exists a sequence of transitions leading to the state $(0, \mathsf{0})$ and we define the set $\mathcal{A}(M)$ of accepted inputs of $\mathcal{M}$ by:

$$\mathcal{A}(\mathcal{M}) = \big\{\mathsf{m} \in \mathbb{N}^n \mid (1, \mathsf{m}) \to^\star_{\mathcal{M}} (0, \mathsf{0})\big\}$$

We give the following example of a 2-counters 3-instructions Minsky machine informally described by the following pseudo-code:

```
1: if c[2]=0 then goto 0 else c[2]:=c[2]-1 ; goto 2
2: if c[1]=0 then goto 3 else c[1]:=c[1]-1 ; goto 1
3: c[1]:=c[1]+1 ; goto 3
```

$$\psi_0(1) = (-, 2, 0, 2)$$
$$\psi_0(2) = (-, 1, 3, 1)$$
$$\psi_0(3) = (+, 1, 3)$$

with formal definition corresponding to $\mathcal{M}_0 = (2, 3, \psi_0)$. With this definition, the reader can check that $\mathcal{A}(\mathcal{M}_0) = \{(c, c) \mid c \in \mathbb{N}\}$.

5.2 The encoding of Minsky machines in eBBI

In the following discussion, we consider a fixed Minsky machine $\mathcal{M} = (n, l, \psi)$. We denote $\Sigma_{\mathcal{M}}$ (resp. $\to_{\mathcal{M}}$) simply by Σ (resp. $\to$). We describe how we encode instructions and simulate computations. The instructions of $\mathcal{M}$ will be represented by $(\mathrel{-\!\!*}, \wedge)$-elementary formulae in the fragment eBBI. For this, we need the following set of propositional variables:

$$\{\mathtt{c}_1, \ldots, \mathtt{c}_n\} \cup \{\mathtt{r}_1, \ldots, \mathtt{r}_n\} \cup \{\mathtt{k}\} \cup \{\mathtt{q}_0, \ldots, \mathtt{q}_l\} \cup \{\mathtt{q}^1_0, \ldots, \mathtt{q}^1_l\} \cup \cdots \cup \{\mathtt{q}^n_0, \ldots, \mathtt{q}^n_l\}$$

composed of $(n+1)(l+3) - 1$ (distinct) logical variables.

Let Σ_0 be the following multiset composed of $n(n+1)+2$ many $(\mathrel{-\!\!*}, \wedge)$-elementary formulae:

$$\Sigma_0 = \left[\begin{array}{c} \big\{\mathtt{c}_p \mathrel{-\!\!*} (\mathtt{k} \mathrel{-\!\!*} \mathtt{k}) \mid p \in [1, n]\big\} \quad \cup \big\{\mathtt{c}_p \mathrel{-\!\!*} (\mathtt{r}_q \mathrel{-\!\!*} \mathtt{r}_q) \mid p \neq q \in [1, n]\big\} \\ \cup \big\{(\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{c}_1) \mathrel{-\!\!*} \mathtt{r}_q \mid q \in [1, n]\big\} \cup \big\{(\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{c}_1) \mathrel{-\!\!*} \mathtt{k}, (\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{c}_1) \mathrel{-\!\!*} \mathtt{q}_0\big\} \end{array}\right]$$

For $i \in [1, l]$, from the value of $\psi(i)$, we define the multiset Σ_i composed of two $(\mathrel{-\!\!*}, \wedge)$-elementary formulae by:

$$\Sigma_i = \{(\mathtt{c}_p \mathrel{-\!\!*} \mathtt{q}_j) \mathrel{-\!\!*} \mathtt{q}^p_j, (\mathtt{k} \wedge \mathtt{q}^p_j) \mathrel{-\!\!*} \mathtt{q}_i\} \quad \text{when } \psi(i) = (+, p, j)$$

$$\text{or} \quad \Sigma_i = \{(\mathtt{r}_p \wedge \mathtt{q}_j) \mathrel{-\!\!*} \mathtt{q}_i, \mathtt{c}_p \mathrel{-\!\!*} (\mathtt{q}_k \mathrel{-\!\!*} \mathtt{q}_i)\} \quad \text{when } \psi(i) = (-, p, j, k)$$

Collecting $\Sigma_0, \ldots, \Sigma_l$, we obtain a multiset composed of $n(n+1)+2(l+1)$ formulae. The Minsky machine instructions of $\mathcal{M} = (n, l, \psi)$ are thus encoded as the multiset $\Sigma_{\mathcal{M}} = \Sigma_0, \Sigma_1, \ldots, \Sigma_l$ of $(\mathrel{-\!\!*}, \wedge)$-elementary formulae.

Given a vector $\mathsf{m} \in \mathbb{N}^n$, we define $\mathsf{c}^\mathsf{m} = m_1.\mathsf{c}_1, \ldots, m_n.\mathsf{c}_n$ as the multiset composed of m_i occurrences of the variable c_i for each $i \in [1, n]$, i.e. the encoding of the vector m as a multiset of $\{\mathsf{c}_1, \ldots, \mathsf{c}_n\}$. As an example, when $\mathsf{m} = (2, 1, 3) \in \mathbb{N}^3$, we have $\mathsf{c}^\mathsf{m} = \mathsf{c}_1, \mathsf{c}_1, \mathsf{c}_2, \mathsf{c}_3, \mathsf{c}_3, \mathsf{c}_3$. Then, it is trivial to verify that for any vector $\mathsf{m} \in \mathbb{N}^n$ and any $i \in [0, l]$, the sequent $\Sigma^\mathsf{l}_\mathcal{M}, \mathsf{c}^\mathsf{m} \vdash \mathsf{q}_i$ belongs to the fragment eBBI.

