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 $\mathbb{Z}$

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

1 Introduction

The logic of bunched implications of Pym and O’Hearn [15] 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 [2,7,12]. 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 [5,13]. Using different techniques, both Larchey-Wendling & Galmiche [13] 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 of [13] 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 [15] is a sub-structural logic which freely combines additive connectives $\land, \lor, \to$ and multiplicative connectives $\ast, \multimap$. 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 [16]. 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 [9] (see [12] 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 dualising 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 (dualising) 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 (dualising) 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 [12] 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 [13] 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 [5,13] 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 sub-classes 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. 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 \( m \in \mathbb{N}^n \) of the machine, we associate 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
\( \circ : M \times M \rightarrow \mathcal{P}(M) \) is naturally extended to a binary operator on \( \mathcal{P}(M) \) by

\[
X \circ Y = \bigcup \{x \circ y \mid x \in X, y \in Y\}
\]

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 \( \circ : M \times M \rightarrow \mathcal{P}(M) \). We require the following conditions to hold:

(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)\(^1\)

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 \(( M, \bullet, e) \) is a (usual) commutative monoid then, defining \( a \circ b = \{ a \bullet b \} \) and \( e = e \) 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 \( \circ : M \times M \rightarrow \mathcal{P}(M) \) can equivalently be understood as a ternary relation \(-\circ- \ni - \) \( : M \times M \times M \rightarrow \{0, 1\} \) through the Curry-Howard isomorphism and the axioms correspond to those of an internal monoid in the category of relations. 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 \( m \in x \circ Y \).

\(^1\) Associativity should be understood using the extension (1) of \( \circ \) to \( \mathcal{P}(M) \).
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 $\text{NDm}$ (resp. $\text{Dm}$, resp. $\text{Tm}$). The class of total deterministic groups is denoted $\text{G}$.

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

**Proof.** The inclusion between those classes of non-deterministic monoids is obvious. We illustrate $\text{NDm} \not\subseteq \text{Dm}$ by the following structure: $((\{\epsilon, x, y\}, \circ, \epsilon)$ where $x \circ x = \{\epsilon, y\}$ and $y \circ \alpha = \{y\}$ for any $\alpha \in \{\epsilon, x, y\}$. □

**Definition 2.6** A non-deterministic groupoid is a tuple $(M, \circ, \epsilon, -, \infty)$ where $(M, \circ, \epsilon)$ is a non-deterministic monoid and $- : M \rightarrow M$ 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 $\mathcal{P}(M) \rightarrow \mathcal{P}(M)$ by $-X = \{-x \mid x \in X\}$. The identities $-\epsilon = \infty$ and $-\epsilon = \infty$ 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 $\text{NDg}$ (resp. $\text{Dg}$, resp. $\text{Tg}$). The class of total deterministic groups is denoted $\text{G}$.

There is no contradiction in the definition of total deterministic groups 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 $\text{G} \subsetneq \text{Tg} \subsetneq \text{Dg} \subsetneq \text{NDg}$ hold.
Proof. See [3,4] for a justification of the strictness of the inclusions. For instance, the bit-arithmetic model is a witness for \( \operatorname{Tg} \not\subseteq \operatorname{G} \). \(\square\)

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 \( \text{Var} \), they are freely build using the logical variables in \( \text{Var} \), the logical constants in \( \{O, I, \top, \bot\} \), the unary connectives in \( \{\sim, \neg\} \) or the binary connectives in \( \{*, -*, \land\} \). 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:

\[
\begin{align*}
\text{BBI} : & \quad A := v | I | \top | \bot | \neg A | A * A | A -* A | A \land A \\
\text{CBI} : & \quad A := v | O | I | \top | \bot | \sim A | \neg A | A * A | A -* A | A \land A
\end{align*}
\]

with \( v \in \text{Var} \). Hence, BBI appears as a fragment of CBI.\(^2\) If \( \delta : \text{Var} \to \mathcal{P}(M) \) is an interpretation of variables where \( M = (\mathcal{M}, \circ, \epsilon) \) 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 BBI/CBI from a given model \((\mathcal{M}, \delta)\) of BBI/CBI, by induction on the structure of formulae:

\[
\begin{align*}
m \models v & \iff m \in \delta(v) \\
m \models \bot & \iff \text{never} \\
m \models \top & \iff \text{always} \\
m \models \neg A & \iff m \not\models A \\
m \models A \land B & \iff m \models A \land m \models B \\
m \models A * B & \iff \exists a, b, m \in a \circ b \land a \models A \land b \models B \\
m \models A -* B & \iff \forall a, b, m \in m \circ a \land a \models A \Rightarrow b \models B
\end{align*}
\]

A formula \( F \) is valid in the model \((\mathcal{M}, \circ, \ldots), \delta)\) if \( m \models F \) holds for any \( m \in M \). A formulae \( F \) is valid in a structure \( \mathcal{M} = (\mathcal{M}, \circ, \ldots) \) if for any interpretation \( \delta : \text{Var} \to \mathcal{P}(M) \) 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

\(^2\) We did not include the two other additive connectives \( \lor \) and \( \rightarrow \) or the other multiplicative connective \( * \lor \) which we consider definable in BBI/CBI by the De Morgan equations \( A \lor B = \neg (\neg A \land \neg B) \), \( A \rightarrow B = \neg (A \land \neg B) \) and \( A * \lor B = \neg (\sim A * \sim B) \).
by a non-deterministic monoid (resp. groupoid) \((M, \circ, \ldots)\), an interpretation \(\delta : \text{Var} \rightarrow \mathcal{P}(M)\) and an element \(m \in M\) such that \(m \not\models F\).

