Looking at Separation Algebras with Boolean BI-eyes

Dominique Larchey-Wendling, Didier Galmiche

Looking at Separation Algebras with Boolean BI-eyes*

Dominique Larchey-Wendling[1] and Didier Galmiche[2]

[1] LORIA – CNRS, Nancy, France
dominique.larchey-wendling@loria.fr
[2] LORIA – Université de Lorraine, Nancy, France
didier.galmiche@loria.fr

Abstract. In this paper, we show that the formulæ of Boolean BI cannot distinguish between some of the different notions of separation algebra found in the literature: partial commutative monoids, either cancellative or not, with a single unit or not, all define the same notion of validity. We obtain this result by the careful study of the specific properties of the counter-models that are generated by tableaux proof-search in Boolean BI.

1 Introduction

Separation logic [18] is a well established logical formalism for reasoning about heaps of memory and programs that manipulate them. The purely propositional part of the logic is usually given by Boolean BI (also denoted BBI) which is a particular *bunched logic* obtained by freely combining the Boolean connectives of classical propositional logic with those of multiplicative intuitionistic linear logic [11]. Provability in BBI is defined by a Hilbert system [17] and corresponds to validity in the class of non-deterministic (or relational) monoids [8]. Restricting that class to e.g. partial monoids gives another notion of validity [14] for which the Hilbert system is not complete anymore.

Separation logic is defined by a particular kind of partial monoids built for instance from memory heaps that are composed by disjoint union; see [3,13,15] for a survey of the different models either abstract or concrete that are usually considered in the literature. These models verify some additional properties that may be invalid in non-deterministic models or even in partial monoidal models. Some of these properties are the foundation of *separation algebras* [5,6,7]. For instance, the existence of *multiple units* for the composition of heaps, or the property that the composition of heaps is a *cancellative* operation, the main focus of this paper. This last property does not hold in an arbitrary partial monoid.

Let us discuss some motivations behind the study of these specific properties of separation algebras. Abstract separation logics and variants of BBI are usually undecidable [3,2,14,15]. But still, being able to prove statements expressed in BBI is required in the framework of Hoare logic. Hence the idea is to try narrowing down the logic and the separation model through the logical

* Work partially supported by the ANR grant DynRes (project No. ANR-11-BS02-011).

or proof-theoretical representations of the specific properties of separation algebras. We notice the lively interest in proof-search for relational BBI [1,10,16], partial monoidal BBI [12,13] and propositional abstract separation logic [9].

In [4], Brotherston and Villard show that cancellativity cannot be axiomatized within BBI: no formula of BBI is able to distinguish cancellative from non-cancellative monoids. Let us note that even though an axiomatization is proposed in some hybrid extension of BBI [4], proof-search in such extensions of BBI is a largely unexplored track of research. In the current paper, we show the stronger result that any BBI formula that is valid in partial and cancellative models is also valid in any partial model: validity of BBI formulæ is the very same predicate if you add cancellativity as a requirement for your models.

In [9], Hóu *et al.* present a labelled sequent calculus for proof-search in *propositional abstract separation logic* extending their work on relational BBI [10] by introducing model specific proof-rules, in particular one for partiality and one for cancellativity. A noticeable consequence of our result is that their rule for cancellativity is redundant when searching for proofs of BBI-formulæ: one may find shorter proofs using that rule but it does not reinforce provability. As another consequence, extending the older labelled tableaux calculus for partial monoidal BBI of Larchey-Wendling and Galmiche [13] to cover cancellativity is trivial: simply do nothing. The difficulty does not lie in the extension of the system but in the proof of the redundancy of cancellativity.

The results obtained in this paper emphasize the importance of the *strong completeness theorem* for partial monoidal BBI [12] from which they derive. The counter-models generated by the labelled tableaux proof-search calculus contain information about the logic itself that, when carefully extracted, can be used to obtain completeness for additional properties of abstract models.

Let us give an overview of the paper. In Section 2, we recall the syntax and Kripke semantics of Boolean BI and we present *non-deterministic monoids* which are the models of BBI, and some sub-classes of monoids related to separation algebras and abstract separation logic models, e.g. cancellative monoids. In Section 3, we study the links between *single unit* and *multi-unit monoids* and give a quick semantic overview of why they are equivalent w.r.t. BBI validity. In Section 4, we define the notion of *partial monoidal equivalence* (or PME for short) to syntactically represent partial monoids with a single unit. We define basic and simple PMEs which are the monoids that are generated by labelled tableaux proof-search [12]. In Section 5, we use the strong completeness result for simple PMEs to derive an equivalence theorem for some separation algebras. It is based on our core result: *basic/simple* PME*s are cancellative and have invertible squares*. We discuss the proof of this result in the following sections. In Section 6, we introduce the notion of invertibility in the context of PMEs. In Section 7, we argue that even though basic PMEs are defined inductively, it is not possible to give a direct inductive proof of cancellativity or of the invertibility of squares for basic PMEs. In Section 8, we show that basic PMEs can be transformed into primary PMEs and that primary PMEs are cancellative with invertible squares. *Omitted proofs can be found in the appendices.*

2 Boolean BI and its non-deterministic Kripke semantics

In this section, we introduce a "compact" syntax for BBI: conjunction $\wedge$ and negation $\neg$ are the only Boolean connectives.[3] Then, we present the Kripke semantics of BBI based on the notion of non-deterministic monoid.