The following result states that acceptance by $\mathcal{M}$ is simulated by validity in eBBI, whichever sub-class of models of BBI/CBI is chosen.

Theorem 5.1 *For any $X \in \{\mathrm{ND}, \mathrm{D}, \mathrm{T}, \mathrm{G}\}$,*

$$\mathcal{A}(\mathcal{M}) = \{\mathsf{m} \in \mathbb{N}^n \mid \Sigma^\mathsf{l}_\mathcal{M}, \mathsf{c}^\mathsf{m} \vdash \mathsf{q}_1 \textit{ is universally valid in } \mathsf{BBI}_X\} \quad \textit{(resp. } \mathsf{CBI}_X\textit{)}$$

We detail the proof in Sections 5.3 and 5.4. But before we prove this characterization, let us come back to our previous example of the two counters Minsky machine $\mathcal{M}_0 = (2, 3, \psi_0)$. With the previous description, the encoding of the instructions of $\mathcal{M}_0$ will be given by the following multiset $\Sigma_{(2,3,\psi_0)}$:

$$\left\{\begin{array}{l} \mathtt{c}_1 \mathrel{-\!\!*} (\mathtt{r}_2 \mathrel{-\!\!*} \mathtt{r}_2), \mathtt{c}_2 \mathrel{-\!\!*} (\mathtt{r}_1 \mathrel{-\!\!*} \mathtt{r}_1), \\ \mathtt{c}_1 \mathrel{-\!\!*} (\mathtt{k} \mathrel{-\!\!*} \mathtt{k}), \mathtt{c}_2 \mathrel{-\!\!*} (\mathtt{k} \mathrel{-\!\!*} \mathtt{k}), \\ (\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{c}_1) \mathrel{-\!\!*} \mathtt{r}_1, (\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{c}_1) \mathrel{-\!\!*} \mathtt{r}_2, \\ (\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{c}_1) \mathrel{-\!\!*} \mathtt{k}, (\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{c}_1) \mathrel{-\!\!*} \mathtt{q}_0 \end{array}\right\} \cup \left\{\begin{array}{l} (\mathtt{r}_2 \wedge \mathtt{q}_0) \mathrel{-\!\!*} \mathtt{q}_1, \mathtt{c}_2 \mathrel{-\!\!*} (\mathtt{q}_2 \mathrel{-\!\!*} \mathtt{q}_1), \\ (\mathtt{r}_1 \wedge \mathtt{q}_3) \mathrel{-\!\!*} \mathtt{q}_2, \mathtt{c}_1 \mathrel{-\!\!*} (\mathtt{q}_1 \mathrel{-\!\!*} \mathtt{q}_2), \\ (\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{q}_3) \mathrel{-\!\!*} \mathtt{q}_3^1, (\mathtt{k} \wedge \mathtt{q}_3^1) \mathrel{-\!\!*} \mathtt{q}_3 \end{array}\right\}$$

5.3 Soundness of the encoding

Proposition 5.2 *For any $\mathsf{m} \in \mathbb{N}^n$ and $p \in [1, n]$, if $m_p = 0$ then the sequent $\Sigma^\mathsf{l}, \mathsf{c}^\mathsf{m} \vdash \mathtt{r}_p$ has a proof in* gBBI.

Proof. Let us fix $p \in [1, n]$. Supposing $m_p = 0$, we build of gBBI proof tree of the sequent $\Sigma^\mathsf{l}, \mathsf{c}^\mathsf{m} \vdash \mathtt{r}_p$ by induction on the size $s = m_1 + \ldots + m_n$ of m.

If $s = 0$ then $m_1 = \cdots = m_n = 0$ and c^m is the empty multiset. Here is a gBBI proof tree:

$$\dfrac{\dfrac{}{\Sigma^\mathsf{l}, \mathtt{c}_1 \vdash \mathtt{c}_1}\langle\mathrm{Ax}\rangle}{\Sigma^\mathsf{l} \vdash \mathtt{r}_p}\,(\mathtt{c}_1 \mathrel{-\!\!*} \mathtt{c}_1) \mathrel{-\!\!*} \mathtt{r}_p \in \Sigma_0 \subseteq \Sigma$$

If $s > 0$, let us choose q such that $m_q > 0$. Then $p \neq q$ holds (because $m_p = 0$ is an hypothesis). Let m' be the unique vector such that $\mathsf{m}' + \mathsf{e}_q = \mathsf{m}$. We derive the identity $\mathsf{c}^\mathsf{m} = \mathsf{c}^{\mathsf{m}'}, \mathsf{c}_q$ between multisets. The size s' of m' is $s' = s - 1$ and we obviously have $m'_p = m_p = 0$. So we can apply the induction hypothesis to m' and obtain a proof tree Q for $\Sigma^\mathsf{l}, \mathsf{c}^{\mathsf{m}'} \vdash \mathtt{r}_p$. From it, we build a proof tree suitable for

$\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathtt{r}_p$:

$$\dfrac{\dfrac{}{\Sigma^{\mathsf{l}}, \mathsf{c}_q \vdash \mathsf{c}_q}\langle \mathrm{Ax} \rangle \qquad \dfrac{Q}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}'} \vdash \mathtt{r}_p}}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}'}, \mathsf{c}_q \vdash \mathtt{r}_p}\ \mathsf{c}_q \mathrel{-\!\!*} (\mathtt{r}_p \mathrel{-\!\!*} \mathtt{r}_p) \in \Sigma_0 \subseteq \Sigma$$