**Definition 3.1** We denote by \(\text{BBI}_{\text{ND}}\) (resp. \(\text{BBI}_D\), \(\text{BBI}_T\), \(\text{BBI}_G\), \(\text{CBI}_{\text{ND}}\), \(\text{CBI}_D\), \(\text{CBI}_T\), \(\text{CBI}_G\)) the set of formulae of \(\text{BBI}\) (resp. \(\text{CBI}\)) which are valid in every structure belonging to the class \(\text{NDm}\) (resp. \(\text{Dm}, \text{Tm}, \text{G}\), \(\text{NDg}, \text{Dg}, \text{Tg}, \text{G}\)).

**Theorem 3.2** The two following inclusions sequences hold:

\[(i) \quad \text{BBI}_{\text{ND}} \subset \text{BBI}_D \subset \text{BBI}_T \subset \text{BBI}_G \quad (ii) \quad \text{CBI}_{\text{ND}} \subset \text{CBI}_D \subset \text{CBI}_T \subset \text{CBI}_G\]

See appendix of [11] for a justification of these strict inclusion relations.

We do not discuss the relations between the different sub-classes of \(\text{BBI}/\text{CBI}\) models further. See [3,5,12,13] for a more detailed presentation.

### 4 Sequents for \(\text{BBI}/\text{CBI}\)

Contrary to (intuitionistic) \(\text{BI}\) or linear logic, bunched logics with classical additives like \(\text{BBI}\) and \(\text{CBI}\) 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 \(\text{BBI}/\text{CBI}\) [2,3]. Nevertheless, we present a set of sound sequent calculi rules with are suitable for many bunched logics with classical additives, because they preserve validity in a particular model.

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

**Definition 4.1** A **sequent** is a pair denoted \(\Gamma \vdash B\) where \(\Gamma\) 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 \((M, \delta)\) and we write \((M, \delta) \models A_1, \ldots, A_p \vdash B\) if

\[
\forall m, m_1, \ldots, m_p \in M, (m \in m_1 \circ \ldots \circ m_p \text{ and } \forall i, m_i \models A_i) \implies m \models B \quad (2)
\]

When \(\Gamma \vdash B\) is valid in the model \((M, \delta)\), we also say that \((M, \delta)\) 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 \((M, \delta)\) if and only if the formula \((A_1 \ast \cdots \ast A_p) \rightarrow B\) is valid in \((M, \delta)\).
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 rules of Figure 1.

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

The proof of this result is standard (see [11]). 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 $\Sigma^l$ for 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. $\langle \text{Ax} \rangle$, $\langle \text{Ax} \rangle$, $\langle \text{Ax} \rangle$, and $\langle \text{Ax} \rangle$.

**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 $(\mathcal{M}, \delta)$.

The rules of $gBBI$ can be obtained as combinations of the sequent rules of Figure 1, and thus are strongly sound for BBI/CBI (see [11]). Neither the set of rules of Figure 1 nor the set of rules of Figure 2 constitute a complete proof-system for either BBI$_{ND}$ or CBI$_{ND}$. But $gBBI$ is sufficient to be able to simulate Minsky machines computations and it is the simplest system we could design for such a goal.

---

3 These sequent rules can be viewed as a subset of the rules of intuitionistic linear logic where the exponential $!A$ is replaced by $1 \wedge A$. 

4.2 The elementary fragment of BBI

We define a fragment called elementary BBI which is common to BBI and CBI. eBBI will be used to encode Minsky machines and corresponds to an extension of the fragment s-IMELL\(^\circ\) of multiplicative exponential linear logic [6,13].

**Definition 4.5** A formula of BBI/CBI is \((-\star, \land)-elementary\) if it is of the form 
\((u \rightarrow v) \rightarrow w, u \rightarrow (v \rightarrow w)\) or \((u \land v) \rightarrow w\) where \(u, v\) and \(w\) are logical variables. The sequents of the fragment eBBI are those of the form \(\Sigma, \Gamma \vdash c\) where \(\Gamma\) is a multiset of variables, \(c\) is a variable and \(\Sigma\) is a multiset of \((-\star, \land)-elementary\) 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.

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 [13], 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. The question of completeness of fragments w.r.t. subclasses of models may be difficult to solve, as illustrated by the examples of the incompleteness of BBI [13] and CBI [4] w.r.t. partial monoidal Kripke semantics.

5 Encoding Minsky machines in BBI/CBI

We propose an encoding of Minsky machines [14] in BBI/CBI. As in [13], the encoding differs from Kanovich’s encoding of Minsky machines in the (!, \(\oplus\))-Horn fragment of intuitionistic linear logic [10]. Compared to the encoding proposed in [13], 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 \((\mathbb{Z}^n, +, 0)\).
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 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 \( m = (m_1, \ldots, m_n) \). Given the values of counters \( m \in \mathbb{N}^n \) 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 \( e_p = (0, \ldots, 0, 1, 0, \ldots, 0) \) the vector of \( \mathbb{N}^n \) with all components to 0 except the \( p \)-th which as value 1. Hence, \((e_1, \ldots, e_n)\) is the canonical base of \( \mathbb{N}^n \) and we have the canonical decomposition: \( m = m_1 e_1 + \cdots + m_n e_n \). We denote by \( 0 \) the vector \((0, \ldots, 0)\) where all components are null.

