Expressivity properties of Boolean BI through relational models

Didier Galmiche[†] and Dominique Larchey-Wendling[♭]

LORIA – CNRS[♭] – UHP Nancy 1[†]
Campus Scientifique, BP 239
54 506 Vandœuvre-lès-Nancy, France

Abstract. In this paper, we study Boolean BI Logic (BBI) from a semantic perspective. This logic arises as a logical basis of some recent separation logics used for reasoning about mutable data structures and we aim at proposing new results from alternative semantic foundations for BBI that seem to be necessary in the context of modeling and proving program properties. Starting from a Kripke relational semantics for BBI which can also be viewed as a non-deterministic monoidal semantics, we first show that BBI includes some S4-like modalities and deduce new results: faithful embeddings of S4 modal logic, and then of intuitionistic logic (IL) into BBI, despite of the classical nature of its additive connectives. Moreover, we provide a logical characterization of the observational power of BBI through an adequate definition of bisimulation.

1 Introduction

Separation logics are logics for reasoning about mutable data structures [9, 12, 15] in which pre- and post-conditions are written in a logic enriched with specific forms of conjunction or implication. They are mainly based on the logic of Bunched Implications (BI) which combines standard (additive) intuitionistic implication $\rightarrow$ and conjunction $\wedge$ (additive connectives) and linear (intuitionistic) implication $\multimap$ and conjunction $*$ (multiplicative connectives) [11]. Actually, they mainly deal with Boolean BI (BBI) that is the version of BI in which the additive connectives are classical. Compared to BI, BBI needs further investigations from both semantic and proof-theoretic points of view. Recently we have proposed results about propositional BI: new semantics (based on relations or partially defined monoids) [8], labelled calculi and related proof-search methods from which decidability and finite model property have been proved [6].
Our aim is to obtain similar results for BBI, in order to provide new proof-theoretical foundations for this logic but also for some computational models of BBI like separation and spatial logics [2, 15]. Even if the difference with BI is mainly the classical nature of additives, we cannot directly derive such results from those of BI, for instance a (complete) based-on monoid semantics like in BI [8] or in classical BI pointer logic [9]. Therefore it seems is necessary to study new semantic foundations of BBI that initially has an algebraic model called Boolean BI-algebra [13]. In this context, we start from a Kripke relational semantics for BBI, that is proved sound and complete, and also provide an equivalent semantics based on non-deterministic monoids. The first ternary-relation

models for BBI, defined by Yang [17], are based on the notion of maximally consistent sets. Their definitions and proofs strongly use classical negation and are tailored towards BBI. Our semantics, that is equivalent, is in the continuation of our works about relational models of (intuitionistic) BI [8] and does not deal with negation. It might be suitable to consider open problems like, for instance, the existence of a (deterministic) based-on monoid semantics for BBI? Even if we can define, from this semantics, labelled calculi and thus prove their completeness for BBI, it would remain to study properties of propositional BBI, like decidability and finite model property. Our relational models for BBI, that extend those for BI, seem to provide good foundations for such a study. As a consequence of the soundness property, we propose as central contributions embeddings of modal logic S4, and then of intuitionistic logic IL into BBI. The later could be surprising despite of the classical nature of its additive connectives. These embeddings have consequences on the use of BBI from proof-search and complexity perspectives. To complete these semantical investigations about BBI, we also provide a logical characterization of its observational power through an adequate definition of bisimulation.

2 Boolean BI

Boolean BI, denoted by BBI, is a mixed logic like BI [13] that has some computational models like separation and spatial logics [2, 15]. It is built on a set Var of propositional variables combined using *additive* connectives of classical propositional logic ($\wedge$, $\vee$, $\rightarrow$, $\neg$, $\perp$ and $\top$) and *linear* connectives of multiplicative linear logic ($*$, $-\!\!*$ and I).

Provability in BBI is defined in [13] by adding the rule of *reductio ad absurdum* denoted [RAA] to the natural deduction calculus of BI.[1] In this paper, like in [17], we rather adopt a Hilbert deduction system to define provability in BBI. We only recall here the axioms and rules that characterize BBI. First, we choose any (finite) set of axioms for the classical part of BBI among the axiom sets for classical propositional logic.[2] We add to it the following axioms for the linear part:

$$\frac{A \vdash \neg\neg B}{A \vdash B}\ [\mathrm{RAA}]$$

$$\begin{array}{ll} 1.\ A \rightarrow (\mathsf{I} * A) & 3.\ (A * B) \rightarrow (B * A) \\ 2.\ (\mathsf{I} * A) \rightarrow A & 4.\ (A * (B * C)) \rightarrow ((A * B) * C) \end{array}$$

All these axioms should be considered as *schemes*, i.e., we consider the closure of the set of axioms under (uniform) substitutions. Moreover, we have the following Hilbert *deduction rules* for BBI:

$$\frac{\vdash A \qquad \vdash A \rightarrow B}{\vdash B}\ [\mathrm{MP}] \qquad \frac{\vdash A \rightarrow C \qquad \vdash B \rightarrow D}{\vdash (A * B) \rightarrow (C * D)}\ [*]$$

$$\frac{\vdash A \rightarrow (B -\!\!* C)}{\vdash (A * B) \rightarrow C}\ [-\!\!*_1] \qquad \frac{\vdash (A * B) \rightarrow C}{\vdash A \rightarrow (B -\!\!* C)}\ [-\!\!*_2]$$

[1] with $\neg A$ defined as $\neg A \equiv A \rightarrow \perp$.

[2] such axioms could be for example $A \rightarrow (A \vee B)$, $A \rightarrow (B \rightarrow (A \wedge B))$, ...

The [MP]-rule is the usual *modus ponens* and the three other rules $[*]$, $[-\!\!*_1]$ and $[-\!\!*_2]$ hold for BI and BBI. Compared to BI, the additive axioms of BBI are those of classical logic instead of intuitionistic logic. So the set of "classical" axioms of BBI contains a form of *reductio ad absurdum*, like for example $\neg\neg A \to A$. An algebraic model for this system is called a *Boolean* BI-*algebra*. We denote by $A \simeq B$ the logical equivalence of A and B (both $\vdash A \to B$ and $\vdash B \to A$ are deducible from the axioms).

Proposition 1. *The following logical equivalences hold in* BI *and* BBI*:*

$$\begin{array}{rcl@{\qquad}rcl} \bot * A & \simeq & \bot & (A \vee B) * C & \simeq & (A * C) \vee (B * C) \\ \bot -\!\!* A & \simeq & \top & (A \vee B) -\!\!* C & \simeq & (A -\!\!* C) \wedge (B -\!\!* C) \\ A -\!\!* \top & \simeq & \top & A -\!\!* (B \wedge C) & \simeq & (A -\!\!* B) \wedge (A -\!\!* C) \end{array}$$

Computational models of BBI, like BI's pointer logic (PL), are used for reasoning about mutable data structures [9] and we aim at studying them in a proof-theoretic perspective from their semantics [7]. Starting from our results on BI [6, 8] we need first to study relational models for BBI.

3 A Kripke Relational Semantics for BBI

Before to study semantics of BBI, we emphasize the relationships between the notions of *non-deterministic* monoid and so-called *relational frame*.

3.1 Non-deterministic monoids and relational semantics

Let us consider a set $\mathcal{M}$. We denote by $\mathcal{P}(\mathcal{M})$ the powerset of $\mathcal{M}$, i.e. its set of subsets. A binary function $\circ : \mathcal{M} \times \mathcal{M} \longrightarrow \mathcal{P}(\mathcal{M})$ is naturally extended to a binary operator on $\mathcal{P}(\mathcal{M})$ by $X \circ Y = \bigcup\{x \circ y \mid x \in X, y \in Y\}$ for any subsets X, Y of $\mathcal{M}$. Using this extension, we can identify an element m of $\mathcal{M}$ with the singleton set $\{m\}$ and derive the equations $m \circ X = \{m\} \circ X$ and $a \circ b = \{a\} \circ \{b\}$.