Hence the sequent $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathtt{r}_p$ has a proof in gBBI. □

Proposition 5.3 *For any* $\mathsf{m} \in \mathbb{N}^n$*, the sequent* $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathtt{k}$ *has a proof in* gBBI*.*

Proof. Same argument as Proposition 5.2 but using side conditions $(\mathsf{c}_1 \mathrel{-\!\!*} \mathsf{c}_1) \mathrel{-\!\!*} \mathtt{k} \in \Sigma_0$ and $\mathsf{c}_q \mathrel{-\!\!*} (\mathtt{k} \mathrel{-\!\!*} \mathtt{k}) \in \Sigma_0$ instead of $\mathsf{c}_q \mathrel{-\!\!*} (\mathtt{r}_p \mathrel{-\!\!*} \mathtt{r}_p) \in \Sigma_0$. □

Lemma 5.4 *For any* $r \in \mathbb{N}$*,* $i \in [0, l]$ *and* $\mathsf{m} \in \mathbb{N}^n$*, if* $(i, \mathsf{m}) \to^r (0, 0)$ *then the sequent* $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i$ *has a proof in* gBBI*.*

Proof. We build a gBBI proof tree for the sequent $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i$ by induction on r. If $r = 0$ then we have $(i, \mathsf{m}) = (0, 0)$. As c^0 is the empty multiset, the sequent $\Sigma^{\mathsf{l}}, \mathsf{c}^0 \vdash \mathsf{q}_0$ has the following proof tree:

$$\dfrac{\dfrac{}{\Sigma^{\mathsf{l}}, \mathsf{c}_1 \vdash \mathsf{c}_1}\langle \mathrm{Ax} \rangle}{\Sigma^{\mathsf{l}} \vdash \mathsf{q}_0}\ (\mathsf{c}_1 \mathrel{-\!\!*} \mathsf{c}_1) \mathrel{-\!\!*} \mathsf{q}_0 \in \Sigma_0 \subseteq \Sigma$$

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

If $\psi(i) = (+, p, i')$ and $\mathsf{m}' = \mathsf{m} + \mathsf{e}_p$. Hence the identity $\mathsf{c}^{\mathsf{m}'} = \mathsf{c}^{\mathsf{m}}, \mathsf{c}_p$ holds. Let Q be a proof tree for $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathtt{k}$ according to Proposition 5.3. We provide the following proof tree for $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{Q}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathtt{k}} \qquad \dfrac{\dfrac{P}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}}, \mathsf{c}_p \vdash \mathsf{q}_{i'}}}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}^p_{i'}}\ (\mathsf{c}_p \mathrel{-\!\!*} \mathsf{q}_{i'}) \mathrel{-\!\!*} \mathsf{q}^p_{i'} \in \Sigma_i}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i}\ (\mathtt{k} \wedge \mathsf{q}^p_{i'}) \mathrel{-\!\!*} \mathsf{q}_i \in \Sigma_i$$

If $\psi(i) = (-, p, i', k)$, $m_p = 0$ and $\mathsf{m}' = \mathsf{m}$. Let Q be a proof tree for $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathtt{r}_p$ according to Proposition 5.2. We provide the following proof tree for $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{Q}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathtt{r}_p} \qquad \dfrac{P}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_{i'}}}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i}\ (\mathtt{r}_p \wedge \mathsf{q}_{i'}) \mathrel{-\!\!*} \mathsf{q}_i \in \Sigma_i$$

If $\psi(i) = (-, p, j, i')$, $\mathsf{m}' + \mathsf{e}_p = \mathsf{m}$ (and $m_p \neq 0$). Then the identity $\mathsf{c}^{\mathsf{m}'}, \mathsf{c}_p = \mathsf{c}^{\mathsf{m}}$

holds. We provide the following proof tree for $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}'}, \mathsf{c}_p \vdash \mathsf{q}_i$:

$$\dfrac{\dfrac{}{\Sigma^{\mathsf{l}}, \mathsf{c}_p \vdash \mathsf{c}_p}\,\langle\mathrm{Ax}\rangle \qquad \dfrac{P}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}'} \vdash \mathsf{q}_{i'}}}{\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}'}, \mathsf{c}_p \vdash \mathsf{q}_i}\ \mathsf{c}_p \mathrel{-\!\!*} (\mathsf{q}_{i'} \mathrel{-\!\!*} \mathsf{q}_i) \in \Sigma_i$$

In any case we obtain a gBBI proof tree for $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i$ which fulfills the requirements of the induction step. □

Thus for any $X \in \{\mathrm{ND}, \mathrm{D}, \mathrm{T}, \mathrm{G}\}$, if the relation $(1, \mathsf{m}) \to^\star (0, 0)$ holds, then by Lemma 5.4 we obtain a proof of $\Sigma^{\mathsf{l}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_1$ in gBBI and by Theorem 4.4, this sequent is (universally) valid in BBI_X (resp. CBI_X).