A \( n \)-counter Minsky machine with \( l \) instructions is given by a total function \( \psi : [1, l] \rightarrow \{+\} \times [1, n] \times [0, l] \sqcup \{-\} \times [1, n] \times [0, l] \times [0, l] \) where, \( \sqcup \) represents disjoint set union. Minsky machines instructions (incrementation, zero test/decrementation) are encoded as illustrated in the two following examples:

\[
\begin{align*}
\psi(1) &= (+, 2, 3) \leadsto 1: \ c[2]:=c[2]+1; \ \text{goto 3} \\
\psi(2) &= (-, 6, 4, 5) \leadsto 2: \text{if c[6]=0 then goto 4 else c[6]:=c[6]-1; goto 5}
\end{align*}
\]

where \( c[] \) contains the array of counters of the Minsky machine.

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

\[
\psi(i) = (+, p, i') \text{ and } m' = m + e_p
\]

or \( \psi(i) = (-, p, i', k), m_p = 0 \text{ and } m' = m \)

or \( \psi(i) = (-, p, j, i'), m'_p + e_p = m \text{ (and } m_p \neq 0) \)

Remark that \((i, m) \rightarrow_M (i', m') \) does not hold if \( i = 0 \) because \( \psi(0) \) is not defined. Let \( \rightarrow_M^* \) be the reflexive and transitive closure of the relation \( \rightarrow_M \).

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

\[
\mathcal{A}(M) = \{ m \in \mathbb{N}^n \mid (1, m) \rightarrow^*_M (0, 0) \}
\]

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  
\[\psi_0(1) = (-, 2, 0, 2)\]

2: if \(c[1]=0\) then goto 3 else \(c[1]:=c[1]-1\) ; goto 1  
\[\psi_0(2) = (-, 1, 3, 1)\]

3: \(c[1]:=c[1]+1\) ; goto 3  
\[\psi_0(3) = (+, 1, 3)\]

with formal definition corresponding to \(M_0 = (2, 3, \psi_0)\). With this definition, the reader can check that \(\mathcal{A}(M_0) = \{(c, c) \mid c \in \mathbb{N}\}\).

### 5.2 The encoding of Minsky machines in eBBI

In the following discussion, we consider a fixed Minsky machine \(M = (n, l, \psi)\). We denote \(\Sigma_M\) (resp. \(\rightarrow_M\)) simply by \(\Sigma\) (resp. \(\rightarrow\)). We describe how we encode instructions and simulate computations. The instructions of \(M\) will be represented by \((-\ast, \wedge)\)-elementary formulae in the fragment eBBI. For this, we need the following set of propositional variables:

\[
\{c_1, \ldots, c_n\} \cup \{r_1, \ldots, r_n\} \cup \{k\} \cup \{q_0, \ldots, q_i\} \cup \{q_0^1, \ldots, q_i^1\} \cup \cdots \cup \{q_0^n, \ldots, q_i^n\}
\]

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

Let \(\Sigma_0\) be the following multiset composed of \(n(n+1) + 2\) many \((-\ast, \wedge)\)-elementary formulae:

\[
\Sigma_0 = \left[ \begin{array}{c}
\{c_p \rightarrow (k \rightarrow k) \mid p \in [1, n]\} \\
\cup \{c_p \rightarrow (r_q \rightarrow r_q) \mid p \neq q \in [1, n]\} \\
\cup \{(c_1 \rightarrow c_1) \rightarrow r_q \mid q \in [1, n]\} \\
\cup \{(c_1 \rightarrow c_1) \rightarrow k, (c_1 \rightarrow c_1) \rightarrow q_0\}
\end{array} \right]
\]

For \(i \in [1, l]\), from the value of \(\psi(i)\), we define the multiset \(\Sigma_i\) composed of two \((-\ast, \wedge)\)-elementary formulae by:

\[
\Sigma_i = \begin{cases} \{c_p \rightarrow q_j \rightarrow q_j^p, (k \land q_j^p) \rightarrow q_i\} & \text{when } \psi(i) = (+, p, j) \\ \{c_p \rightarrow q_j \rightarrow q_i, c_p \rightarrow (q_k \rightarrow q_i)\} & \text{when } \psi(i) = (-, p, j, k) \end{cases}
\]

Collecting \(\Sigma_0, \ldots, \Sigma_l\), we obtain a multiset composed of \(n(n+1) + 2(l+1)\) formulae. The Minsky machine instructions of \(M = (n, l, \psi)\) are thus encoded as the multiset \(\Sigma_M = \Sigma_0, \Sigma_1, \ldots, \Sigma_l\) of \((-\ast, \wedge)\)-elementary formulae.

Given a vector \(m \in \mathbb{N}^n\), we define \(c^m = c_1, c_2, \ldots, c_n\) 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 \( \{c_1, \ldots, c_n\} \). As an example, when \( m = (2, 1, 3) \in \mathbb{N}^3 \), we have \( c^m = c_1, c_2, c_3, c_3, c_3 \). Then, it is trivial to verify that for any vector \( m \in \mathbb{N}^n \) and any \( i \in [0, l] \), the sequent \( \Sigma M, c^m \vdash q_i \) belongs to the fragment eBBI.