Definition 1. *A* non-deterministic monoid *is a triple* $(\mathcal{M}, \circ, \mathsf{e})$ *where* $\mathsf{e} \in \mathcal{M}$ *and* $\circ : \mathcal{M} \times \mathcal{M} \longrightarrow \mathcal{P}(\mathcal{M})$ *for which the following conditions hold:*
1. $\forall a \in \mathcal{M}, \mathsf{e} \circ a = \{a\}$ *(identity)*
2. $\forall a, b \in \mathcal{M}, a \circ b = b \circ a$ *(commutativity)*
3. $\forall a, b, c \in \mathcal{M}, a \circ (b \circ c) = (a \circ b) \circ c$ *(associativity)*[3]

The term *non-deterministic* is introduced in order to emphasize the fact that the composition $a \circ b$ may yield not only one but several results including the possible incompatibility of a and b in which case $a \circ b = \emptyset$. If $(\mathcal{M}, \times, 1)$ is a commutative monoid then, defining $a \circ b = \{a \times b\}$ and $\mathsf{e} = 1$ induces a non-deterministic monoid structure on $\mathcal{M}$. Partial monoids can also be represented using the empty set $\emptyset$ as the result of undefined compositions. We claim that the notion of non-deterministic monoid is an extension of the notion of partial commutative monoid. Then, these models generalize the (associative and commutative) tree based models [5] or the process based models [3] of separation logics. We establish an algebraic link between non-deterministic monoids and Boolean-BI algebras.

[3] The axiom of associativity should be understood using the extension of $\circ$ to $\mathcal{P}(\mathcal{M})$.

Proposition 2. *Let the triple* $(\mathcal{M}, \circ, \mathsf{e})$ *be a non-deterministic monoid. Then* $(\mathcal{P}(\mathcal{M}), \subseteq, \circ)$ *is a quantale and also a complete boolean algebra.*

Using the isomorphism between $\mathcal{M} \times \mathcal{M} \longrightarrow \mathcal{P}(\mathcal{M})$ and $\mathcal{M} \times \mathcal{M} \times \mathcal{M} \longrightarrow \mathbf{2} = \{\mathsf{false} < \mathsf{true}\}$, we define a ternary relation $\triangleright \subseteq \mathcal{M} \times \mathcal{M} \times \mathcal{M}$ by: $\quad a, b \triangleright c$ iff $c \in a \circ b$. Then we can also consider non-deterministic monoids as relational frames.

Definition 2. *A* relational frame *is a triple* $(\mathcal{M}, \triangleright, \mathsf{e})$ *where* e *is an element of* $\mathcal{M}$ *and* $\triangleright$ *a ternary relation on* $\mathcal{M}$ *satisfying, for all* $a, b, c, d \in \mathcal{M}$*:*
1. $e, a \triangleright b$ *iff* $a = b$ *(identity)*
2. $a, b \triangleright c$ *iff* $b, a \triangleright c$ *(commutativity)*
3. if $\exists k\, (a, k \triangleright d$ *and* $b, c \triangleright k)$ *then* $\exists p\, (a, b \triangleright p$ *and* $p, c \triangleright d)$ *(associativity)*

The relation $m, a \triangleright b$ can be read in both directions: "the composition of m and a yields b" or "b is decomposable into m and a." We claim that relational frames can model process calculi and resource calculi or a combination of both like in [14]. The two notions of non-deterministic monoid and relational frame are in fact completely isomorphic. In the following, we will rather use the relational frame notion.
Moreover, from Proposition 2, it is clear that non-deterministic monoids (or equivalently relational frames) induce Boolean BI algebras on the powerset of their career.

3.2 A Relational Semantics for BBI

Let $(\mathcal{M}, \triangleright, \mathsf{e})$ be a relational frame and $v : \mathsf{Var} \longrightarrow \mathcal{P}(\mathcal{M})$ be a *valuation*, i.e. an interpretation of propositional variables. We define, by induction on formulae, a *forcing relation* $\Vdash$ between elements of $\mathcal{M}$ and formulae of BBI:

$$
\begin{array}{rcl@{\qquad}rcl}
m \Vdash \mathsf{I} & \text{iff} & m = \mathsf{e} & m \Vdash X & \text{iff} & m \in v(X) \\
m \Vdash \bot & \text{iff} & \text{never} & m \Vdash A \vee B & \text{iff} & m \Vdash A \text{ or } m \Vdash B \\
m \Vdash \top & \text{iff} & \text{always} & m \Vdash A \wedge B & \text{iff} & m \Vdash A \text{ and } m \Vdash B \\
m \Vdash \neg A & \text{iff} & m \nVdash A & m \Vdash A \rightarrow B & \text{iff} & m \nVdash A \text{ or } m \Vdash B
\end{array}
$$

$$
\begin{array}{rcl}
m \Vdash A * B & \text{iff} & \exists a, b \text{ s.t. } a, b \triangleright m \text{ and } a \Vdash A \text{ and } b \Vdash B \\
m \Vdash A \mathrel{-\!\!*} B & \text{iff} & \forall a, b\ (m, a \triangleright b \text{ and } a \Vdash A) \text{ implies } b \Vdash B
\end{array}
$$

Theorem 1 (Soundness). *Let* $(\mathcal{M}, \triangleright, \mathsf{e})$ *be a relational frame and* v *a valuation. If* $A \in \mathsf{BBI}$ *is provable then for any element* m *of* $\mathcal{M}$*,* $m \Vdash A$ *holds.*

Proof. Let us fix a relational frame $(\mathcal{M}, \triangleright, \mathsf{e})$ and a valuation $v : \mathsf{Var} \longrightarrow \mathcal{P}(\mathcal{M})$. Since the interpretation of the additive connectives of BBI is the standard Kripke interpretation of classical propositional connectives, all theorems of classical logic are forced by all elements of $\mathcal{M}$. Moreover the rule [MP] preserves forcing since it is the standard *modus ponens* rule of classical logic. We only have to check that the linear axioms are forced and also that the three deduction rules $[*]$, $[\mathrel{-\!\!*}_1]$ and $[\mathrel{-\!\!*}_2]$ preserve forcing.
Let us check axiom 4 (section 2). Let m be such that $m \Vdash A * (B * C)$. We prove that $m \Vdash (A * B) * C$. By definition of the forcing relation, there exist a, k s.t. $a, k \triangleright m$ and $a \Vdash A$ and $k \Vdash B * C$. So there exist $b, c \triangleright k$ s.t. $b \Vdash B$ and $c \Vdash C$. Thus $a, k \triangleright m$ and $b, c \triangleright k$ holds. By associativity of the $\triangleright$ relation, there exists p s.t. $a, b \triangleright p$ and $p, c \triangleright m$. Since

$a,b \triangleright p$, we deduce $p \Vdash A * B$ and since $p,c \triangleright m$, we deduce $m \Vdash (A*B)*C$.
Now let us check the deduction rule $[\multimap_1]$. Suppose that for any element m of $\mathcal{M}$, $m \Vdash A \to (B \multimap C)$ holds. Let k be an element of $\mathcal{M}$ such that $k \Vdash A*B$ holds. Let us prove that $k \Vdash C$ holds. Since $k \Vdash A*B$, there exist a,b s.t. $a,b \triangleright k$ and $a \Vdash A$ and $b \Vdash B$. Since $a \Vdash A$ holds and $a \Vdash A \to (B \multimap C)$ holds (by instantiation of the hypothesis), then $a \Vdash B \multimap C$ holds. But since $a,b \triangleright k$ holds, by definition of the forcing relation, we deduce $k \Vdash C$.

Let us study the completeness of this relational semantics by extending techniques we used to prove completeness of the relational semantics of BI [8]. We define a term model based on the *Lindenbaum construction* and the *prime filters* of this boolean algebra. We denote by $\mathcal{L}$ the set of classes of logically equivalent formulae and these classes by the letters $a,b,c...$ The class of a formula A is denoted $[A] = \{B \mid A \simeq B\}$. The $\simeq$ equivalence relation is a congruence and the logical connectives induce algebraic operators on the Lindenbaum algebra. An order relation is defined between classes by $[A] \leqslant [B]$ iff $\vdash A \to B$ is provable and $(\mathcal{L}, \leqslant)$ has the structure of a boolean algebra with least element $0 = [\bot]$ and greatest element $1 = [\top]$, each classical connective inducing a corresponding boolean operator. We introduce $\mathsf{i} = [\mathsf{I}]$ as the class of the monoidal unit.