Definition 1. *The* formulæ of BBI *are freely built using logical variables in* Var*, the logical constant* $\mathbb{I}$*, the unary connective* $\neg$ *or binary connectives in* $\{*, -\!\!*, \wedge\}$*. The formal grammar is* $F ::= v \mid \mathbb{I} \mid \neg F \mid F \wedge F \mid F * F \mid F -\!\!* F$ *with* $v \in \mathsf{Var}$*.*

We introduce the semantic foundations of BBI. Let us consider a set M.[4] We denote by $\mathcal{P}(M)$ the power-set of M, i.e. its set of subsets. A binary function $\circ : M \times M \longrightarrow \mathcal{P}(M)$ is naturally extended to a binary operator on $\mathcal{P}(M)$ by $X \circ Y = \bigcup\{x \circ y \mid x \in X, y \in Y\}$ for any subsets X, Y of M. Using this extension, we can view an element m of M as the singleton set $\{m\}$ and derive equations like $m \circ X = \{m\} \circ X$, $a \circ b = \{a\} \circ \{b\}$ or $\emptyset \circ X = \emptyset$.

Definition 2. *A* non-deterministic monoid *(*ND*-monoid for short) is a triple* $\mathfrak{M} = (M, \circ, U)$ *where* $U \subseteq M$ *is the* set of units *and* $\circ : M \times M \longrightarrow \mathcal{P}(M)$ *is a* composition *for which the axioms of* (neutrality) $\forall x \in M\ x \circ U = \{x\}$, (commutativity) $\forall x, y \in M\ x \circ y = y \circ x$*, and* (associativity)[5] $\forall x, y, z \in M\ (x \circ y) \circ z = x \circ (y \circ z)$ *hold.*

The extension of $\circ$ to $\mathcal{P}(M)$ thus induces a (usual) commutative monoidal structure with unit U on $\mathcal{P}(M)$. The term *non-deterministic* was introduced in [8] 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 $a \circ b = \emptyset$. Notice that $\mathfrak{M}$ is called a BBI-*model* in [4].

Given $\mathfrak{M} = (M, \circ, U)$ and an interpretation $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(M)$ of variables, we define the Kripke forcing relation by induction on the structure of formulæ:

$$\mathfrak{M}, x \Vdash_\delta v \text{ iff } x \in \delta(v) \qquad \mathfrak{M}, x \Vdash_\delta \mathbb{I} \text{ iff } x \in U \qquad \mathfrak{M}, x \Vdash_\delta \neg A \text{ iff } \mathfrak{M}, x \nVdash_\delta A$$
$$\mathfrak{M}, x \Vdash_\delta A \wedge B \text{ iff } \mathfrak{M}, x \Vdash_\delta A \text{ and } \mathfrak{M}, x \Vdash_\delta B$$
$$\mathfrak{M}, x \Vdash_\delta A * B \text{ iff } \exists a, b,\ x \in a \circ b \text{ and } \mathfrak{M}, a \Vdash_\delta A \text{ and } \mathfrak{M}, b \Vdash_\delta B$$
$$\mathfrak{M}, x \Vdash_\delta A -\!\!* B \text{ iff } \forall a, b,\ (b \in x \circ a \text{ and } \mathfrak{M}, a \Vdash_\delta A) \Rightarrow \mathfrak{M}, b \Vdash_\delta B$$

Definition 3 (BBI-validity, counter-models). *A formula* F *of* BBI *is* valid in $\mathfrak{M} = (M, \circ, U)$ *if for any interpretation* $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(M)$ *the relation* $\mathfrak{M}, m \Vdash_\delta F$ *holds for any* $m \in M$*. A* counter-model *of the formula* F *is given by a* ND*-monoid* $\mathfrak{M}$*, an interpretation* $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(M)$*, and an element* $m \in M$ *such that* $\mathfrak{M}, m \nVdash_\delta F$*.*

In some papers, you might find BBI defined by non-deterministic monoidal Kripke semantics [1,4,8,10], in other papers it is defined by partial deterministic monoidal Kripke semantics [12,13] and generally separation logic models are particular instances of partial (deterministic) monoids [3,4,9]. See [13] for a general discussion about these issues.

---

[3] The other Boolean connectives can be obtained by De Morgan's laws.

[4] The case $M = \emptyset$ is *allowed* but arguably not very interesting in the case of BBI.