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

**Theorem 5.1** For any \( x \in \{ND, D, T, G\} \),

\[
\mathcal{A}(M) = \{m \in \mathbb{N}^n \mid \Sigma^I M, c^m \vdash q_1 \text{ is universally valid in BBI}_x\} \quad (\text{resp. CBI}_x)
\]

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 \( M_0 = (2, 3, \psi_0) \). With the previous description, the encoding of the instructions of \( M_0 \) will be given by the following multiset \( \Sigma_{(2,3,\psi_0)} \):

\[
\begin{align*}
    \{ & c_1 \rightarrow (r_2 \rightarrow r_2), \ c_2 \rightarrow (r_1 \rightarrow r_1), \ c_1 \rightarrow (k \rightarrow k), \ c_2 \rightarrow (k \rightarrow k), \\
    & (c_1 \rightarrow c_1) \rightarrow r_1, \ (c_1 \rightarrow c_1) \rightarrow r_2, \ (c_1 \rightarrow c_1) \rightarrow k, \ (c_1 \rightarrow c_1) \rightarrow q_0 \} \cup \\
    \{ & (r_2 \rightarrow q_0) \rightarrow q_1, \ c_2 \rightarrow (q_2 \rightarrow q_1), \\
    & (r_1 \rightarrow q_3) \rightarrow q_2, \ c_1 \rightarrow (q_1 \rightarrow q_2), \\
    & (c_1 \rightarrow q_3) \rightarrow q_3, \ (k \rightarrow q_3) \rightarrow q_3 \}
\end{align*}
\]

### 5.3 Soundness of the encoding

**Proposition 5.2** For any \( m \in \mathbb{N}^n \) and \( p \in [1, n] \), if \( m_p = 0 \) then the sequent \( \Sigma^I, c^m \vdash r_p \) has a proof in gBBI.

**Proposition 5.3** For any \( m \in \mathbb{N}^n \), the sequent \( \Sigma^I, c^m \vdash k \) has a proof in gBBI.

**Proof.** Both proofs are similar to that in [13] and can be found in [11].

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

**Proof.** We build a gBBI proof tree for the sequent \( \Sigma^I, c^m \vdash q_i \) by induction on \( r \). If \( r = 0 \) then we have \((i, m) = (0, 0)\). As \( c^0 \) is the empty multiset, the sequent \( \Sigma^I, c^0 \vdash q_0 \) has the following proof tree:

\[
\frac{\Sigma^I, c^0 \vdash c_1 \quad \langle \text{Ax} \rangle}{\Sigma^I \vdash q_0}
\]

(c_1 \rightarrow c_1) \rightarrow q_0 \in \Sigma_0 \subseteq \Sigma

Let us now consider a transition sequence \((i, m) \rightarrow (i', m') \rightarrow^r (0, 0)\) of length \( r + 1 \). By the evident induction hypothesis, let \( P \) be a proof tree for the sequent \( \Sigma^I, c^{m'} \vdash q_{i'} \). We consider the three cases for \((i, m) \rightarrow (i', m')\).
If $\psi(i) = (+, p, i')$ and $m' = m + e_p$. Hence the identity $c^{m'} = c^m, c_p$ holds. Let $Q$ be a proof tree for $\Sigma^l, c^m \vdash k$ according to Proposition 5.3. We provide the following proof tree for $\Sigma^l, c^m \vdash q_i$:

$\Sigma^l, c^m \vdash k$

\[
\frac{Q}{\Sigma^l, c^m, c_p \vdash q_{i'}} (c_p \dashv q_{i'}) \dashv q_{i'} \in \Sigma_i
\]

\[
\frac{Q}{\Sigma^l, c^m \vdash q_i} (k \land q_{i'}) \dashv q_i \in \Sigma_i
\]

If $\psi(i) = (-, p, i', k)$, $m_p = 0$ and $m' = m$. Let $Q$ be a proof tree for $\Sigma^l, c^m \vdash r_p$ according to Proposition 5.2. We provide the following proof tree for $\Sigma^l, c^m \vdash q_i$:

$\Sigma^l, c^m \vdash r_p$

\[
\frac{Q}{\Sigma^l, c^m \vdash q_{i'}} (r_p \land q_{i'}) \dashv q_i \in \Sigma_i
\]

If $\psi(i) = (-, p, j, i')$, $m' + e_p = m$ (and $m_p \neq 0$). Then the identity $c^{m'}, c_p = c^m$ holds. We provide the following proof tree for $\Sigma^l, c^{m'}, c_p \vdash q_i$:

$\Sigma^l, c_p \vdash c_p$

\[
\frac{P}{\Sigma^l, c^{m'} \vdash q_{i'}} (q_{i'} \dashv q_i) \in \Sigma_i
\]

In any case we obtain a $g\mathbb{B}\mathbb{I}$ proof tree for $\Sigma^l, c^m \vdash q_i$ which fulfills the requirements of the induction step. \qed

Thus for any $x \in \{\text{ND}, D, T, G\}$, if the relation $(1, m) \rightarrow^* (0, 0)$ holds, then by Lemma 5.4 we obtain a proof of $\Sigma^l, c^m \vdash q_1$ in $g\mathbb{B}\mathbb{I}$ and by Theorem 4.4, this sequent is (universally) valid in $\mathbb{B}\mathbb{I}_x$ (resp. $\mathbb{C}\mathbb{I}_x$).

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 $\mathbb{B}\mathbb{I}$ and $\mathbb{C}\mathbb{I}$. 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 $(\mathbb{Z}^n, \circ, 0, -, 0)$ is thus a non-deterministic groupoid of the class G.

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

$$\delta(c_p) = \{e_p\} \quad \delta(r_p) = \{m \in \mathbb{N}^n \mid m_p = 0\} \quad \delta(k) = \mathbb{N}^n$$

$$\delta(q_j) = \{m \in \mathbb{N}^n \mid (i, m) \to^* (0, 0)\} \quad \delta(q^p_j) = \{m \in \mathbb{Z}^n \mid m + e_p \in \delta(q_j)\}$$

Let us now consider the Kripke semantics of the compound formulae of $\Sigma$.