Filters and prime filters. The *upward closure* of a subset X of $\mathcal{L}$ is defined by $\uparrow X = \{k \in \mathcal{L} \mid \exists x \in X, x \leqslant k\}$. A *filter* F of $\mathcal{L}$ is a non-empty ($1 \in F$) upward closed ($\uparrow F = F$) and meet-stable ($\forall x,y \in F, x \wedge y \in F$) subset of $\mathcal{L}$. If x is an element of $\mathcal{L}$ then $\uparrow x = \{k \in \mathcal{L} \mid x \leqslant k\}$ is the least filter containing x. $\uparrow 0 = \mathcal{L}$ is the greatest filter.

A *prime filter* F_p of $\mathcal{L}$ is a filter which is *proper* ($0 \notin F_p$) and satisfies $\forall a,b \in \mathcal{L}, a \vee b \in F_p$ implies ($a \in F_p$ or $b \in F_p$). Let us recall the following result: since $\mathcal{L}$ is a boolean algebra, the prime filters are exactly the maximal proper filters of $\mathcal{L}$ [4].

Proposition 3. *Let F_p, G_p be prime filters of $\mathcal{L}$. If $F_p \subseteq G_p$ then $F_p = G_p$.*

We denote by $\mathbb{F}$ (resp. $\mathbb{F}_p$) the set of filters (resp. prime filters) of $\mathcal{L}$. They are ordered by inclusion $\subseteq$ and, by Proposition 3, the order on $\mathbb{F}_p$ is flat. We define a (commutative) monoidal operation on $\mathbb{F}$ by $A \bullet B = \uparrow\{a * b \mid a \in A \text{ and } b \in B\}$. Then $(\mathbb{F}, \subseteq, \bullet, \uparrow\mathsf{i})$ is an *ordered commutative monoid*. The greatest filter $\uparrow 0$ is an absorbing element of $\bullet$.[4]

Definition 3. *A* prime predicate $\varphi : \mathbb{F} \longrightarrow \mathbf{2} = \{\mathsf{false} < \mathsf{true}\}$ *satisfies*
1. $\bigwedge_k \varphi(F_k) \leqslant \varphi(\bigcup_k F_k)$ *for any chain* $(F_k)_{k \in I}$.
2. $\varphi(F \cap G) \leqslant \varphi(F) \vee \varphi(G)$ *for any filters* F, G.
3. $\varphi(\uparrow 0) = \mathsf{false}$.

Let us give two examples of prime predicates. Let $x < 1$ be an element of $\mathcal{L}$. Then the map $F \mapsto x \notin F$ is a prime predicate. Let $A \in \mathbb{F}$ and $H_p \in \mathbb{F}_p$ then $F \mapsto A \bullet F \subseteq H_p$ is also a prime predicate.[5]

Lemma 1 (prime extension). *If φ if a prime predicate and F a filter such that $\varphi(F) = \mathsf{true}$, then there exists a prime filter F_p extending F ($F \subseteq F_p$) and such that $\varphi(F_p) = \mathsf{true}$.*

[4] So for any filters F, G, if $0 \in F$ then $0 \in F \bullet G$.
[5] This property involves the distributivity of $*$ over $\vee$ (see Proposition 1).

This lemma is proved using Zorn's lemma and expresses that a filter satisfying a prime predicate can be extended to a prime filter satisfying the same predicate.

Corollary 1. *We have the two following results:*
1. Let $x \in \mathcal{L}$ and $F \in \mathbb{F}$ s.t. $x \notin F$. There exists $F_p \in \mathbb{F}_p$ s.t. $F \subseteq F_p$ and $x \notin F_p$.
In particular, if $x < 1$, there exists $F_p \in \mathbb{F}_p$ s.t. $x \notin F_p$.
2. Let $A, B \in \mathbb{F}$ and $H_p \in \mathbb{F}_p$ s.t. $A \bullet B \subseteq H_p$. There exist $A_p, B_p \in \mathbb{F}_p$ s.t. $A \subseteq A_p$, $B \subseteq B_p$ and $A_p \bullet B_p \subseteq H_p$.

Term models with one unit. Indeed, the set $\mathbb{F}_p$ of prime filters cannot be used directly as a model of BBI because several extensions of the unit I exist. We have to select a particular one to obtain a model with a unique unit. This problem is also studied in [17].

Definition 4. *Let I_p, F_p be prime filters. I_p is a* unit *if $\mathsf{i} \in I_p$. I_p is a* unit of F_p *if I_p is a unit and $I_p \bullet F_p \subseteq F_p$.*

Since $\mathsf{i} \in I_p$, for any filter F we have $F \subseteq I_p \bullet F$. Consequently if I_p is a unit of F_p then the identity $I_p \bullet F_p = F_p$ holds.

Proposition 4. *Let I_p, I'_p be two units and F_p be a prime filter, we have*
1. I_p is a unit of I_p;
2. $0 \notin I_p \bullet I'_p$ if and only if $I_p = I'_p$;
3. $0 \notin I_p \bullet F_p$ if and only if I_p is a unit of F_p.

Proposition 5. *Every prime filter has a unique unit.*

Proposition 6. *Let A_p, B_p and C_p be prime filters. If $A_p \bullet B_p \subseteq C_p$ holds then A_p, B_p and C_p share the same unit.*

Proof. Proofs of Proposition 4,5,6 are given in appendix A.

We now can build a term model with a unique unit. Let us fix a unit I_p. Among the primer filters, we only consider those having I_p for unit. Let $\mathcal{M} = \{F_p \in \mathbb{F}_p \mid I_p \text{ is a unit of } F_p\}$. We define the ternary relation $\triangleright$ on $\mathcal{M}$ by $A_p, B_p \triangleright C_p$ iff $A_p \bullet B_p \subseteq C_p$. We also define a valuation $v : \mathsf{Var} \longrightarrow \mathcal{P}(\mathcal{M})$ by $F_p \in v(X)$ iff $[X] \in F_p$. We interpret propositional variables with the valuation v and obtain a forcing relation $\Vdash$.

Lemma 2. *The triple $(\mathcal{M}, \triangleright, I_p)$ is a relational frame, in which we use the previously defined forcing relation $\Vdash$. Then, for any formula A of BBI and any prime filter F_p of $\mathcal{M}$, $F_p \Vdash A$ iff $[A] \in F_p$.*

Proof. See appendix B.

Theorem 2 (Completeness). *If A is not provable in BBI, then there exists a relational frame which is a counter-model of A.*

Proof. Let A be not provable in BBI. Let a be its class $[A]$ in $\mathcal{L}$. Then $a < 1$. So by Corollary 1, there exists a prime filter F_p such that $a \notin F_p$. Let I_p be the unit of F_p and $\mathcal{M}$ be relation frame associated to I_p according to Lemma 2. Then $F_p \in \mathcal{M}$ since I_p is the unit of F_p. Moreover $[A] = a \notin F_p$ and thus $F_p \nVdash A$.

Compared to the relational semantics, based on maximally consistent sets, proposed by Yang [17], our semantics can be seen as more abstract and extends the one we defined for (intuitionistic) BI [8]. It generalizes previous models for separation logics for trees and processes. From such a semantics we could define a tableau method for BBI and proved its completeness but in order to study decidability and finite model properties for BBI we need to deeper analyze the resolution of relational constraints.

4 Embeddings of S4 and IL into BBI

In this section, we exploit the relational semantics of BBI, mainly its soundness, in addition to the definition of a S4-like modality of BBI in order to faithfully embed the modal logic S4, and then the intuitionistic logic IL, into BBI.

4.1 A S4-like modality in BBI

We introduce the denotation $\Box A$ as an abbreviation of $\top \mathrel{-\!\!*} A$. Given a relational frame $(\mathcal{M}, \triangleright, \mathsf{e})$, we define the relation $\preccurlyeq$ between elements of $\mathcal{M}$ by $a \preccurlyeq b$ if there exists $m \in \mathcal{M}$ such that $m, a \triangleright b$. It is easy to verify that $\preccurlyeq$ is a *preorder* on the set $\mathcal{M}$, i.e., a reflexive and transitive relation. Moreover the Kripke interpretation of the $\Box$ operator is expressed by: $m \Vdash \Box A$ iff $\forall k, m \preccurlyeq k$ implies $k \Vdash A$.
Then $\Box A$ is Kripke interpreted the same way as in S4. Let us check now if the axioms of S4 are theorems of BBI.