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

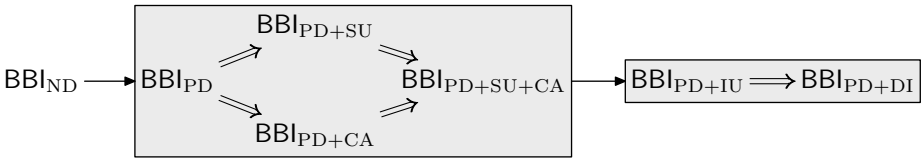

Fig. 1. Inclusions between BBI-validity in some sub-classes of ND-monoids.

Definition 4. *For any* ND*-monoid* $(M, \circ, U)$*, we name some properties as follows:*

(PD)	*Partial deterministic*	$\forall x, y, a, b \ \{x, y\} \subseteq a \circ b \Rightarrow x = y$
(SU)	*Single unit*	$\exists u \ U = \{u\}$
(CA)	*Cancellativity*	$\forall k, a, b \ (k \circ a) \cap (k \circ b) \neq \emptyset \Rightarrow a = b$
(IU)	*Indivisible units*	$\forall x, y \ x \circ y \cap U \neq \emptyset \Rightarrow x \in U$
(DI)	*Disjointness*	$\forall x \ x \circ x \neq \emptyset \Rightarrow x \in U$

These properties allow us to consider sub-classes of the full class of ND-monoids. Other properties like *divisibility* or *cross-split* are considered as well in [4] but in this paper, we focus on the properties of Definition 4.

We denote by ND the full class of non-deterministic monoids. We identify the property X with the sub-class $X \subseteq \mathrm{ND}$ of monoids which satisfy property X. If X and Y are two properties, we read $X + Y$ as the sub-class of monoids of ND that satisfy the *conjunction of* X *and* Y. This is the meaning of the equation $X + Y = X \cap Y$ which might look strange at first. As an example, $\mathrm{PD} + \mathrm{SU} + \mathrm{CA} + \mathrm{IU}$ is both the conjunction of those four properties and the sub-class of cancellative partial deterministic monoids with a single and indivisible unit.

Proposition 1. *The two strict inclusions* $\mathrm{DI} \subsetneq \mathrm{IU}$ *and* $\mathrm{PD} + \mathrm{DI} \subsetneq \mathrm{PD} + \mathrm{IU}$ *hold.*

The sub-class HM of *heap monoids* verifies all the properties of Definition 4. However, it is not defined by a property but it is described by the concrete models of Separation Logic [15].

Various notions of *separation algebra* can be found in the literature: for instance the "original" notion of separation algebra is defined in [5] as the elements of the sub-class $\mathrm{PD} + \mathrm{SU} + \mathrm{CA}$; in the "views" framework of [6], a separation algebra is an element of sub-class PD; while it is of sub-class $\mathrm{PD} + \mathrm{CA}$ in [7]. To finish, in [13], though not called separation algebra, a BBI-model is an element of sub-class $\mathrm{PD} + \mathrm{SU}$.

In general the sub-classes of ND define different notions of validity on the formulæ of BBI [14]. However, it was proved recently that theses properties are not axiomatizable in BBI [4], *with the exception of* IU.[6] We define a notation to express the relations between those potentially different notions of validity.

Definition 5 (BBI_X). *For any sub-class* $X \subseteq \mathrm{ND}$*, we denote by* BBI_X *the set of formulæ of* BBI *which are valid in any* ND*-monoid of the sub-class* X*.*

[6] In [4], $\mathbb{I} \to (A * B) \to A$ is used as a BBI-axiom for IU but we favor $\neg(\mathbb{I} \wedge (\neg\mathbb{I} * \neg\mathbb{I}))$.

Obviously, if the inclusion $X \subseteq Y$ holds between the sub-classes X and Y of ND-monoids then inclusion $\mathsf{BBI}_Y \subseteq \mathsf{BBI}_X$ holds between the sets of valid formulæ. The sets BBI_X are usually not recursive (at least for the sub-classes we consider here) because of the undecidability of BBI [3,2,14,15]. The identity $\mathsf{BBI}_X = \mathsf{BBI}_Y$ implies for instance that a semi-decision algorithm for validity (of formulæ) in sub-class X can be replaced by some semi-decision algorithm for validity in sub-class Y. It also "suggests" that there might exist some kind of relation (like a map [4] or a bisimulation [15]) between the models of sub-class X and those of sub-class Y.[7]

To the best of our knowledge, the graph of Figure 1 summarizes what was known about the inclusion relations between the formulæ valid in the previously mentioned sub-classes of ND-monoids, the single arrow $\rightarrow$ representing strict inclusion, the double arrow $\Rightarrow$ representing non-strict inclusion. In fact, besides trivial inclusion results derived from the obvious inclusions of sub-classes of monoids, not very much was known except the strict inclusion $\mathsf{BBI}_{\mathrm{ND}} \subsetneq \mathsf{BBI}_{\mathrm{PD}}$ proved[8] in [14] and the strict inclusions $\mathsf{BBI}_{\mathrm{ND}} \subsetneq \mathsf{BBI}_{\mathrm{IU}}$ and $\mathsf{BBI}_{\mathrm{PD}} \subsetneq \mathsf{BBI}_{\mathrm{PD+IU}}$ which are trivial consequences of the stronger result that IU can be axiomatized in BBI. Beware that PD *cannot* be axiomatized in BBI [4].