**Proposition 5.5** For any $\sigma \in \Sigma$, $0 \models \sigma$ holds.

**Proof.** First let us prove that $m \models c_1 \to c_1$ iff $m = 0$. Indeed, $m \models c_1 \to c_1$ iff $m \circ \delta(c_1) \subseteq \delta(c_1)$ iff $m \circ \{e_1\} \subseteq \{e_1\}$ iff $\{m + e_1\} \subseteq \{e_1\}$ iff $m = 0$.

Then $m \models (c_1 \to c_1) \to x$ iff $m \circ \{0\} \subseteq \delta(x)$ iff $m \in \delta(x)$. As $0$ belongs to $\delta(r_q)$, $\delta(k)$ and $\delta(q_0)$, for any variable $x \in \{r_q \mid q \in [1, n]\} \cup \{k, q_0\}$, we have $0 \models (c_1 \to c_1) \to x$.

Let us choose $p \neq q \in [1, n]$ and let us prove that $0 \models c_p \to (r_q \to r_q)$. We derive the following logical equivalences: $m \models c_p \to (r_q \to r_q)$ iff $m \circ \delta(c_p) \circ \delta(r_q) \subseteq \delta(r_q)$ iff $m \circ \{e_p\} \circ \{m' \in \mathbb{N}^n \mid m'_q = 0\} \subseteq \{m' \in \mathbb{N}^n \mid m'_q = 0\}$ iff $\{m + e_p + m' \mid m' \in \mathbb{N}^n \text{ and } m'_q = 0\} \subseteq \{m' \in \mathbb{N}^n \mid m'_q = 0\}$. But for any $m' \in \mathbb{N}^n$ s.t. $m'_q = 0$, we have $(m + e_p + m')_q = m_q + 0 + 0 = m_q$. Now $(0 + e_p + m')_q = 0$, so $0 \models c_p \to (r_q \to r_q)$.

Let us choose $p \in [1, n]$ and let us prove that $0 \models c_p \to (k \to k)$. We compute: $m \models c_p \to (k \to k)$ iff $m \circ \{e_p\} \circ \mathbb{N}^n \subseteq \mathbb{N}^n$ iff $\{m + e_p + m' \mid m' \in \mathbb{N}^n\} \subseteq \mathbb{N}^n$ iff $m + e_p \in \mathbb{N}^n$. Thus, as $0 + e_p = e_p \in \mathbb{N}^n$ holds, we obtain $0 \models c_p \to (k \to k)$.

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

If $\psi(i) = (+, p, j)$. Let us prove $0 \models (c_p \to q_j) \to q^p_j$, i.e. $m \models c_p \to q_j$ implies $m \models q^p_j$ for any $m \in \mathbb{Z}^n$. Let us suppose $m \models c_p \to q_j$. Then $\{m + e_p\} = m \circ \delta(c_p) \subseteq \delta(q_j)$ and thus $m + e_p \in \delta(q_j)$. By definition of $\delta(q^p_j)$, we obtain $m \in \delta(q^p_j)$ and thus $m \models q^p_j$.

Then let us prove $0 \models (k \wedge q^p_j) \to q_j$, i.e. $m \models k$ and $m \models q^p_j$ implies $m \models q_j$ for any $m \in \mathbb{Z}^n$. Let us pick $m \in \mathbb{Z}^n$ and let us suppose $m \models k$ and $m \models q^p_j$. From $m \models k$, we derive $m \in \delta(k)$ and hence $m \in \mathbb{N}^n$. From $m \models q^p_j$, we derive $m + e_p \in \delta(q_j)$. Let $m' = m + e_p$. From $m' \in \delta(q_j)$, we get $(j, m') \to^* (0, 0)$. As $m \in \mathbb{N}^n$ and $\psi(i) = (+, p, j)$, we have $(i, m) \to (j, m')$. Thus $(i, m) \to (j, m') \to^* (0, 0)$ and we conclude $m \models q_j$.

If $\psi(i) = (-, p, j, k)$. Let us first prove that $0 \models (r_p \wedge q_j) \to q_i$, i.e. $\delta(r_p) \cap \delta(q_j) \subseteq \delta(q_i)$. Let us pick $m \in \delta(r_p) \cap \delta(q_j)$. Then $m \in \delta(r_p)$ and thus $m_p = 0$ and $m \in \mathbb{N}^n$. As $\psi(i) = (-, p, j, k)$, we obtain $(i, m) \to (j, m)$. From $m \in \delta(q_j)$, we obtain $(j, m) \to^* (0, 0)$. Thus $(i, m) \to (j, m) \to^* (0, 0)$ and we conclude $m \models q_i$.

Let us finally prove that $0 \models c_p \to (q_k \to q_i)$, i.e. $\delta(c_p) \circ \delta(q_k) \subseteq \delta(q_i)$.
As \( \delta(c_p) = \{e_p\} \), let us choose \( m' \in \delta(q_k) \) and define \( m = m' + e_p \). From \( m' \in \delta(q_k) \), we derive \( m' \in \mathbb{N}^n \) and \((k, m') \rightarrow^* (0,0)\). Then \( m \in \mathbb{N}^n \) and \( m_p = m'_p + 1 \neq 0 \). As \( \psi(i) = (-p, p, j, k) \), we get \((i, m) \rightarrow (k, m')\). We derive \((i, m) \rightarrow (k, m') \rightarrow^* (0,0) \) and obtain \( m \in \delta(q_i) \). Thus \( m' + e_p \in \delta(q_i) \). Hence, for any \( m' \in \delta(q_k) \) we get \( \delta(c_p) \circ m' \subseteq \delta(q_i) \). Thus \( \delta(c_p) \circ \delta(q_k) \subseteq \delta(q_i) \). \( \square \)