5.4 *Faithfulness of the encoding*

We use a particular Kripke semantics interpretation in the free abelian group $(\mathbb{Z}^n, +, 0, -)$. This is the crucial point: provide a model which is suitable for both BBI and CBI. Considering $\mathbb{N}^n \subseteq \mathbb{Z}^n$ as the strict subset of $\mathbb{Z}^n$ whose vectors have positive components, we define $x \circ y = \{x + y\}$ and $(\mathbb{Z}^n, \circ, \mathsf{0}, -, \mathsf{0})$ is thus a non-deterministic groupoid of the class G.

We provide the following Kripke interpretation for the variables that might occur in Σ. For $p \in [1, n]$ and $i \in [0, l]$, we define:

$$\delta(\mathsf{c}_p) = \{\mathsf{e}_p\} \qquad \delta(\mathtt{r}_p) = \{\mathsf{m} \in \mathbb{N}^n \mid m_p = 0\} \qquad \delta(\mathtt{k}) = \mathbb{N}^n$$

$$\delta(\mathsf{q}_i) = \{\mathsf{m} \in \mathbb{N}^n \mid (i, \mathsf{m}) \to^\star (0, 0)\} \qquad \delta(\mathsf{q}_i^p) = \{\mathsf{m} \in \mathbb{Z}^n \mid \mathsf{m} + \mathsf{e}_p \in \delta(\mathsf{q}_i)\}$$

Let us now consider the Kripke semantics of the compound formulae of Σ.

Proposition 5.5 *For any $\sigma \in \Sigma$, $\mathsf{0} \Vdash \sigma$ holds.*

Proof. First let us prove that $\mathsf{m} \Vdash \mathsf{c}_1 \mathrel{-\!\!*} \mathsf{c}_1$ iff $\mathsf{m} = \mathsf{0}$. Indeed, $\mathsf{m} \Vdash \mathsf{c}_1 \mathrel{-\!\!*} \mathsf{c}_1$ iff $\mathsf{m} \circ \delta(\mathsf{c}_1) \subseteq \delta(\mathsf{c}_1)$ iff $\mathsf{m} \circ \{\mathsf{e}_1\} \subseteq \{\mathsf{e}_1\}$ iff $\{\mathsf{m} + \mathsf{e}_1\} \subseteq \{\mathsf{e}_1\}$ iff $\mathsf{m} = \mathsf{0}$.

Then $\mathsf{m} \Vdash (\mathsf{c}_1 \mathrel{-\!\!*} \mathsf{c}_1) \mathrel{-\!\!*} x$ iff $\mathsf{m} \circ \{\mathsf{0}\} \subseteq \delta(x)$ iff $\mathsf{m} \in \delta(x)$. As $\mathsf{0}$ belongs to $\delta(\mathtt{r}_q)$, $\delta(\mathtt{k})$ and $\delta(\mathsf{q}_0)$, for any variable $x \in \{\mathtt{r}_q \mid q \in [1, n]\} \cup \{\mathtt{k}, \mathsf{q}_0\}$, we have $\mathsf{0} \Vdash (\mathsf{c}_1 \mathrel{-\!\!*} \mathsf{c}_1) \mathrel{-\!\!*} x$.

Let us choose $p \neq q \in [1, n]$ and let us prove that $\mathsf{0} \Vdash \mathsf{c}_p \mathrel{-\!\!*} (\mathtt{r}_q \mathrel{-\!\!*} \mathtt{r}_q)$. We derive the following logical equivalences: $\mathsf{m} \Vdash \mathsf{c}_p \mathrel{-\!\!*} (\mathtt{r}_q \mathrel{-\!\!*} \mathtt{r}_q)$ iff $\mathsf{m} \circ \delta(\mathsf{c}_p) \circ \delta(\mathtt{r}_q) \subseteq \delta(\mathtt{r}_q)$ iff $\mathsf{m} \circ \{\mathsf{e}_p\} \circ \{\mathsf{m}' \in \mathbb{N}^n \mid m'_q = 0\} \subseteq \{\mathsf{m}' \in \mathbb{N}^n \mid m'_q = 0\}$ iff $\{\mathsf{m} + \mathsf{e}_p + \mathsf{m}' \mid \mathsf{m}' \in \mathbb{N}^n \text{ and } m'_q = 0\} \subseteq \{\mathsf{m}' \in \mathbb{N}^n \mid m'_q = 0\}$. But for any $\mathsf{m}' \in \mathbb{N}^n$ s.t. $m'_q = 0$, we have $(\mathsf{m} + \mathsf{e}_p + \mathsf{m}')_q = m_q + 0 + 0 = m_q$. Now $(\mathsf{0} + \mathsf{e}_p + \mathsf{m}')_q = 0$, so $\mathsf{0} \Vdash \mathsf{c}_p \mathrel{-\!\!*} (\mathtt{r}_q \mathrel{-\!\!*} \mathtt{r}_q)$.

Let us choose $p \in [1, n]$ and let us prove that $\mathsf{0} \Vdash \mathsf{c}_p \mathrel{-\!\!*} (\mathtt{k} \mathrel{-\!\!*} \mathtt{k})$. We compute: $\mathsf{m} \Vdash \mathsf{c}_p \mathrel{-\!\!*} (\mathtt{k} \mathrel{-\!\!*} \mathtt{k})$ iff $\mathsf{m} \circ \{\mathsf{e}_p\} \circ \mathbb{N}^n \subseteq \mathbb{N}^n$ iff $\{\mathsf{m} + \mathsf{e}_p + \mathsf{m}' \mid \mathsf{m}' \in \mathbb{N}^n\} \subseteq \mathbb{N}^n$ iff $\mathsf{m} + \mathsf{e}_p \in \mathbb{N}^n$. Thus, as $\mathsf{0} + \mathsf{e}_p = \mathsf{e}_p \in \mathbb{N}^n$ holds, we obtain $\mathsf{0} \Vdash \mathsf{c}_p \mathrel{-\!\!*} (\mathtt{k} \mathrel{-\!\!*} \mathtt{k})$.