The left gray box in Figure 1 is the main motivation behind the current paper. It contains the four different definitions of separation algebras mentioned earlier: PD, PD + SU, PD + CA and PD + SU + CA. In this paper, we show that these four sub-classes of ND-monoids define the same set of valid formulæ, i.e. the double arrows are in fact identities. To obtain these results, we first give a simple proof that $\mathsf{BBI}_{\mathrm{PD+SU}} \subseteq \mathsf{BBI}_{\mathrm{PD}}$ in Section 3, and then a much more involved proof that $\mathsf{BBI}_{\mathrm{PD+SU+CA}} \subseteq \mathsf{BBI}_{\mathrm{PD+SU}}$ in the latest sections of the paper. This proof is based on a careful study of the properties of the counter-models generated by proof-search, which are complete for $\mathsf{BBI}_{\mathrm{PD+SU}}$ [12].

The right gray box in Figure 1 is a secondary focus of our paper. We prove the identities $\mathsf{BBI}_{\mathrm{PD+IU}} = \mathsf{BBI}_{\mathrm{PD+DI}} = \mathsf{BBI}_{\mathrm{PD+SU+CA+IU+DI}}$ by exploiting the fact that the counter-models generated by proof-search which satisfy property IU also satisfy property DI.

3 Single units in non-deterministic monoids

We give a quick overview of the relations between the multi-unit semantics and the single unit semantics. We recall that they define the same notion of validity for BBI and we give a model-theoretic account of this equivalence. Soundness/completeness for the single unit semantics w.r.t. the Hilbert proof system for BBI were already established in [8].[9]

Definition 6 (The unit of x). *Let $(M, \circ, U)$ be a* ND*-monoid. For any $x \in M$, there exists a unique $u_x \in U$ such that $x \circ u_x = \{x\}$. It is called* the unit of x.

[7] relation from which a constructive proof of $\mathsf{BBI}_X = \mathsf{BBI}_Y$ could be derived.

[8] In fact only $\mathsf{BBI}_{\mathrm{SU}} \subsetneq \mathsf{BBI}_{\mathrm{PD+SU}}$ is proved in [14] but the *same argument* will do.

[9] The *same proof* works for the more general multi-unit semantics, as assumed for instance in Theorem 2.5 of [4]. Hence the identity $\mathsf{BBI}_{\mathrm{ND}} = \mathsf{BBI}_{\mathrm{SU}}$ was known since [8].

Definition 7 (Slice monoid at x). *Let $\mathfrak{M} = (M, \circ, U)$ be a* ND*-monoid and let $x \in M$. Then the triple $\mathfrak{M}_x = (M_x, \circ', \{u_x\})$ is a* ND*-monoid of sub-class* SU *where $M_x = \{k \in M \mid u_k = u_x\}$ and $\circ'$ is the restriction of $\circ$ to M_x which is defined on $M_x \times M_x$ by $u \circ' v = u \circ v$. The triple $\mathfrak{M}_x$ is called the* slice monoid at x.

Lemma 1. *Let $\mathfrak{M} = (M, \circ, U)$ be a* ND*-monoid, $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(M)$ and $x \in M$. Let us consider $\mathfrak{M}_x$, the slice monoid at x and let $\delta' : \mathsf{Var} \longrightarrow \mathcal{P}(M_x)$ be defined by $\delta'(z) = \delta(z) \cap M_x$ for any $z \in M_x$. For any formula F of* BBI *and any $z \in M_x$, we have $\mathfrak{M}, z \Vdash_\delta F$ iff $\mathfrak{M}_x, z \Vdash_{\delta'} F$.*

Theorem 1. *If $K \subseteq$ ND is a sub-class of* ND*-monoids closed under slicing, then $\mathsf{BBI}_K = \mathsf{BBI}_{K+\mathrm{SU}}$ holds. In particular, $\mathsf{BBI}_{\mathrm{ND}} = \mathsf{BBI}_{\mathrm{SU}}$ and $\mathsf{BBI}_{\mathrm{PD}} = \mathsf{BBI}_{\mathrm{PD+SU}}$.*

Remark: the property SU cannot be axiomatized in BBI [4]. The identity $\mathsf{BBI}_{\mathrm{ND}} = \mathsf{BBI}_{\mathrm{SU}}$ gives another proof argument for this result.