Proposition 7. *The three axioms $\Box(A \to B) \to (\Box A \to \Box B)$, $\Box A \to A$ and $\Box A \to \Box\Box A$ of* S4 *are provable in* BBI*. If A is provable in* BBI*, then $\Box A$ is provable in* BBI*.*

Proof. We give a proof of $\Box A \to A$. Let $K_1 \equiv (\top \mathrel{-\!\!*} A) * \mathsf{I}$, $K_2 \equiv (\top \mathrel{-\!\!*} A) * \top$. $(\top \mathrel{-\!\!*} A) \to (\top \mathrel{-\!\!*} A)$ is a (classical) axiom of BBI. So by rule $[\mathrel{-\!\!*}_1]$, $K_2 \to A \equiv ((\top \mathrel{-\!\!*} A) * \top) \to A$ is provable. Moreover $\mathsf{I} \to \top$ is a (classical) tautology of BBI and then, by rule $[*]$, $K_1 \to K_2 \equiv ((\top \mathrel{-\!\!*} A) * \mathsf{I}) \to ((\top \mathrel{-\!\!*} A) * \top)$ is provable. As $(\top \mathrel{-\!\!*} A) \to K_1 \equiv (\top \mathrel{-\!\!*} A) \to ((\top \mathrel{-\!\!*} A) * \mathsf{I})$ is an axiom of BBI, by combining $(\top \mathrel{-\!\!*} A) \to K_1$ with $K_1 \to K_2$ and $K_2 \to A$ we get a proof of $\Box A \to A$.
We now prove the deduction rule. Let A be a provable formula of BBI. Then $\top \to A$ is provable. Moreover $(\top * \top) \to \top$ is (classical) tautology of BBI. Combining those two, $(\top * \top) \to A$ is provable and then by rule $[\mathrel{-\!\!*}_2]$, $\top \to (\top \mathrel{-\!\!*} A)$ is provable. Moreover $\top$ is a (classical) axiom and thus, by rule [MP], $\top \mathrel{-\!\!*} A$ is provable, i.e., $\Box A$ is provable.

As a corollary to this result, we define a mapping from formulae of S4 to formulae of BBI built on the same set Var of propositional variables. Let $A \mapsto A^{\Box}$ be recursively defined by the following equations:

$$\begin{array}{rclrclr} (\neg A)^{\Box} & = & \neg A^{\Box} & K^{\Box} & = & K & \text{for } K \in \mathsf{Var} \cup \{\bot, \top\} \\ (\Box A)^{\Box} & = & \top \mathrel{-\!\!*} A^{\Box} & (A \otimes B)^{\Box} & = & A^{\Box} \otimes B^{\Box} & \text{for } \otimes \in \{\wedge, \vee, \to\} \end{array}$$

Corollary 2. *If A is a provable formula of* S4 *then $A^{\Box}$ is provable in* BBI*.*

Proof. By Proposition 7, all the (specific) axioms and deductions rules of S4 are also derivable in BBI. The other rule of S4 (which is [MP]) and the other axioms of S4 are those of classical propositional logic, which is a part of BBI.

4.2 From trees to relational frames

A *partial order* $\leqslant$ is a reflexive, antisymmetric and transitive relation. Two elements a and b are *upper bounded* when they have a common upper bound m such that $a \leqslant m$ and $b \leqslant m$. Two elements a and b are *comparable* if either $a \leqslant b$ or $b \leqslant a$.

Definition 5. *A* tree $(\mathcal{T}, \leqslant, r)$ *is a partial order where r is the least element of $\mathcal{T}$. Moreover any two upper bounded elements of $\mathcal{T}$ are comparable.*

Theorem 3. *If A is a formula of* $\mathsf{S4}$ *which is not provable, then there exists a tree $(\mathcal{T}, \leqslant, r)$ such that $r \nVdash A$.*

Proof. We recall the main argument of the proof given in [1] (pages 59–63). Since A is not provable, it has a counter-model $(\mathcal{Q}, \leqslant)$ in the class of preorders. For some element $r \in \mathcal{Q}$, the property $r \nVdash A$ holds. Consider the set $\mathcal{S}$ of *finite increasing sequences* of the form $(r = a_0, a_1, \ldots, a_n)$ for $n \geqslant 0$. The set $\mathcal{S}$ is ordered by the *prefix order* between sequences and thus $\mathcal{S}$ is a tree with root (r). The mapping $(a_0, a_1, \ldots, a_n) \mapsto a_n$ from $\mathcal{S}$ to $\mathcal{Q}$ is a *surjective bounded morphism* so it preserves the forcing relation. Thus $r \nVdash A$ in the tree $\mathcal{S}$.

Let $(\mathcal{T}, \leqslant, r)$ be a tree. Then the max operator is a partial commutative monoidal operator with unit r. We build a ternary relation on $\mathcal{T}$ by:

$$a, b \triangleright m \ \text{ iff } \ a \text{ and } b \text{ are comparable and } m = \max\{a, b\}$$

Proposition 8. *$(\mathcal{T}, \triangleright, r)$ is a relational frame and the preorder $\preccurlyeq$ induced by $\triangleright$ matches $\leqslant$, i.e., $\preccurlyeq = \leqslant$.*

Proof. Since r is the neutral element of $\mathcal{T}$, the identity axiom is obvious. Commutativity is also obviously verified. Let us check associativity. If $a, k \triangleright d$ and $b, c \triangleright k$ hold, then b and c are comparable and $k = \max\{b, c\}$. Then d is an upper bound of a, b and c. Since, $k \in \{b, c\}$ and $d \in \{a, k\}$, then $d \in \{a, b, c\}$. Thus $d = \max\{a, b, c\}$. Since $\mathcal{T}$ is a tree and a and b are upper bounded by d, then a and b are comparable[6] and let $p = \max\{a, b\}$. Then $a, b \triangleright p$ and $p, c \triangleright d$. We conclude that $\triangleright$ is associative. If $a \preccurlyeq b$ there exists m s.t. $m, a \triangleright b$. Then $b = \max\{m, a\}$ and we obtain $a \leqslant b$. Conversely if $a \leqslant b$ then $r, a \triangleright b$ and thus $a \preccurlyeq b$ holds. Consequently the identity $\preccurlyeq = \leqslant$ holds.

Theorem 4. *If A is not provable in* $\mathsf{S4}$*, then $A^{\Box}$ is not provable in* BBI.

Proof. Since A is not provable in $\mathsf{S4}$, by Theorem 3, there exist a (potentially infinite) tree $(\mathcal{T}, \leqslant, r)$ and a valuation $v : \mathsf{Var} \longrightarrow \mathcal{P}(\mathcal{T})$ s.t. $r \nVdash_{\mathsf{S4}} A$. We consider the associated relational frame $(\mathcal{T}, \triangleright, r)$ and use the same valuation v. By Proposition 8, the identity $\preccurlyeq = \leqslant$ holds. By a structural induction on F, formula of $\mathsf{S4}$, we prove that for any $m \in \mathcal{T}$, $m \Vdash_{\mathsf{S4}} F$ iff $m \Vdash_{\mathsf{BBI}} F^{\Box}$. Then, in particular, $r \nVdash_{\mathsf{BBI}} A^{\Box}$. Then $(\mathcal{T}, \triangleright, r)$ associated to v is a counter-model of $A^{\Box}$. By soundness, we deduce that $A^{\Box}$ is not provable in BBI.

[6] Here the fact that $\mathcal{T}$ is a tree is required. The max operator would not necessarily be associative if $\mathcal{T}$ was only a partial order or preorder.

A direct consequence of the faithful embedding $A \mapsto A^{\Box}$ is the following: it is well known that propositional intuitionistic logic IL can be faithfully embedded into $\mathsf{S4}$ by prefixing with a $\Box$ all variables $X \mapsto \Box X$ and implications $(A \to B) \mapsto \Box(A \to B)$ while preserving the rest of the structure of the formula. Thus combining both embeddings we have the following result:

Theorem 5. *There exist faithful embeddings of* $\mathsf{S4}$ *and* IL *into* BBI.