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

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

**Proof.** Let \( \Sigma^l = \{\varphi_1, \ldots, \varphi_r\} \). Let \( \varphi \in \Sigma^l \). There exists \( \sigma \in \Sigma \) s.t. \( \varphi = 1 \wedge \sigma \). Then \( 0 \models \sigma \) by Proposition 5.5 and thus we get \( 0 \models 1 \wedge \sigma \). Hence, for any \( \varphi \in \Sigma^l \), we have \( 0 \not\models \varphi \). As \( e_p \models c_p \) for any \( p \in [1, n] \), \( 0 \models \sigma \) for any \( \sigma \in \Sigma^l \) and

\[
m = m_1 e_1 + \cdots + m_n e_n \in 0 \cdots 0 e_1 \cdots e_1 \cdots e_n \cdots e_n
\]

(where \( 0 \) occurs \( r \) times and \( e_p \) occurs \( m_p \) times for each \( p \in [1, n] \)), from the validity of \( \Sigma^l, c^m \vdash q_i \) in the interpretation \((([Z^n,\ldots,\delta]), \delta)\), we obtain \( m \models q_i \). Thus \( m \in \delta(q_i) \) and by definition of \( \delta(q_i) \), \((i, m) \rightarrow^* (0,0)\) holds. \( \square \)

As the relational monoid \((Z^n, \circ, 0)\) (resp. groupoid \((Z^n, \circ, 0, -0)\)) belongs to all the sub-classes of non-deterministic monoids (resp. groupoids) considered in this paper, for any \( x \in \{ND, D, T, G\} \), if the sequent \( \Sigma^l, c^m \vdash q_i \) is universally valid in \textsc{BBI}_x (resp. \textsc{CBI}_x), then it is valid in the model \((([Z^n,\ldots,\delta]), \delta)\), and by Lemma 5.6, the relation \( m \in \mathcal{A}(M) \) must hold.

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

**Proof.** Choose a two counter Minsky machine for which acceptance is not recursive [14]. \( \square \)

6 Perspectives and Acknowledgments

From this direct simulation of Minsky machines, we obtain a proof of the undecidability of \textsc{BBI}/\textsc{CBI} based on a very simple semantic structure, the free commutative group \( Z \times Z \). Our undecidability proof would not work for the group \( Z \). Indeed, one counter Minsky machines are a special case of pushdown automata\(^4\) for which the acceptance/reachability problems are known to be

\(^4\) with just one stack symbol and a non-removable bottom symbol for the empty stack.
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 and its proof can be found in the appendix of [11]. 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


A Different classes of models for BBI/CBI

Theorem 3.2 The two following inclusions sequences hold:

(i) \( \text{BBI}_{ND} \subsetneq \text{BBI}_D \subsetneq \text{BBI}_T \subsetneq \text{BBI}_G \)

(ii) \( \text{CBI}_{ND} \subsetneq \text{CBI}_D \subsetneq \text{CBI}_T \subsetneq \text{CBI}_G \)

Proof. Let us consider a BBI/CBI-model \( \mathcal{M} = (M,\circ,\epsilon,...) \). In the following table, we consider some formulae and their respective Kripke interpretation in the model \( \mathcal{M} \):

<table>
<thead>
<tr>
<th>Name</th>
<th>Formula ( F )</th>
<th>( m \vdash F )</th>
<th>BBI</th>
<th>CBI</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{I} )</td>
<td>( \neg (\top \rightarrow \neg I) )</td>
<td>( \epsilon \in m \circ M )</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>( \mathcal{O} )</td>
<td>( \neg (\neg O \rightarrow \neg I) )</td>
<td>( \epsilon \in m \circ \infty )</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>( \mathcal{O}' )</td>
<td>( \neg (\neg O \rightarrow \neg O) \rightarrow \neg O )</td>
<td>( m \in \infty \circ \infty \Rightarrow m = \infty )</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>( \Box A )</td>
<td>( \top \ast (1 \land (\top \rightarrow A)) )</td>
<td>( \forall x \in M, x \vdash A )</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

For \( \text{BBI}_D \not\subset \text{BBI}_{ND} \) (resp. \( \text{BBI}_T \not\subset \text{BBI}_D \)), the witness formula \( (\mathcal{I} \ast \mathcal{I}) \rightarrow \mathcal{I} \) (resp. \( \mathcal{T} \)) was given in [13]. The formula \( \mathcal{I} \) encodes invertibility in BBI/CBI, thus \( \mathcal{I} \) belongs to \( \text{BBI}_G \) but not to \( \text{BBI}_T \). Hence \( \text{BBI}_G \not\subset \text{BBI}_T \).

For \( \text{CBI}_D \not\subset \text{CBI}_{ND} \), 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 \( \text{CBI}_G \not\subset \text{CBI}_T \).

Let us provide a witness for \( \text{CBI}_T \not\subset \text{CBI}_D \). The formula \( \mathcal{O}' \) is valid in a structure of the class \( T_g \) 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 \( \Box \mathcal{O}' \rightarrow \mathcal{O} \) belongs to \( \text{CBI}_T \).