4 Partial Monoidal Equivalences

We recall the framework of labels and constraints that is used to syntactically represent partial monoids of sub-class PD + SU which form the semantic basis of partial monoidal Boolean BI. The section is a short reminder of the theory developed in [13] where a labelled tableaux system is introduced and its soundness w.r.t. the sub-class PD + SU is established. Moreover, the (strong) completeness of this tableaux system is proved in [12] and this crucial (albeit non-constructive) result is restated here as Theorem 2.

4.1 Words, constraints, PMEs and the sub-class PD + SU

Let $L^\star$ be the set of *finite multisets of letters* of the alphabet L. We call the elements of $L^\star$ *words*; they do not account for the order of letters. The composition of words is denoted *multiplicatively*[10] and the *empty word* is denoted ϵ. Hence $(L^\star, \cdot, \epsilon)$ is the (usual) commutative monoid freely generated by L.

We view the alphabet L or any of its subsets $X \subseteq L$ as a subset $X \subsetneq L^\star$, i.e. we assume letters as one-letter words. We denote $x \prec y$ when x is a *sub-word* of y (i.e. $\exists k, xk = y$). If $x \prec y$, the unique k such that $xk = y$ is denoted y/x and we have $y = x(y/x)$. The *carrier alphabet* of a word m is $\mathcal{A}_m = \{\mathsf{c} \in L \mid \mathsf{c} \prec m\}$.

A *constraint* is an ordered pair of words in $L^\star \times L^\star$ denoted $m \rightharpoonup n$. A binary relation $R \subseteq L^\star \times L^\star$ between words of $L^\star$ is a set of constraints, hence $x \; R \; y$ is a shortcut for $x \rightharpoonup y \in R$. The *language* of a binary relation $R \subseteq L^\star \times L^\star$ denoted $\mathcal{L}_R$ is defined by $\mathcal{L}_R = \{x \in L^\star \mid \exists m, n \in L^\star \text{ s.t. } xm \; R \; n \text{ or } m \; R \; xn\}$. The *carrier alphabet* of R is $\mathcal{A}_R = \bigcup\{\mathcal{A}_m \cup \mathcal{A}_n \mid m \; R \; n\}$.

A word $m \in L^\star$ is said to be *defined in* R if $m \in \mathcal{L}_R$ and is *undefined in* R otherwise. A letter $\mathsf{c} \in L$ is *new to* R if $\mathsf{c} \notin \mathcal{A}_R$. The language $\mathcal{L}_R$ is downward closed w.r.t. the sub-word order $\prec$. The inclusion $\mathcal{L}_R \subseteq \mathcal{A}_R^\star$ and the identity

[10] the additive notation $+$ would conflict with the $\rightharpoonup$ sign later used for constraints.

$\mathcal{A}_R = \mathcal{L}_R \cap L$ hold. If R_1 and R_2 are two relations such that $R_1 \subseteq R_2$ then the inclusions $\mathcal{A}_{R_1} \subseteq \mathcal{A}_{R_2}$ and $\mathcal{L}_{R_1} \subseteq \mathcal{L}_{R_2}$ hold. Let us define the particular sets of constraints/relations we are interested in.

Definition 8 (PME). *A* partial monoidal equivalence *(*PME *for short) over the alphabet L is a binary relation $\sim \subseteq L^\star \times L^\star$ which is closed under the rules $\langle \epsilon, s, c, d, t \rangle$:*

$$\frac{}{\epsilon \nsim \epsilon}\ \langle\epsilon\rangle \quad \frac{x \nsim y}{y \nsim x}\ \langle s\rangle \quad \frac{ky \nsim ky \quad x \nsim y}{kx \nsim ky}\ \langle c\rangle \quad \frac{xy \nsim xy}{x \nsim x}\ \langle d\rangle \quad \frac{x \nsim y \quad y \nsim z}{x \nsim z}\ \langle t\rangle$$

Proposition 2. *Any* PME $\sim$ *is also closed under the (derived) rules $\langle p_l, p_r, e_l, e_r \rangle$:*

$$\frac{kx \nsim y}{x \nsim x}\ \langle p_l\rangle \quad \frac{x \nsim ky}{y \nsim y}\ \langle p_r\rangle \quad \frac{x \nsim y \quad yk \nsim m}{xk \nsim m}\ \langle e_l\rangle \quad \frac{x \nsim y \quad m \nsim yk}{m \nsim xk}\ \langle e_r\rangle$$

and the identities $\mathcal{L}_\sim = \{x \in L^\star \mid x \sim x\}$ and $\mathcal{A}_\sim = \{\mathsf{c} \in L \mid \mathsf{c} \sim \mathsf{c}\}$ hold.

See [13] for a proof of Proposition 2. These derived rules will be more suitable for proving properties of PMEs throughout this paper. Rule $\langle p_l \rangle$ (resp. $\langle p_r \rangle$) is a left (resp. right) projection rule. Rules $\langle e_l \rangle$ and $\langle e_r \rangle$ express the possibility to exchange related sub-words inside the PME $\sim$, either on the left or on the right.