This result is surprising because we could naively think that BBI with its classical propositional connectives has a "classical" nature. Moreover, such embeddings have an impact on proof-search in BBI. In particular, if BBI is decidable as we still hope to prove it in further works, its complexity is at least polynomial-space complete (the complexity of IL [16] and $\mathsf{S4}$). Even if it is complete w.r.t. to partial orders or trees, $\mathsf{S4}$, does not have the finite model property for these models. However, $\mathsf{S4}$ has the finite model property for preorders [1]. This point emphasizes the importance of the right tuning of axioms when seeking the finite model property and could be a hint to a finer axiomatization of relational semantics. Moreover, BBI is also an extension of multiplicative intuitionistic linear logic MILL [13] and we cannot say if it is faithful.

5 BBI and bisimulation in relational frames

In this section, we deal with the formulae of BBI in order to distinguish elements of relational frames. We provide a characterization of the *observational power* of BBI: it is the ω-limit denoted $\sim_\omega$ of the transfinite decreasing sequence leading to the greatest bisimulation (see [10]) denoted $\sim$. Then, we discuss further conditions under which the identity $\sim = \sim_\omega$ would hold. We consider the Lindenbaum algebra $\mathcal{L}$ of BBI. Unlike what we have done before, we do not distinguish between a formula A and its class of logical equivalence $[A]$. So we write $A = B$ when we have $A \simeq B$.

5.1 BBI in finite slices

Let δ be the function defining the weight of binary logical connectives: $\delta(\vee) = \delta(\wedge) = \delta(\to) = 0$ and $\delta(*) = \delta(-\!\!*) = 1$. The *rank* of a formula A, denoted $\mathsf{rank}(A)$, is defined by induction on the structure of A as follows:

$$\mathsf{rank}(\neg A) = \mathsf{rank}(A) \;\text{ and }\; \mathsf{rank}(K) = 0 \text{ for } K \in \mathsf{Var} \cup \{\bot, \top, \mathsf{I}\}$$
$$\mathsf{rank}(A \otimes B) = \max\{\mathsf{rank}(A), \mathsf{rank}(B)\} + \delta(\otimes) \text{ for } \otimes \in \{\vee, \wedge, \to, *, -\!\!*\}$$

Then an additive connective preserves the rank while a linear connective increases the rank by one. This notion of rank is not the same as in [5] but it serves the same purpose: to cut BBI into finite slices. The rank of a class of logically equivalent formulae is the least rank of its representatives (i.e. its elements). We denote by $\mathcal{L}_r$ the subset of $\mathcal{L}$ composed of (classes of) formulae of rank at most r. Obviously, since boolean (additive) connectives preserve the rank, $\mathcal{L}_r = \{A \in \mathcal{L} \mid \mathsf{rank}(A) \leqslant r\}$ is a sub-boolean algebra of $\mathcal{L}$. In particular, $\mathcal{L}_0$ contains all the propositional variables of Var and the multiplicative unit I.

Let $\mathcal{K}$ be a subset of $\mathcal{L}$. The *sub-boolean algebra generated by* $\mathcal{K}$, denoted $\mathcal{B}(\mathcal{K})$, is the least subset of $\mathcal{L}$ containing $\mathcal{K} \cup \{\bot, \top\}$ and closed under the boolean operators $\vee$, $\wedge$, $\rightarrow$ and $\neg$. It is clear that $\mathcal{B}(\cdot)$ is a *closure operator* on $\mathcal{L}$. Moreover formulae of rank 0 cannot contain the $*$ or $-\!*$ connectives, so any formula of $\mathcal{L}_0$ is a boolean combination of atomic formulae and $\mathcal{L}_0 = \mathcal{B}(\mathsf{Var} \cup \{\mathsf{I}\})$.

Proposition 9. *If $\mathcal{K}$ is a finite subset of $\mathcal{L}$ then $\mathcal{B}(\mathcal{K})$ is finite.*

Proof. Suppose $\mathcal{K} = \{K_1, \ldots, K_n\}$ and let $\mathcal{X} = \{X_1, \ldots, X_n\}$ be a set of (distinct) variables. We denote by $\mathcal{B}_{\mathcal{X}}$ the (finite) boolean algebra freely generated by $\mathcal{X}$. There is a unique boolean algebra homomorphism $\varphi : \mathcal{B}_{\mathcal{X}} \longrightarrow \mathcal{L}$ such that $\forall i\ \varphi(X_i) = K_i$. Its image is the least sub-boolean algebra of $\mathcal{L}$ containing $\mathcal{K}$: $\varphi(\mathcal{B}_{\mathcal{X}}) = \mathcal{B}(\mathcal{K})$. Since $\mathcal{B}_{\mathcal{X}}$ is finite, then $\mathcal{B}(\mathcal{K})$ is finite.

Let $\mathcal{K}$ be a finite subset of $\mathcal{L}$. We define a mapping $\overline{(\cdot)} : \mathcal{P}(\mathcal{K}) \longrightarrow \mathcal{L}$ from subsets of $\mathcal{K}$ to $\mathcal{L}$ by: $\quad \overline{\Gamma} = \bigwedge\{A \mid A \in \Gamma\} \wedge \bigwedge\{\neg A \mid A \in \mathcal{K} - \Gamma\}$
It is clear that for any $\Gamma \in \mathcal{P}(\mathcal{K})$, $\overline{\Gamma}$ is an element of $\mathcal{B}(\mathcal{K})$. In fact, the direct image of the mapping $\overline{(\cdot)} : \mathcal{P}(\mathcal{K}) \longrightarrow \mathcal{B}(\mathcal{K})$ is either Min or $\mathsf{Min} \cup \{\bot\}$, where Min is the set of *minimal elements* of $\mathcal{B}(\mathcal{K}) - \{\bot\}$.

Proposition 10. *For $A \in \mathcal{K}$, the identity $A = \bigvee\{\overline{\Gamma} \mid A \in \Gamma$ and $\Gamma \subseteq \mathcal{K}\}$ holds.*

This property is inherited from the freely generated boolean algebra $\mathcal{B}_{\mathcal{X}}$ we introduced in the preceding proof. We now associate to a finite set $\mathcal{K}$ of formulae of $\mathcal{L}$, a finite set $\psi(\mathcal{K})$ containing formulae of potentially greater rank:

$$\psi(\mathcal{K}) = \{\overline{\Gamma} * \overline{\Delta} \mid \Gamma, \Delta \in \mathcal{P}(\mathcal{K})\} \cup \{\neg(\overline{\Gamma} -\!* \neg\overline{\Delta}) \mid \Gamma, \Delta \in \mathcal{P}(\mathcal{K})\}$$

Proposition 11. *If $\mathcal{K}$ is a finite subset of $\mathcal{L}_r$ then $\psi(\mathcal{K})$ is a finite subset of $\mathcal{L}_{r+1}$.*
If $\mathsf{I} \in \mathcal{K}$ then $\mathcal{K} \subseteq \mathcal{B}(\psi(\mathcal{K}))$.

Proof. The first result is trivial. If $\mathsf{I} \in \mathcal{K}$ then $\mathsf{I} = \bigvee\{\overline{\Gamma} \mid \mathsf{I} \in \Gamma$ and $\Gamma \in \mathcal{P}(\mathcal{K})\}$ by Proposition 10. Let $A \in \mathcal{K}$, by Proposition 10, we have $A = \bigvee\{\overline{\Delta} \mid A \in \Delta$ and $\Delta \in \mathcal{P}(\mathcal{K})\}$. Then, by distributivity of $*$ over $\vee$ (see Proposition 1), we obtain the identities $A = \mathsf{I} * A = \bigvee\{\overline{\Gamma} * \overline{\Delta} \mid \mathsf{I} \in \Gamma, A \in \Delta$ and $\Gamma, \Delta \in \mathcal{P}(\mathcal{K})\}$. Then $A \in \mathcal{B}(\psi(\mathcal{K}))$.

Proposition 12. *If $\mathcal{L}_r$ is finite then $\mathcal{L}_{r+1} = \mathcal{B}(\psi(\mathcal{L}_r))$.*

Proof. See appendix C.