Let us consider the formulae in Σ_i for $i \in [1, l]$. Let us prove that the relation $\mathsf{0} \in [\![\sigma]\!]$ holds for any $\sigma \in \Sigma_i$.

If $\psi(i) = (+, p, j)$. Let us prove $\mathsf{0} \Vdash (\mathsf{c}_p \mathrel{-\!\!*} \mathsf{q}_j) \mathrel{-\!\!*} \mathsf{q}_j^p$, i.e. $\mathsf{m} \Vdash \mathsf{c}_p \mathrel{-\!\!*} \mathsf{q}_j$ implies $\mathsf{m} \Vdash \mathsf{q}_j^p$ for any $\mathsf{m} \in \mathbb{Z}^n$. Let us suppose $\mathsf{m} \Vdash \mathsf{c}_p \mathrel{-\!\!*} \mathsf{q}_j$. Then $\{\mathsf{m} + \mathsf{e}_p\} = \mathsf{m} \circ \delta(\mathsf{c}_p) \subseteq \delta(\mathsf{q}_j)$ and thus $\mathsf{m} + \mathsf{e}_p \in \delta(\mathsf{q}_j)$. By definition of $\delta(\mathsf{q}_j^p)$, we obtain $\mathsf{m} \in \delta(\mathsf{q}_j^p)$ and thus $m \Vdash \mathsf{q}_j^p$.

Then let us prove $\mathsf{0} \Vdash (\mathtt{k} \wedge \mathsf{q}_j^p) \mathrel{-\!\!*} \mathsf{q}_i$, i.e. $\mathsf{m} \Vdash \mathtt{k}$ and $\mathsf{m} \Vdash \mathsf{q}_j^p$ implies $\mathsf{m} \Vdash \mathsf{q}_i$ for any $\mathsf{m} \in \mathbb{Z}^n$. Let us pick $\mathsf{m} \in \mathbb{Z}^n$ and let us suppose $\mathsf{m} \Vdash \mathtt{k}$ and $\mathsf{m} \Vdash \mathsf{q}_j^p$. From $\mathsf{m} \Vdash \mathtt{k}$, we derive $\mathsf{m} \in \delta(\mathtt{k})$ and hence $\mathsf{m} \in \mathbb{N}^n$. From $\mathsf{m} \Vdash \mathsf{q}_j^p$, we derive $\mathsf{m} + \mathsf{e}_p \in \delta(\mathsf{q}_j)$. Let $\mathsf{m}' = \mathsf{m} + \mathsf{e}_p$. From $\mathsf{m}' \in \delta(\mathsf{q}_j)$, we get $(j, \mathsf{m}') \rightarrow^\star (0, \mathsf{0})$. As $\mathsf{m} \in \mathbb{N}^n$ and $\psi(i) = (+, p, j)$, we have $(i, \mathsf{m}) \rightarrow (j, \mathsf{m}')$. Thus $(i, \mathsf{m}) \rightarrow (j, \mathsf{m}') \rightarrow^\star (0, \mathsf{0})$ and we conclude $\mathsf{m} \Vdash \mathsf{q}_i$.

If $\psi(i) = (-, p, j, k)$. Let us first prove that $\mathsf{0} \Vdash (\mathtt{r}_p \wedge \mathsf{q}_j) \mathrel{-\!\!*} \mathsf{q}_i$, i.e. $\delta(\mathtt{r}_p) \cap \delta(\mathsf{q}_j) \subseteq \delta(\mathsf{q}_i)$. Let us pick $\mathsf{m} \in \delta(\mathtt{r}_p) \cap \delta(\mathsf{q}_j)$. Then $\mathsf{m} \in \delta(\mathtt{r}_p)$ and thus $m_p = 0$ and $\mathsf{m} \in \mathbb{N}^n$. As $\psi(i) = (-, p, j, k)$, we obtain $(i, \mathsf{m}) \rightarrow (j, \mathsf{m})$. From $\mathsf{m} \in \delta(\mathsf{q}_j)$, we obtain $(j, \mathsf{m}) \rightarrow^\star (0, \mathsf{0})$. Thus $(i, \mathsf{m}) \rightarrow (j, \mathsf{m}) \rightarrow^\star (0, \mathsf{0})$ and we conclude $\mathsf{m} \in \delta(\mathsf{q}_i)$.