Definition 9. *A* PME is cancellative *(resp.* has indivisible units*, resp.* has disjointness*) if it is closed under rule $\langle ca \rangle$ (resp. rule $\langle iu \rangle$, resp. rule $\langle di \rangle$).*[11]

$$\frac{kx \nsim ky}{x \nsim y}\ \langle ca\rangle \qquad \frac{\epsilon \nsim xy}{\epsilon \nsim x}\ \langle iu\rangle \qquad \frac{xx \nsim xx}{\epsilon \nsim x}\ \langle di\rangle$$

Let us see how the rules $\langle ca \rangle$, $\langle iu \rangle$ and $\langle di \rangle$ relate to sub-classes CA, IU and DI. Let $\sim$ be a PME over L. The relation $\sim$ is a partial equivalence on $L^\star$ by rules $\langle s \rangle$ and $\langle t \rangle$. The partial equivalence class of a word x is $[x] = \{y \mid x \sim y\}$. The partial quotient $L^\star/\!\sim$ is the set of non-empty classes $L^\star/\!\sim = \{[x] \mid x \sim x\}$. We define a non-deterministic composition on $L^\star/\!\sim$ by $[z] \in [x] \bullet [y]$ iff $z \sim xy$.

Proposition 3. *The triple $\mathfrak{M}_\sim = (L^\star/\!\sim, \bullet, \{[\epsilon]\})$ is a* ND*-monoid of sub-class* PD + SU*. $\mathfrak{M}_\sim$ is of sub-class* CA *(resp. sub-class* IU*, resp. sub-class* DI*) if and only if $\sim$ is closed under rule $\langle ca \rangle$ (resp. rule $\langle iu \rangle$, resp. rule $\langle di \rangle$).*

4.2 Generated PME, basic PME extensions and simple PMEs

Defined by closure under some deduction rules, the class of PMEs over an alphabet L is thus closed under arbitrary intersections. Let $\mathcal{C}$ be a set of constraints over the alphabet L. The PME *generated by* $\mathcal{C}$ is the least PME containing $\mathcal{C}$. It is either denoted by $\sim_\mathcal{C}$ or $\overline{\mathcal{C}}$ and the notations $m \sim_\mathcal{C} n$ and $m \nsim n \in \overline{\mathcal{C}}$ are synonymous. The operator $\mathcal{C} \mapsto \overline{\mathcal{C}}$ is a closure operator on sets of constraints, i.e. it is extensive ($\mathcal{C} \subseteq \overline{\mathcal{C}}$), monotonic ($\mathcal{C} \subseteq \mathcal{D}$ implies $\overline{\mathcal{C}} \subseteq \overline{\mathcal{D}}$) and idempotent ($\overline{\overline{\mathcal{C}}} \subseteq \overline{\mathcal{C}}$). The identity $\mathcal{A}_\mathcal{C} = \mathcal{A}_{\overline{\mathcal{C}}}$ holds (see [13] Proposition 3.16) but the identity $\mathcal{L}_\mathcal{C} = \mathcal{L}_{\overline{\mathcal{C}}}$ *does not hold* in general, only the inclusion $\mathcal{L}_\mathcal{C} \subseteq \mathcal{L}_{\overline{\mathcal{C}}}$ holds.

[11] Not every PME is cancellative; e.g. $\sim = \{\epsilon \nsim \epsilon, \mathsf{x} \nsim \mathsf{x}, \mathsf{y} \nsim \mathsf{y}, \mathsf{k} \nsim \mathsf{k}, \mathsf{kx} \nsim \mathsf{kx}, \mathsf{ky} \nsim \mathsf{ky}, \mathsf{kx} \nsim \mathsf{ky}, \mathsf{ky} \nsim \mathsf{kx}\}$ is a non-cancellative PME over $L = \{\mathsf{x}, \mathsf{y}, \mathsf{k}\}$.

Proposition 4 (Compactness). *Let $\mathcal{C}$ be a set of constraints over the alphabet L and $m, n \in L^\star$ be s.t. $m \sim_{\mathcal{C}} n$ holds. There exists a finite subset $\mathcal{C}_f \subseteq \mathcal{C}$ such that $m \sim_{\mathcal{C}_f} n$.*

This *compactness property* (proved in [13] Proposition 3.17) is not related to the particular nature of rules defining PMEs but solely to the fact that the rules $\langle \epsilon, s, c, d, t \rangle$ only have a *finite number of premises*.