Theorem 6. Var *is finite iff $\mathcal{L}_0$ is finite iff for all r, $\mathcal{L}_r$ is finite.*

5.2 Observational equivalence and bisimulation

Now we use formulae of BBI and the forcing relation to distinguish between elements of relational frames. We suppose that the set of propositional variables Var is finite and we consider a fixed relational frame $(\mathcal{M}, \triangleright, \mathsf{e})$. We also have a fixed interpretation $v(X) \subseteq \mathcal{M}$ for each propositional variable X.
The valuation v is the atomic observational tool to distinguish between elements of $\mathcal{M}$.

X distinguishes the elements of $v(X)$ from the elements of $\mathcal{M} - v(X)$ and I distinguishes e from the other elements of $\mathcal{M}$. We define the *atomic observational equivalence* $\sim_0$ by $a \sim_0 b$ if $\forall F \in \mathsf{Var} \cup \{\mathsf{I}\}, a \Vdash F$ iff $b \Vdash F$. So $a \sim_0 b$ holds when no atomic observation can distinguish a from b.
Now we generalize the observational equivalence to a subset $\mathcal{K}$ of $\mathcal{L}$. We define $\sim_{\mathcal{K}}$, the *observational equivalence under* $\mathcal{K}$ by: $\quad a \sim_{\mathcal{K}} b \;$ iff $\; \forall F \in \mathcal{K}, a \Vdash F$ iff $b \Vdash F$.
Then a and b are observationally equivalent under $\mathcal{K}$ when they cannot be distinguished from each other using forcing and formulae of $\mathcal{K}$. Then they are neither distinguishable by any boolean combination of formulae of $\mathcal{K}$.

Proposition 13. $\sim_{\mathcal{K}} = \sim_{\mathcal{B}(\mathcal{K})}$.

Now we suppose that $\mathcal{K}$ is a finite subset of $\mathcal{L}$. Given a in $\mathcal{M}$, we define the subset $\mathcal{K}_a$ of $\mathcal{K}$ by $\mathcal{K}_a = \{F \in \mathcal{K} \mid a \Vdash F\}$. $\overline{\mathcal{K}_a}$ is a formula which characterizes the $\sim_{\mathcal{K}}$-class of a.

Proposition 14. *For any $a, b \in \mathcal{M}$, $a \sim_{\mathcal{K}} b$ if and only if $b \Vdash \overline{\mathcal{K}_a}$.*

Definition 6. *We define $\sim_\omega$, the* observational equivalence *by $\sim_\omega = \sim_{\mathcal{L}}$ and the* observational equivalence up to rank r *by $\sim_r = \sim_{\mathcal{L}_r}$.*

This definition is coherent with the previous definition of $\sim_0$ because of $\mathcal{L}_0 = \mathcal{B}(\mathsf{Var} \cup \{\mathsf{I}\})$ and Proposition 13: the atomic observational equivalence coincides with the observational equivalence up to rank 0. We now generalize this identity for rank r. We recall the notion of bisimulation. We define an increasing operator $\mathcal{F} : \mathcal{P}(\mathcal{M}^2) \longrightarrow \mathcal{P}(\mathcal{M}^2)$ on the set of binary relation over $\mathcal{M}$. Let $R \in \mathcal{P}(\mathcal{M}^2)$ be a binary relation on $\mathcal{M}$. Then $\mathcal{F}(R)$ is the binary relation on $\mathcal{M}$ characterized by:

$$m \; \mathcal{F}(R) \; m' \quad \text{iff} \quad \begin{cases} \forall a, b \triangleright m, \; \exists a', b' \triangleright m', \; a \, R \, a' \text{ and } b \, R \, b' \\ \forall a', b' \triangleright m', \; \exists a, b \triangleright m, \; a \, R \, a' \text{ and } b \, R \, b' \\ \forall m, a \triangleright b, \; \exists m', a' \triangleright b', \; a \, R \, a' \text{ and } b \, R \, b' \\ \forall m', a' \triangleright b', \; \exists m, a \triangleright b, \; a \, R \, a' \text{ and } b \, R \, b' \end{cases}$$

With this definition, we could check that the full relation $\mathcal{M}^2$ is a fixpoint of $\mathcal{F}$, i.e. $\mathcal{F}(\mathcal{M}^2) = \mathcal{M}^2$. In order to obtain the bisimulation, we combine $\mathcal{F}$ with an atomic distinction feature using the $\sim_0$ atomic observational equivalence.

Definition 7. *The* bisimulation equivalence $\sim$ *is the greatest fixpoint of the increasing function $\mathcal{F}_0$ where $\mathcal{F}_0(R) = \mathcal{F}(R) \cap \sim_0$.*

As noted by Milner [10], $\sim$ could be obtained either by the union of all bisimulations (i.e. binary relations satisfying $R \subseteq \mathcal{F}_0(R)$) or as the limit of the decreasing *transfinite* sequence $\bigcap_\lambda \mathcal{F}_0^\lambda(\mathcal{M}^2)$, λ ranges over the class of *ordinals*.

5.3 The observational power of BBI

The function $\mathcal{F}$ operates on binary relations and thus on observational equivalences $\sim_{\mathcal{K}}$. The next result shows when $\mathcal{K}$ is finite, the behavior of $\mathcal{F}$ on $\sim_{\mathcal{K}}$ can be represented by a finitary transformation on the set $\mathcal{K}$.

Lemma 3. *For any finite subset $\mathcal{K}$ of $\mathcal{L}$, $\mathcal{F}(\sim_{\mathcal{K}}) = \sim_{\psi(\mathcal{K})}$.*

Proof. See appendix D.

Theorem 7. *For any rank r, $\mathcal{F}(\sim_r) = \sim_{r+1}$ and $\sim_r = \mathcal{F}^r(\sim_0)$.*

Proof. Using Propositions 12, 13 and Lemma 3 we derive $\mathcal{F}(\sim_r) = \mathcal{F}(\sim_{\mathcal{L}_r}) = \sim_{\psi(\mathcal{L}_r)} = \sim_{\mathcal{B}(\psi(\mathcal{L}_r))} = \sim_{\mathcal{L}_{r+1}} = \sim_{r+1}$. Then by induction on r, we prove $\sim_r = \mathcal{F}^r(\sim_0)$.

Corollary 3. *Observational equivalence is the ω-limit of the decreasing sequence*

$$\mathcal{M}^2 \supseteq \mathcal{F}_0(\mathcal{M}^2) \supseteq \mathcal{F}_0^2(\mathcal{M}^2) \supseteq \cdots \supseteq \bigcap_{r<\omega} \mathcal{F}_0^r(\mathcal{M}^2) = \sim_\omega \supseteq \cdots \supseteq \bigcap_{\lambda} \mathcal{F}_0^\lambda(\mathcal{M}^2) = \sim$$

Proof. We prove $\mathcal{F}_0^{r+1}(\mathcal{M}^2) = \sim_r$ by induction on r once having noticed that $\mathcal{F}_0(\mathcal{M}^2) = \sim_0$. Then, any pre-fixpoint of $\mathcal{F}_0$ (i.e. any bisimulation, including $\sim$) is smaller than any element of the transfinite decreasing sequence $\mathcal{F}_0^\lambda(\mathcal{M}^2)$, and in particular when $\lambda = \omega$.

Observational equivalence $\sim_\omega$ is *not necessarily equal* to bisimulation equivalence $\sim$ because iterations up to ordinals λ greater than ω could be necessary to reach the greatest fixpoint $\bigcap_\lambda \mathcal{F}_0^\lambda(\mathcal{M}^2)$. As Milner noticed [10], one should use infinitary logics to make infinite observations. In this context, our results can be related to a recent study on resources and processes based on BBI [14] and provide a characterization of the observational power of BBI. Though in general $\sim$ is not equal to $\sim_\omega$, it is interesting to study under which further conditions the identity $\sim = \sim_\omega$ holds. For example, it holds when $\mathcal{M}$ is finite or when the relation $\triangleright$ is *locally finite* or more generally, when the model has the *Hennessy-Milner property*. The results obtained in the context of modal logic [1] could be adapted to BBI. To obtain the identity $\sim = \sim_\omega$ is an important goal: it provides a constructive tool to show equivalence (through a bisimulation) and also a constructive tool to distinguish (through a distinguishing formula).