Let us finally prove that $\mathsf{0} \Vdash \mathsf{c}_p \mathrel{-\!\!*} (\mathsf{q}_k \mathrel{-\!\!*} \mathsf{q}_i)$, i.e. $\delta(\mathsf{c}_p) \circ \delta(\mathsf{q}_k) \subseteq \delta(\mathsf{q}_i)$. As $\delta(\mathsf{c}_p) = \{\mathsf{e}_p\}$, let us choose $\mathsf{m}' \in \delta(\mathsf{q}_k)$ and define $\mathsf{m} = \mathsf{m}' + \mathsf{e}_p$. From $\mathsf{m}' \in \delta(\mathsf{q}_k)$, we derive $\mathsf{m}' \in \mathbb{N}^n$ and $(k, \mathsf{m}') \rightarrow^\star (0, \mathsf{0})$. Then $\mathsf{m} \in \mathbb{N}^n$ and $m_p = m'_p + 1 \neq 0$. As $\psi(i) = (-, p, j, k)$, we get $(i, \mathsf{m}) \rightarrow (k, \mathsf{m}')$. We derive $(i, \mathsf{m}) \rightarrow (k, \mathsf{m}') \rightarrow^\star (0, \mathsf{0})$ and obtain $\mathsf{m} \in \delta(\mathsf{q}_i)$. Thus $\mathsf{m}' + \mathsf{e}_p \in \delta(\mathsf{q}_i)$. Hence, for any $\mathsf{m}' \in \delta(\mathsf{q}_k)$ we get $\delta(\mathsf{c}_p) \circ \mathsf{m}' \subseteq \delta(\mathsf{q}_i)$. Thus $\delta(\mathsf{c}_p) \circ \delta(\mathsf{q}_k) \subseteq \delta(\mathsf{q}_i)$. □

In the following lemma and subsequent discussion, we use the common denotation $((\mathbb{Z}^n, \ldots), \delta)$ to represent either the BBI-model $((\mathbb{Z}^n, \circ, \mathsf{0}), \delta)$ or the CBI-model $((\mathbb{Z}^n, \circ, \mathsf{0}, -, \mathsf{0}), \delta)$. In fact, the non-deterministic monoidal structure is sufficient to interpret the sequents of the fragment eBBI.

Lemma 5.6 *For any $\mathsf{m} \in \mathbb{N}^n$ and any $i \in [0, l]$, if the sequent $\Sigma^{\mathsf{I}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i$ is valid in the model $((\mathbb{Z}^n, \ldots), \delta)$ then the relation $(i, \mathsf{m}) \rightarrow^\star (0, \mathsf{0})$ holds.*

Proof. Let $\Sigma^{\mathsf{I}} = \{\varphi_1, \ldots, \varphi_r\}$. Let $\varphi \in \Sigma^{\mathsf{I}}$. There exists $\sigma \in \Sigma$ s.t. $\varphi = \mathsf{I} \wedge \sigma$. Then $\mathsf{0} \Vdash \sigma$ by Proposition 5.5 and thus we get $\mathsf{0} \Vdash \mathsf{I} \wedge \sigma$. Hence, for any $\varphi \in \Sigma^{\mathsf{I}}$, we have $\mathsf{0} \Vdash \varphi$. As $\mathsf{e}_p \Vdash \mathsf{c}_p$ for any $p \in [1, n]$, $\mathsf{0} \Vdash \sigma$ for any $\sigma \in \Sigma^{\mathsf{I}}$ and

$$\mathsf{m} = m_1\mathsf{e}_1 + \cdots + m_n\mathsf{e}_n \in \mathsf{0} \circ \cdots \circ \mathsf{0} \circ \mathsf{e}_1 \circ \cdots \circ \mathsf{e}_1 \circ \cdots \circ \mathsf{e}_n \circ \cdots \circ \mathsf{e}_n$$

(where $\mathsf{0}$ occurs r times and e_p occurs m_p times for each $p \in [1, n]$), from the validity of $\Sigma^{\mathsf{I}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_i$ in the interpretation $((\mathbb{Z}^n, \ldots), \delta)$, we obtain $\mathsf{m} \Vdash \mathsf{q}_i$. Thus $\mathsf{m} \in \delta(\mathsf{q}_i)$ and by definition of $\delta(\mathsf{q}_i)$, $(i, \mathsf{m}) \rightarrow^\star (0, \mathsf{0})$ holds. □

As the relational monoid $(\mathbb{Z}^n, \circ, \mathsf{0})$ (resp. groupoid $(\mathbb{Z}^n, \circ, \mathsf{0}, -, \mathsf{0})$) belongs to all the sub-classes of non-deterministic monoids (resp. groupoids) considered in this paper, for any $X \in \{\mathrm{ND}, \mathrm{D}, \mathrm{T}, \mathrm{G}\}$, if the sequent $\Sigma^{\mathsf{I}}, \mathsf{c}^{\mathsf{m}} \vdash \mathsf{q}_1$ is universally valid in BBI_X (resp. CBI_X), then it is valid in the model $((\mathbb{Z}^n, \ldots), \delta)$, and by Lemma 5.6, the relation $m \in \mathcal{A}(\mathcal{M})$ must hold.

Corollary 5.7 BBI *and* CBI *restricted to their Kripke interpretation on pairs of integers in $\mathbb{Z} \times \mathbb{Z}$ are both undecidable.*

Proof. Choose a two counter Minsky machine for which acceptance is not recursive [15]. □

6 Perspectives and Acknowledgments

From this direct simulation of Minsky machines, we obtain a proof of the undecidability of BBI/CBI based on a very simple semantic structure, the free commutative group $\mathbb{Z} \times \mathbb{Z}$. Our undecidability proof would not work for the group $\mathbb{Z}$. Indeed, one counter Minsky machines are a special case of pushdown automata[5] for which the acceptance/reachability problems are known to be decidable [1]. An interesting development would be to study the decidability of BBI/CBI restricted to $\mathbb{Z}$ (or only $\mathbb{N}$ for BBI).

I wish to thank the anonymous referees for their helpful reviews. Thanks to some observations, Theorem 3.2 has been strengthened. As to one of the remarks, I would not say that the undecidability of the BBI/CBI logics presented in this paper is *purely a consequence* of the undecidability of the calculus gBBI on the fragment eBBI: we do not know (yet) whether gBBI is complete for all the classes of models considered (i.e. Tg and G).