Definition 10 (PME extension). *Let $\sim$ be a* PME *and $\mathcal{C}$ be a set of constraints, both over L. We denote by $\sim + \mathcal{C} = \overline{(\sim \cup \mathcal{C})}$ the* extension of $\sim$ *by the constraints of $\mathcal{C}$.*

The extension $\sim + \mathcal{C}$ is the least PME containing both $\sim$ and $\mathcal{C}$. Let $\sim$ be a PME and $\mathcal{C}_1$, $\mathcal{C}_2$ be two sets of constraints. The identities $(\sim + \mathcal{C}_1) + \mathcal{C}_2 = (\sim + \mathcal{C}_2) + \mathcal{C}_1 = \sim + (\mathcal{C}_1 \cup \mathcal{C}_2)$ hold. Moreover, for any $m, n \in L^\star$, the relation $m \sim n$ holds if and only if the identity $\sim + \{m \twoheadrightarrow n\} = \sim$ holds.

We single out PME extensions of the forms $\sim + \{\mathsf{ab} \twoheadrightarrow m\}$, $\sim + \{\mathsf{a}m \twoheadrightarrow \mathsf{b}\}$ or $\sim + \{\epsilon \twoheadrightarrow m\}$ where m is defined in $\sim$ and $\mathsf{a} \neq \mathsf{b}$ are two letters new to $\sim$. These extensions are generated by proof-search in the tableau method for BBI [12].

Definition 11 (Basic extension). *Given a* PME *$\sim$ over the alphabet L, a constraint is* basic w.r.t. *$\sim$ when it is of one of the three forms $\mathsf{ab} \twoheadrightarrow m$, $\mathsf{a}m \twoheadrightarrow \mathsf{b}$ or $\epsilon \twoheadrightarrow m$ with $m \sim m$ and $\mathsf{a} \neq \mathsf{b} \in L \backslash \mathcal{A}_\sim$. When $x \twoheadrightarrow y$ is basic w.r.t. $\sim$, we say that $\sim + \{x \twoheadrightarrow y\}$ is a* basic extension of the PME *$\sim$.*

Let $k \in \mathbb{N} \cup \{\infty\}$ and $(x_i \twoheadrightarrow y_i)_{i<k}$ be a sequence of constraints. Let $\mathcal{C}_p = \{x_i \twoheadrightarrow y_i \mid i < p\}$ for $p < k$. We suppose that each extension $\sim_{\mathcal{C}_p} + \{x_p \twoheadrightarrow y_p\}$ is basic for any $p < k$. If $k < \infty$ (resp. $k = \infty$) then the sequence $(x_i \twoheadrightarrow y_i)_{i<k}$ is called *basic* (resp. *simple*). The empty sequence of constraints is basic.

Definition 12. *A* basic (resp. simple) PME *is of the form $\sim_{\mathcal{C}}$ where $\mathcal{C} = \{x_i \twoheadrightarrow y_i \mid i < k\}$ and $(x_i \twoheadrightarrow y_i)_{i<k}$ is a basic (resp. simple) sequence of constraints.*

Any basic PME is simple: indeed, by rule $\langle \epsilon \rangle$ we have $\sim + \{\epsilon \twoheadrightarrow \epsilon\} = \sim$ for any PME $\sim$. Thus, using case $\epsilon \twoheadrightarrow m$ of Definition 11 with $m = \epsilon$, we can complete any basic sequence into a simple sequence by looping on $\epsilon \twoheadrightarrow \epsilon$. The converse does not hold: simple PMEs with infinite alphabets are not basic.

Remark: we point out that in the set of constraints $\mathcal{C}$, the order of appearance of constraints does not impact the closure $\sim_{\mathcal{C}}$. However, in a basic (or simple) sequence of constraints, the order is important because the newness of letters depends on the previous constraints in the sequence. Moreover, to prove that a PME is not basic, it is not sufficient to show that the sequence that defines it is not basic: maybe there exists another defining sequence which is basic.

5 Equivalence results for some Separation Algebras

In this section, we show our main result: many of the different classes of separation algebra found in the literature (see discussion of Section 2) cannot be distinguished by any formula of Boolean BI. This is a stronger result than the

impossibility to axiomatize those classes in BBI [4]. Our result relies in an essential way on the (non-constructive) strong completeness theorem for partial monoidal BBI [12].[12] "Strong" means that $\mathsf{BBI}_{\mathrm{PD+SU}}$ is complete for the specific monoids that are generated by tableaux proof-search, i.e. simple PMEs.

Theorem 2 (Strong completeness for partial monoidal BBI). *Let F be a* BBI*-formula that is invalid in some partial deterministic monoid with single unit, i.e. $F \notin \mathsf{BBI}_{\mathrm{PD+SU}}$. There exists a countable alphabet L, a simple* PME *$\sim$ over L, a valuation $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(L^\star/\!\sim)$ and a letter $\mathsf{a} \in L$ such that $\mathsf{a} \sim \mathsf{a}$ and $\mathfrak{M}_\sim, [\mathsf{a}] \not\Vdash_\delta F$.*

We will exploit the following properties of simple PMEs to derive our equivalence results for some separation algebras / abstract separation logics.