Let us show that \( \Box \mathcal{O}' \rightarrow \mathcal{O} \) does not belong to \( \text{CBI}_D \). Consider the partial deterministic groupoid \( \mathcal{M} = (\{\epsilon,\ x,\ y,\ \infty\}, \circ, \epsilon, -, \) \) defined by the following tables:

<table>
<thead>
<tr>
<th>( \circ )</th>
<th>( \epsilon )</th>
<th>( x )</th>
<th>( y )</th>
<th>( \infty )</th>
<th>( - )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \epsilon )</td>
<td>{\epsilon}</td>
<td>{x}</td>
<td>{y}</td>
<td>{\infty}</td>
<td>\epsilon</td>
</tr>
<tr>
<td>( x )</td>
<td>{x}</td>
<td>\emptyset</td>
<td>{\infty}</td>
<td>\emptyset</td>
<td>x</td>
</tr>
<tr>
<td>( y )</td>
<td>{y}</td>
<td>{\infty}</td>
<td>\emptyset</td>
<td>\emptyset</td>
<td>y</td>
</tr>
<tr>
<td>( \infty )</td>
<td>{\infty}</td>
<td>\emptyset</td>
<td>\emptyset</td>
<td>\emptyset</td>
<td>\infty</td>
</tr>
</tbody>
</table>
There is no need to provide $\delta$ 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, $\mathcal{M} \in \text{Dg}$ holds. The formula $\Omega'$ is valid in this structure because $\square \circ \square = \emptyset$. Hence, $\square \Omega'$ is valid in $\mathcal{M}$. Obviously $\square \neq \epsilon$ holds in $\mathcal{M}$ and thus $\mathcal{M}$ is a counter-model to the formula $\square \Omega' \rightarrow \Omega$. Moreover, $\mathcal{M}$ belongs to the class $\text{Dg}$.

\[\square \]

B The soundness of sequent rules

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

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

For rule $\langle w \rangle$, we suppose $(\mathcal{M}, \delta) \models \Gamma_1, \ldots, \Gamma_p, 1 \land A \models B$ and we prove $(\mathcal{M}, \delta) \models \Gamma_1, \ldots, \Gamma_p, 1 \land A \models B$. For this, let us pick $m, m_1, \ldots, m_p, a \in \mathcal{M}$ such that $m \in m_1 \circ \ldots \circ m_p \circ a$, $m_1 \models \Gamma_1, \ldots, m_p \models \Gamma_p$ and $a \models 1 \land A$. Let us prove $m \models B$. From $a \models 1 \land A$, we deduce $a \models 1$ 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 $m_1 \models \Gamma_1, \ldots, m_p \models \Gamma_p$, so, by validity of the sequent $\Gamma_1, \ldots, \Gamma_p \models B$ in $\langle \mathcal{M}, \delta \rangle$, we deduce $m \models B$.

For rule $\langle c \rangle$, we suppose $(\mathcal{M}, \delta) \models \Gamma_1, \ldots, \Gamma_p, 1 \land A, 1 \land A \models B$ and we prove $(\mathcal{M}, \delta) \models \Gamma_1, \ldots, \Gamma_p, 1 \land A \models B$. For this, let us pick $m, m_1, \ldots, m_p, a \in \mathcal{M}$ such that $m \in m_1 \circ \ldots \circ m_p \circ a$, $m_1 \models \Gamma_1, \ldots, m_p \models \Gamma_p$ and $a \models 1 \land A$. Let us prove $m \models B$. From $a \models 1 \land A$, we deduce $a \models 1$ 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 $m_1 \models \Gamma_1, \ldots, m_p \models \Gamma_p$, so, by validity of the sequent $\Gamma_1, \ldots, \Gamma_p, 1 \land A, 1 \land A \models B$ in $\langle \mathcal{M}, \delta \rangle$, we deduce $m \models B$.

For rule $\langle l \rangle$, we suppose $(\mathcal{M}, \delta) \models \Gamma_1, \ldots, \Gamma_p, A \models B$ and we prove $(\mathcal{M}, \delta) \models \Gamma_1, \ldots, \Gamma_p, 1 \land A \models B$. For this, let us pick $m, m_1, \ldots, m_p, a \in \mathcal{M}$ such that $m \in m_1 \circ \ldots \circ m_p \circ a$, $m_1 \models \Gamma_1, \ldots, m_p \models \Gamma_p$ and $a \models 1 \land A$. Let us prove $m \models B$. From $a \models 1 \land A$, we deduce $a \models A$. We also have $m_1 \models \Gamma_1, \ldots, m_p \models \Gamma_p$, so, by validity of the sequent $\Gamma_1, \ldots, \Gamma_p, A \models B$ in $\langle \mathcal{M}, \delta \rangle$, we deduce $m \models B$.

For rule $\langle \rightarrow_L \rangle$, we suppose that $\Gamma_1, \ldots, \Gamma_p \models A$ and $\Delta_1, \ldots, \Delta_k, B \models C$ are valid in $\langle \mathcal{M}, \delta \rangle$ and we prove that the sequent $\Gamma_1, \ldots, \Gamma_p, \Delta_1, \ldots, \Delta_k, A \rightarrow B \models C$ is valid in $\langle \mathcal{M}, \delta \rangle$. For this, let us pick $m \in m_1 \circ \ldots \circ m_p \circ m'_1 \circ \ldots \circ m'_k \circ a$ such that $m_1 \models \Gamma_1, \ldots, m_p \models \Gamma_p, m'_1 \models \Delta_1, \ldots, m'_k \models \Delta_k$ and $a \models A \rightarrow B$. Let us prove $m \models C$. From $m \in (m_1 \circ \ldots \circ m_p) \circ (m'_1 \circ \ldots \circ m'_k \circ a)$, we obtain $a \models m_1 \circ \ldots \circ m_p$ such that $a \models a \circ m'_1 \circ \ldots \circ m'_k \circ a$ (see Proposition 2.3). From $m \in m'_1 \circ \ldots \circ m'_k \circ (a \circ a)$, we obtain $b \models a \circ a$ such that $m \models m'_1 \circ \ldots \circ m'_k \circ b$. By validity of the sequent $\Gamma_1, \ldots, \Gamma_p \models A$, we deduce $a \models A$. Since, $a \models A \rightarrow B$, $a \models A$ and $b \models a \circ a$, we deduce $b \models B$. Then, by validity of the sequent $\Delta_1, \ldots, \Delta_k, B \models C$ in $\langle \mathcal{M}, \delta \rangle$, we deduce $m \models C$.