References

[1] Bouajjani, A., J. Esparza and O. Maler, *Reachability Analysis of Pushdown Automata: Application to Model-Checking*, in: A. W. Mazurkiewicz and J. Winkowski, editors, *CONCUR*, Lecture Notes in Computer Science **1243** (1997), pp. 135–150.

[2] Brotherston, J., *A cut free proof theory for Boolean BI*, Technical Report DTR09-13, Imperial College London (2009), available at `http://www.doc.ic.ac.uk/~jbrother`.

[3] Brotherston, J. and C. Calcagno, *Classical BI: a logic for reasoning about dualising resources*, in: Z. Shao and B. C. Pierce, editors, *POPL* (2009), pp. 328–339.

[4] Brotherston, J. and C. Calcagno, *Classical BI: Its Semantics and Proof Theory*, Logical Methods in Computer Science (2010), to appear, available at `http://www.doc.ic.ac.uk/~jbrother`.

[5] Brotherston, J. and M. Kanovich, *Undecidability of propositional separation logic and its neighbours*, in: *LICS* (2010), also available as technical report `http://www.doc.ic.ac.uk/research/technicalreports/2010/DTR10-1.pdf`.

[6] de Groote, P., B. Guillaume and S. Salvati, *Vector addition tree automata*, in: *LICS'04* (2004), pp. 64–73.

[7] Galmiche, D. and D. Larchey-Wendling, *Expressivity properties of Boolean BI through relational models*, in: S. Arun-Kumar and N. Garg, editors, *FSTTCS*, LNCS **4337** (2006), pp. 357–368.

[8] Galmiche, D., D. Méry and D. Pym, *The semantics of BI and resource tableaux*, Mathematical Structures in Computer Science **15** (2005), pp. 1033–1088.

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

[10] Girard, J.-Y., *Linear logic*, Theoretical Computer Science **50** (1987), pp. 1–102.

[11] Ishtiaq, S. and P. O'Hearn, *BI as an Assertion Language for Mutable Data Structures*, in: *POPL*, 2001, pp. 14–26.

[5] with just one stack symbol and a non-removable bottom symbol for the empty stack.

[12] Kanovich, M., *The direct simulation of Minsky machines in linear logic*, in: J.-Y. Girard, Y. Lafont and L. Regnier, editors, *Advances in Linear Logic*, London Mathematical Society Lecture Note Series **222**, Cambridge University Press, 1995 pp. 123–145.

[13] Larchey-Wendling, D. and D. Galmiche, *Exploring the relation between Intuitionistic BI and Boolean BI: an unexpected embedding*, Math. Struct. in Comp. Science **19** (2009), pp. 435–500.

[14] Larchey-Wendling, D. and D. Galmiche, *The Undecidability of Boolean BI through Phase Semantics*, in: *LICS* (2010), full version available at `http://www.loria.fr/~larchey`.

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

[16] O'Hearn, P. and D. Pym, *The logic of bunched implications*, Bulletin of Symbolic Logic **5** (1999), pp. 215–244.

[17] Pym, D., "The Semantics and Proof Theory of the Logic of Bunched Implications," Applied Logic Series **26**, Kluwer Academic Publishers, 2002, errata available at `http://www.cs.bath.ac.uk/~pym/BI.html`.

[18] Troelstra, A., "Lectures on Linear Logic," Lecture Notes **29**, Center for the Study of Language and Information, Stanford, California, 1992.

A The soundness of sequent rules

Proposition 4.3 *The rules of Figure 1 preserve validity in the model $(\mathcal{M}, \delta)$.*

Proof. The case of rules $\langle \text{id} \rangle$ and $\langle \wedge_R \rangle$ are trivial. For the other rules, let us write $\Gamma = \Gamma_1, \ldots, \Gamma_p$ (resp. $\Delta = \Delta_1, \ldots, \Delta_k$) where the Γ_i's (resp. Δ_i's) are the BBI/CBI formulae composing the multiset Γ (resp. Δ).

For rule $\langle \text{w} \rangle$, we suppose $(\mathcal{M}, \delta) \Vdash \Gamma_1, \ldots, \Gamma_p \vdash B$ and we prove $(\mathcal{M}, \delta) \Vdash \Gamma_1, \ldots, \Gamma_p, \mathsf{I} \wedge A \vdash B$. For this, let us pick $m, m_1, \ldots, m_p, a \in \mathcal{M}$ such that $m \in m_1 \circ \ldots \circ m_p \circ a$, $m_1 \Vdash \Gamma_1, \ldots, m_p \Vdash \Gamma_p$ and $a \Vdash \mathsf{I} \wedge A$. Let us prove $m \Vdash B$. From $a \Vdash \mathsf{I} \wedge A$, we deduce $a \Vdash \mathsf{I}$ and thus $a = \epsilon$. Hence, $m \in m_1 \circ \ldots \circ m_p \circ \epsilon$ and thus $m \in m_1 \circ \ldots \circ m_p$. We also have $m_1 \Vdash \Gamma_1, \ldots, m_p \Vdash \Gamma_p$, so, by validity of the sequent $\Gamma_1, \ldots, \Gamma_p \vdash B$ in $(\mathcal{M}, \delta)$, we deduce $m \Vdash B$.