References

1. P. Blackburn, M. de Rijke, and Y. Venema. *Modal logic*. Cambridge University Press, New York, NY, USA, 2001.
2. L. Caires and L. Cardelli. A Spatial Logic for Concurrency (part II). In *Int. Conf. on Concurrency Theory, CONCUR 2002, LNCS 2421*, pages 209–225, 2002.
3. L. Caires and E. Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. In *CONCUR 2004, LNCS 3170*, pages 240–257, 2004.
4. B. Davey and H. Priestley. *Introduction to Lattices and Order*. Cambridge Mathematical Textbooks. Cambridge University Press, 1990.
5. A. Dawar, P. Gardner, and G. Ghelli. Adjunct Elimination through Games in Static Ambient Logic. In *FSTTCS 2004, LNCS 3328*, pages 211–223, 2004.
6. D. Galmiche and D. Méry. Semantic labelled tableaux for propositional BI without bottom. *Journal of Logic and Computation*, 13(5):707–753, 2003.
7. D. Galmiche and D. Méry. Characterizing provability in BI's pointer logic through resource graphs. In *LPAR 2005, LNAI 3835*, pages 459–473, Montego Bay, Jamaica, December 2005.
8. D. Galmiche, D. Méry, and D.Pym. The semantics of BI and Resource Tableaux. *Math. Struct. in Comp. Science*, 15(6):1033–1088, 2005.

9. S. Ishtiaq and P. O'Hearn. BI as an assertion language for mutable data structures. In *28th ACM Symposium on Principles of Programming Languages, POPL 2001*, pages 14–26, London, UK, 2001.
10. R. Milner. *Communication and Concurrency*. International series in computer science. Prentice Hall, 1989.
11. P. O'Hearn and D. Pym. The Logic of Bunched Implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.
12. P. O'Hearn, J. Reynolds, and H. Yang. Local reasoning about programs that alter data structures. In *15th Int. Workshop on Computer Science Logic, CSL 2001, LNCS 2142*, pages 1–19, Paris, France, 2001.
13. D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002.
14. D. Pym and C. Tofts. A calculus and logic of resources and processes. Technical Report HPL-2004-170, HP Labs, 2004.
15. J. Reynolds. Separation logic: A logic for shared mutable data structures. In *IEEE Symposium on Logic in Computer Science*, pages 55–74, Copenhagen, July 2002.
16. R. Statman. Intuitionistic Propositional Logic is Polynomial-Space Complete. *Theoretical Computer Science*, 9:67–72, 1979.
17. H. Yang. Ternary-relation Models of Boolean BI: Soundness and Completeness. Unpublished note, 2004.

A Proofs of Propositions 4,5,6

Proposition 4. *Let I_p, I'_p be two units and F_p be a prime filter, we have*
1. I_p is a unit of I_p;
2. $0 \notin I_p \bullet I'_p$ if and only if $I_p = I'_p$;
3. $0 \notin I_p \bullet F_p$ if and only if I_p is a unit of F_p.

Proof. We give a proof of item 3. Suppose $0 \notin I_p \bullet F_p$. By Corollary 1, there exists a prime filter H_p s.t. $0 \notin H_p$ and $I_p \bullet F_p \subseteq H_p$. But then, $F_p \subseteq I_p \bullet F_p \subseteq H_p$ holds and thus by Proposition 3, $F_p = H_p$ holds. So $I_p \bullet F_p \subseteq F_p$ and I_p is a unit of F_p. For the converse, suppose $0 \in I_p \bullet F_p$. It is impossible that $I_p \bullet F_p \subseteq F_p$ (otherwise $0 \in F_p$ would hold and F_p would not be proper).

Proposition 5. *Every prime filter has a unique unit.*

Proof. Let $F_p \in \mathbb{F}_p$. The identity $\uparrow\mathsf{i} \bullet F_p = F_p$ holds. Thus by Corollary 1, there exists $I_p \in \mathbb{F}_p$ s.t. $\uparrow\mathsf{i} \subseteq I_p$ and $I_p \bullet F_p \subseteq F_p$. Thus $\mathsf{i} \in I_p$ and I_p is a unit of F_p. Let I_p and I'_p be two units of F_p. Then $I_p \bullet I'_p \bullet F_p \subseteq I_p \bullet F_p \subseteq F_p$. So if $0 \in I_p \bullet I'_p$, we would have $0 \in F_p$ which is impossible since F_p is proper. Thus $0 \notin I_p \bullet I'_p$ holds and so $I_p = I'_p$.

Proposition 6. *Let A_p, B_p and C_p be prime filters. If $A_p \bullet B_p \subseteq C_p$ holds then A_p, B_p and C_p share the same unit.*

Proof. Let I_a, I_b and I_c be the units of A_p, B_p and C_p respectively. Then $(I_a \bullet I_b) \bullet (A_p \bullet B_p) = (I_a \bullet A_p) \bullet (I_b \bullet B_p) \subseteq A_p \bullet B_p \subseteq C_p$. So if $0 \in I_a \bullet I_b$ holds, C_p would contain 0 and would not be proper. Thus $0 \notin I_a \bullet I_b$ and then $I_a = I_b$. We also have $(I_c \bullet I_a) \bullet (A_p \bullet B_p) = I_c \bullet (I_a \bullet A_p) \bullet B_p \subseteq I_c \bullet (A_p \bullet B_p) \subseteq I_c \bullet C_p \subseteq C_p$. If $0 \in I_c \bullet I_a$ holds then C_p would contain 0 and would not be proper. We deduce $I_c = I_a$.

B Proof of Lemma 2

Lemma 2. *The triple $(\mathcal{M}, \triangleright, I_p)$ is a relational frame, in which we use the previously defined forcing relation $\Vdash$. Then, for any formula A of* BBI *and any prime filter F_p of $\mathcal{M}$, $F_p \Vdash A$ iff $[A] \in F_p$.*

Proof. The fact that $(\mathcal{M}, \triangleright, I_p)$ is a relational frame can be easily deduced from the preceding results. The property $F_p \Vdash A$ iff $[A] \in F_p$ is proved by induction on the formula A. The case of classical connectives is standard. We only give the case of the $-\!\!*$ connective because it appears the most tricky to us.
First we suppose that $F_p \in \mathcal{M}$ and $F_p \Vdash A -\!\!* B$. Let $a = [A]$ and $b = [B]$. We prove that $b \in F_p \bullet \uparrow a$ by absurd. We suppose $b \notin F_p \bullet \uparrow a$. Then by Corollary 1, there exists a prime filter H_p s.t. $b \notin H_p$ and $F_p \bullet \uparrow a \subseteq H_p$. Applying this corollary again, there exists a prime filter A_p s.t. $\uparrow a \subseteq A_p$ and $F_p \bullet A_p \subseteq H_p$. Thus A_p and H_p have the same unit as F_p by Proposition 6. So A_p and H_p belong to $\mathcal{M}$ and $F_p, A_p \triangleright H_p$. Since $\uparrow a \subseteq A_p$, we have $[A] = a \in A_p$ and thus, by induction hypothesis (A being a sub-formula of $A -\!\!* B$), $A_p \Vdash A$. By definition of the forcing relation, since $F_p \Vdash A -\!\!* B$, we obtain $H_p \Vdash B$ and by induction again (B being a sub-formula of $A -\!\!* B$), we obtain $b = [B] \in H_p$. This contradicts $b \notin H_p$ found earlier. As a consequence $b \in F_p \bullet \uparrow a$. Thus there exists $k = [K] \in F_p$ s.t. $k * a \leqslant b$. This means that the formula $(K * A) \rightarrow B$ is provable and then so is $K \rightarrow (A -\!\!* B)$ by rule $[-\!\!*_2]$. Thus $k \leqslant a -\!\!* b$. Since $k \in F_p$ then $a -\!\!* b \in F_p$. We conclude $[A -\!\!* B] \in F_p$.
For the converse, we suppose $[A -\!\!* B] \in F_p$. Then $a -\!\!* b \in F_p$. We prove that $F_p \Vdash A -\!\!* B$. Let A_p and B_p be two prime filters of $\mathcal{M}$ s.t. $F_p, A_p \triangleright B_p$ and $A_p \Vdash A$. Then by induction $a \in A_p$ and therefore $(a -\!\!* b) * a \in F_p \bullet A_p \subseteq B_p$. Moreover, since $((A -\!\!* B) * A) \rightarrow B$ is provable, we obtain $(a -\!\!* b) * a \leqslant b$ and thus $[B] = b \in B_p$. Thus by induction we have $B_p \Vdash B$.