For rule $\langle \rightarrow_R \rangle$, we suppose that $(\mathcal{M}, \delta) \models \Gamma_1, \ldots, \Gamma_p, A \models B$ and we prove
(\mathcal{M}, \delta) \models \Gamma_1, \ldots, \Gamma_p \models A \rightarrow 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 \(m_1 \models \Gamma_1, \ldots, m_p \models \Gamma_p\). Let us prove \(m \models A \rightarrow B\). Thus, let \(a, b\) be such that \(b \in m \circ a\) and \(a \models A\) and let us prove \(b \models B\). 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 \(\Gamma_1, \ldots, \Gamma_p, A \models B\) in \((\mathcal{M}, \delta)\), we obtain \(b \models B\). \(\square\)

\textbf{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 \((\mathcal{M}, \delta)\).

\textbf{Proof.} First, we show that each rule of gBBI can be obtained as a combination of rules \(\langle \text{id} \rangle, \langle w \rangle, \langle c \rangle, \langle \ast_L \rangle, \langle \ast_R \rangle, \langle 1_l \rangle\) and \(\langle \land \rangle\).

\emph{case of rule} \(\langle \text{Ax} \rangle\)

\begin{align*}
\text{id} & : A \vdash A \\
\text{w} & : \sum^l, A \vdash A
\end{align*}

\emph{case of rule} \(\langle \ast (\rightarrow) \rangle\)

\begin{align*}
\text{id} & : \sum^l, \Delta \vdash B \quad C \vdash C \\
\langle \ast_L \rangle & : \sum^l, \Gamma \vdash A \\
\langle \ast_L \rangle & : \sum^l, \Delta, B \vdash C \quad C \vdash C \\
\langle \ast_L \rangle & : \sum^l, \Gamma, \sum^l, \Delta, A \vdash (B \rightarrow C) \quad C \vdash C \\
\langle \ast_L \rangle & : \sum^l, \Gamma, \sum^l, \Delta, 1 \land (A \rightarrow (B \rightarrow C)) \quad C \vdash C \\
\langle \ast_L \rangle & : \sum^l, \Gamma, \Delta \vdash C
\end{align*}

Remark that in the cases of rules \(\langle \text{Ax} \rangle\) and \(\langle \ast (\rightarrow) \rangle\), \(n\) represents the size of the multiset \(\Sigma\) (counting all the occurrences of the formulae that appear in \(\Sigma\)). Since the rules of \(\langle \text{id} \rangle, \langle w \rangle, \langle c \rangle, \langle \ast_L \rangle, \langle \ast_R \rangle, \langle 1_l \rangle\) and \(\langle \land \rangle\) 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 \((\mathcal{M}, \delta)\). \(\square\)

\textbf{C} The soundness of the encoding

\textbf{Proposition 5.2} For any \(m \in \mathbb{N}^n\) and \(p \in [1, n]\), if \(m_p = 0\) then the sequent \(\sum^l, c^m \models r_p\) has a proof in gBBI.
Proof. Let us fix \( p \in [1, n] \). Supposing \( m_p = 0 \), we build a \( \text{gBBI} \) proof tree of the sequent \( \Sigma^l, c^m \vdash r_p \) by induction on the size \( s = m_1 + \ldots + m_n \) of \( m \).

If \( s = 0 \) then \( m_1 = \ldots = m_n = 0 \) and \( c^m \) is the empty multiset. Here is a \( \text{gBBI} \) proof tree:

\[
\begin{array}{c}
\frac{\Sigma^l, c_1 \vdash c_1}{\Sigma^l \vdash r_p (c_1 \rightarrow c_1) \rightarrow r_p \in \Sigma_0 \subseteq \Sigma} \\
\end{array}
\]

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 \( m' + e_q = m \). We derive the identity \( c^m = c^{m'}, c_q \) between multisets. The size \( s' \) of \( m' \) is \( s' = s - 1 \) and we obviously have \( m'_p = 0 \). So we can apply the induction hypothesis to \( m' \) and obtain a proof tree \( Q \) for \( \Sigma^l, c^{m'} \vdash r_p \). From it, we build a proof tree suitable for \( \Sigma^l, c^m \vdash r_p \):

\[
\begin{array}{c}
\frac{\Sigma^l, c_q \vdash c_q}{\Sigma^l \vdash r_p (c_q \rightarrow (r_p \rightarrow r_p)) \in \Sigma_0 \subseteq \Sigma} \\
\end{array}
\]

Hence by induction, the sequent \( \Sigma^l, c^m \vdash r_p \) has a proof in \( \text{gBBI} \).

\[\square\]

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

**Proof.** Same argument as Proposition 5.2 but using side conditions \( (c_1 \rightarrow c_1) \rightarrow k \in \Sigma_0 \) and \( c_q \rightarrow (k \rightarrow k) \in \Sigma_0 \) instead of \( c_q \rightarrow ((r_p \rightarrow r_p) \in \Sigma_0 \).

\[\square\]