For rule $\langle \text{c} \rangle$, we suppose $(\mathcal{M}, \delta) \Vdash \Gamma_1, \ldots, \Gamma_p, \mathsf{I} \wedge A, \mathsf{I} \wedge A \vdash B$ and we prove $(\mathcal{M}, \delta) \Vdash \Gamma_1, \ldots, \Gamma_p, \mathsf{I} \wedge A \vdash B$. For this, let us pick $m, m_1, \ldots, m_p, a \in \mathcal{M}$ such that $m \in m_1 \circ \ldots \circ m_p \circ a$, $m_1 \Vdash \Gamma_1, \ldots, m_p \Vdash \Gamma_p$ and $a \Vdash \mathsf{I} \wedge A$. Let us prove $m \Vdash B$. From $a \Vdash \mathsf{I} \wedge A$, we deduce $a \Vdash \mathsf{I}$ and thus $a = \epsilon$. Hence $\{a\} = a \circ a$ and thus $m \in m_1 \circ \ldots \circ m_p \circ a \circ a$. We also have $m_1 \Vdash \Gamma_1, \ldots, m_p \Vdash \Gamma_p$, so, by validity of the sequent $\Gamma_1, \ldots, \Gamma_p, \mathsf{I} \wedge A, \mathsf{I} \wedge A \vdash B$ in $(\mathcal{M}, \delta)$, we deduce $m \Vdash B$.

For rule $\langle \mathsf{I}_L \rangle$, we suppose $(\mathcal{M}, \delta) \Vdash \Gamma_1, \ldots, \Gamma_p, A \vdash B$ and we prove $(\mathcal{M}, \delta) \Vdash \Gamma_1, \ldots, \Gamma_p, \mathsf{I} \wedge A \vdash B$. For this, let us pick $m, m_1, \ldots, m_p, a \in \mathcal{M}$ such that $m \in m_1 \circ \ldots \circ m_p \circ a$, $m_1 \Vdash \Gamma_1, \ldots, m_p \Vdash \Gamma_p$ and $a \Vdash \mathsf{I} \wedge A$. Let us prove $m \Vdash B$. From $a \Vdash \mathsf{I} \wedge A$, we deduce $a \Vdash A$. We also have $m_1 \Vdash \Gamma_1, \ldots, m_p \Vdash \Gamma_p$, so, by validity of the sequent $\Gamma_1, \ldots, \Gamma_p, A \vdash B$ in $(\mathcal{M}, \delta)$, we deduce $m \Vdash B$.

For rule $\langle -\!\!* _L \rangle$, we suppose that $\Gamma_1, \ldots, \Gamma_p \vdash A$ and $\Delta_1, \ldots, \Delta_k, B \vdash C$ are valid in $(\mathcal{M}, \delta)$ and we prove that the sequent $\Gamma_1, \ldots, \Gamma_p, \Delta_1, \ldots, \Delta_k, A -\!\!* B \vdash C$ is valid in $(\mathcal{M}, \delta)$. For this, let us pick $m \in m_1 \circ \ldots \circ m_p \circ m'_1 \circ \cdots m'_k \circ \alpha$ such that $m_1 \Vdash \Gamma_1, \ldots, m_p \Vdash \Gamma_p, m'_1 \Vdash \Delta_1, \ldots, m_k \Vdash \Delta_k$ and $\alpha \Vdash A -\!\!* B$. Let us prove $m \Vdash C$. From $m \in (m_1 \circ \ldots \circ m_p) \circ (m'_1 \circ \cdots m'_k \circ \alpha)$, we obtain $a \in m_1 \circ \ldots \circ m_p$ such that $m \in a \circ m'_1 \circ \cdots m'_k \circ \alpha$ (see Proposition 2.3). From $m \in m'_1 \circ \cdots m'_k \circ (a \circ \alpha)$, we obtain $b \in a \circ \alpha$ such that $m \in m'_1 \circ \cdots m'_k \circ b$. By validity of the sequent

$\Gamma_1, \ldots, \Gamma_p \vdash A$, we deduce $a \Vdash A$. Since, $\alpha \Vdash A \mathrel{-\!\!*} B$, $a \Vdash A$ and $b \in \alpha \circ a$, we deduce $b \Vdash B$. Then, by validity of the sequent $\Delta_1, \ldots, \Delta_k, B \vdash C$ in $(\mathcal{M}, \delta)$, we deduce $m \Vdash C$.

For rule $\langle \mathrel{-\!\!*}_R \rangle$, we suppose that $(\mathcal{M}, \delta) \Vdash \Gamma_1, \ldots, \Gamma_p, A \vdash B$ and we prove $(\mathcal{M}, \delta) \Vdash \Gamma_1, \ldots, \Gamma_p \vdash A \mathrel{-\!\!*} B$. For this, let us pick $m, m_1, \ldots, m_p \in \mathcal{M}$ such that $m \in m_1 \circ \ldots \circ m_p$ and $m_1 \Vdash \Gamma_1, \ldots, m_p \Vdash \Gamma_p$. Let us prove $m \Vdash A \mathrel{-\!\!*} B$. Thus, let a, b be such that $b \in m \circ a$ and $a \Vdash A$ and let us prove $b \Vdash B$. From $b \in m \circ a$ and $m \in m_1 \circ \ldots \circ m_p$, we deduce $b \in m_1 \circ \ldots \circ m_p \circ a$. By validity of the sequent $\Gamma_1, \ldots, \Gamma_p, A \vdash B$ in $(\mathcal{M}, \delta)$, we obtain $b \Vdash B$. □