C Proof of Proposition 12

Proposition 12. *If $\mathcal{L}_r$ is finite then $\mathcal{L}_{r+1} = \mathcal{B}(\psi(\mathcal{L}_r))$.*

Proof. Since $\psi(\mathcal{L}_r) \subseteq \mathcal{L}_{r+1}$ holds, it is clear that $\mathcal{B}(\psi(\mathcal{L}_r)) \subseteq \mathcal{L}_{r+1}$ holds. For the converse, we suppose that there exists at least one formula of rank less than $r+1$ which is not an element of $\mathcal{B}(\psi(\mathcal{L}_r))$. Among all such formulae, we choose a formula F with minimal size. Clearly, the principal connective of F is not classical, otherwise F would not be minimal. Indeed suppose for example $F \equiv \neg A$. Then A has rank less than $r+1$ so it belongs to $\mathcal{L}_{r+1}$. Since F has minimal size, A must belong to $\mathcal{B}(\psi(\mathcal{L}_r))$. Thus $\neg A = F$ also belongs to $\mathcal{B}(\psi(\mathcal{L}_r))$ which is absurd. F is not atomic either.[7] Then the principal connective of F is either $*$ or $-\!\!*$.
Let us consider the case $F \equiv A * B$. Since $\mathsf{rank}(F) \leqslant r+1$, then $\mathsf{rank}(A) \leqslant r$ and $\mathsf{rank}(B) \leqslant r$. Then $A, B \in \mathcal{L}_r$. We have $A = \bigvee\{\overline{\Gamma} \mid A \in \Gamma \text{ and } \Gamma \in \mathcal{P}(\mathcal{L}_r)\}$ and by Proposition 10 $B = \bigvee\{\overline{\Delta} \mid B \in \Delta \text{ and } \Delta \in \mathcal{P}(\mathcal{L}_r)\}$. We deduce $A * B = \bigvee\{\overline{\Gamma} * \overline{\Delta} \mid A \in \Gamma, B \in \Delta \text{ and } \Gamma, \Delta \in \mathcal{P}(\mathcal{L}_r)\}$. Thus $F = A * B \in \mathcal{B}(\psi(\mathcal{L}_r))$ which is absurd again.

[7] because $\mathcal{L}_0 \subseteq \mathcal{L}_r \subseteq \mathcal{B}(\psi(\mathcal{L}_r))$ holds by Proposition 11 and $\mathsf{I} \in \mathcal{L}_0$.

The last case is $F \equiv A \twoheadrightarrow\!\!\!* B$. We obtain $A = \bigvee\{\overline{\Gamma} \mid A \in \Gamma \text{ and } \Gamma \in \mathcal{P}(\mathcal{L}_r)\}$ and $\neg B = \bigvee\{\overline{\Delta} \mid \neg B \in \Delta \text{ and } \Delta \in \mathcal{P}(\mathcal{L}_r)\}$. Thus $B = \bigwedge\{\neg\overline{\Delta} \mid \neg B \in \Delta \text{ and } \Delta \in \mathcal{P}(\mathcal{L}_r)\}$. So $A \twoheadrightarrow\!\!\!* B = \bigwedge\{\overline{\Gamma} \twoheadrightarrow\!\!\!* \neg\overline{\Delta} \mid A \in \Gamma, \neg B \in \Delta \text{ and } \Gamma, \Delta \in \mathcal{P}(\mathcal{L}_r)\}$. Then $F = A \twoheadrightarrow\!\!\!* B = \neg \bigvee\{\neg(\overline{\Gamma} \twoheadrightarrow\!\!\!* \neg\overline{\Delta}) \mid A \in \Gamma, \neg B \in \Delta \text{ and } \Gamma, \Delta \in \mathcal{P}(\mathcal{L}_r)\}$ and $F \in \mathcal{B}(\psi(\mathcal{L}_r))$ which again is absurd.

D Proof of Lemma 3

Lemma 3. *For any finite subset $\mathcal{K}$ of $\mathcal{L}$, $\mathcal{F}(\sim_{\mathcal{K}}) = \sim_{\psi(\mathcal{K})}$.*

Proof. First we prove $\mathcal{F}(\sim_{\mathcal{K}}) \subseteq \sim_{\psi(\mathcal{K})}$. We suppose $m\ \mathcal{F}(\sim_{\mathcal{K}})\ m'$ and prove $m \sim_{\psi(\mathcal{K})} m'$. Let $F \in \psi(\mathcal{K})$, we consider the case $F \equiv \overline{\Gamma} * \overline{\Delta}$ for $\Gamma, \Delta \in \mathcal{P}(\mathcal{K})$. We aim to prove $m \Vdash \overline{\Gamma} * \overline{\Delta}$ iff $m' \Vdash \overline{\Gamma} * \overline{\Delta}$. We suppose $m \Vdash \overline{\Gamma} * \overline{\Delta}$ holds. Then there exist a, b s.t. $a, b \triangleright m$ and $a \Vdash \overline{\Gamma}$ and $b \Vdash \overline{\Delta}$. Since $m\ \mathcal{F}(\sim_{\mathcal{K}})\ m'$, there exist a', b' s.t. $a', b' \triangleright m'$ and $a \sim_{\mathcal{K}} a'$ and $b \sim_{\mathcal{K}} b'$. Then by Proposition 13, $a \sim_{\mathcal{B}(\mathcal{K})} a'$ and $b \sim_{\mathcal{B}(\mathcal{K})} b'$ and since $\overline{\Gamma}, \overline{\Delta} \in \mathcal{B}(\mathcal{K})$, we deduce $a' \Vdash \overline{\Gamma}$ and $b' \Vdash \overline{\Delta}$. Combining with $a', b' \triangleright m'$, we obtain $m' \Vdash \overline{\Gamma} * \overline{\Delta}$. For the converse ($m' \Vdash \overline{\Gamma} * \overline{\Delta}$ implies $m \Vdash \overline{\Gamma} * \overline{\Delta}$,) a similar proof can be given. Now the case $F \equiv \neg(\overline{\Gamma} \twoheadrightarrow\!\!\!* \neg\overline{\Delta})$ can be treated by similar arguments. So for any $F \in \psi(\mathcal{K})$, $m \Vdash F$ iff $m' \Vdash F$ holds. We can conclude $m \sim_{\psi(\mathcal{K})} m'$.
We now prove $\sim_{\psi(\mathcal{K})} \subseteq \mathcal{F}(\sim_{\mathcal{K}})$. We suppose $m \sim_{\psi(\mathcal{K})} m'$ and prove $m\ \mathcal{F}(\sim_{\mathcal{K}})\ m'$. We consider for example the third condition of the definition of $\mathcal{F}$. Let a, b be s.t. $m, a \triangleright b$. We have $a \Vdash \overline{\mathcal{K}_a}$ and $b \Vdash \overline{\mathcal{K}_b}$. Then $m \Vdash \neg(\overline{\mathcal{K}_a} \twoheadrightarrow\!\!\!* \neg\overline{\mathcal{K}_b})$. But since $\mathcal{K}_a, \mathcal{K}_b \in \mathcal{P}(\mathcal{K})$, we deduce $\neg(\overline{\mathcal{K}_a} \twoheadrightarrow\!\!\!* \neg\overline{\mathcal{K}_b}) \in \psi(\mathcal{K})$. Thus, since $m \sim_{\psi(\mathcal{K})} m'$, we obtain $m' \Vdash \neg(\overline{\mathcal{K}_a} \twoheadrightarrow\!\!\!* \neg\overline{\mathcal{K}_b})$. There exist a', b' s.t. $m', a' \triangleright b'$, $a' \Vdash \overline{\mathcal{K}_a}$ and $b' \Vdash \overline{\mathcal{K}_b}$. Then by Proposition 14, we deduce $a \sim_{\mathcal{K}} a'$ and $b \sim_{\mathcal{K}} b'$. Thus we have $\forall m, a \triangleright b, \exists m', a' \triangleright b',\ a \sim_{\mathcal{K}} a'$ and $b \sim_{\mathcal{K}} b'$. The three other conditions of the definition of $\mathcal{F}$ are proved using similar arguments. Thus we can conclude that $m\ \mathcal{F}(\sim_{\mathcal{K}})\ m'$.