Theorem 3. *Simple* PME*s are closed under rule $\langle ca \rangle$. Simple* PME*s which are closed under rule $\langle iu \rangle$ are also closed under rule $\langle di \rangle$.*

Theorem 3 is the core result of the current paper. In Section 6, we introduce the tools used in its proof. In Section 7, we show that this proof cannot be done by direct induction on the sequence of constraints. In Section 8, we develop the argumentation using a detour via primary PMEs. The result is formally obtained as a conjunction of Corollaries 2 and 3.

Theorem 4. *The following notions of separation algebras found in the literature collapse to the same validity on* BBI *formulæ. Formally, we have the identities:*

(a) $\mathsf{BBI}_{\mathrm{PD}} = \mathsf{BBI}_{\mathrm{PD+SU}} = \mathsf{BBI}_{\mathrm{PD+CA}} = \mathsf{BBI}_{\mathrm{PD+SU+CA}}$;
(b) $\mathsf{BBI}_{\mathrm{PD+IU}} = \mathsf{BBI}_{\mathrm{PD+DI}} = \mathsf{BBI}_{\mathrm{PD+SU+CA+IU+DI}}$.

Proof. Let Q and K be the two following sub-classes $Q = \mathrm{PD} + \mathrm{SU} + \mathrm{CA}$ and $K = Q + \mathrm{IU} + \mathrm{DI}$ of ND-monoids. For (a), we prove the inclusions $\mathsf{BBI}_Q \subseteq \mathsf{BBI}_{\mathrm{PD+SU}} \subseteq \mathsf{BBI}_{\mathrm{PD}} \subseteq \mathsf{BBI}_{\mathrm{PD+CA}} \subseteq \mathsf{BBI}_Q$. We have $\mathsf{BBI}_{\mathrm{PD}} \subseteq \mathsf{BBI}_{\mathrm{PD+CA}} \subseteq \mathsf{BBI}_Q$ by sub-class inclusion in ND-monoids. By Theorem 1, we have $\mathsf{BBI}_{\mathrm{PD}} = \mathsf{BBI}_{\mathrm{PD+SU}}$. Hence, to obtain (a), it is sufficient to prove $\mathsf{BBI}_Q \subseteq \mathsf{BBI}_{\mathrm{PD+SU}}$. For (b), we show the inclusions $\mathsf{BBI}_K \subseteq \mathsf{BBI}_{\mathrm{PD+IU}} \subseteq \mathsf{BBI}_{\mathrm{PD+DI}} \subseteq \mathsf{BBI}_K$. Since we have $K \subseteq \mathrm{PD} + \mathrm{DI}$, the inclusion $\mathsf{BBI}_{\mathrm{PD+DI}} \subseteq \mathsf{BBI}_K$ is immediate. Then the inclusion $\mathsf{BBI}_{\mathrm{PD+IU}} \subseteq \mathsf{BBI}_{\mathrm{PD+DI}}$ is a direct consequence of Proposition 1. Hence, to obtain (b), it is sufficient to prove $\mathsf{BBI}_K \subseteq \mathsf{BBI}_{\mathrm{PD+IU}}$.

Let us prove the contrapositive of the inclusion $\mathsf{BBI}_Q \subseteq \mathsf{BBI}_{\mathrm{PD+SU}}$. Let us consider $F \notin \mathsf{BBI}_{\mathrm{PD+SU}}$ and let us show $F \notin \mathsf{BBI}_Q$. By Theorem 2, we obtain a simple PME $\sim$, a valuation $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(L^\star/\!\sim)$ and a letter $\mathsf{a} \in L$ such that $\mathsf{a} \sim \mathsf{a}$ and $\mathfrak{M}_\sim, [\mathsf{a}] \not\Vdash_\delta F$. By Theorem 3, the simple PME $\sim$ is closed under rule $\langle ca \rangle$ and thus, by Propositions 3, the partial quotient monoid $\mathfrak{M}_\sim$ belongs to the sub-class $\mathrm{PD} + \mathrm{SU} + \mathrm{CA}$. We deduce $F \notin \mathsf{BBI}_Q$.

Before we prove the inclusion $\mathsf{BBI}_K \subseteq \mathsf{BBI}_{\mathrm{PD+IU}}$, let us make a remark on the formula $\mathbb{U} = \neg(\neg\mathbb{I} * \neg\mathbb{I})$ and the scheme $(\mathbb{I} \wedge \mathbb{U}) \mathrel{-\!\!*} (\cdot)$. Let $\mathfrak{M} = (M, \circ, \{e\})$ be a ND-monoid of sub-class SU and let $\delta : \mathsf{Var} \longrightarrow \mathcal{P}(M)$. Then we have $\mathfrak{M}, e \Vdash_\delta \mathbb{U}$

[12] The proof in Coq is available at `http://www.loria.fr/~larchey/BBI`.

if and only if $\mathfrak{M}$ is of sub-class IU. Let F be a BBI-formula. Then for any $x \in M$, we have $\mathfrak{M}, x \nVdash_\delta (\mathbb{I} \wedge \mathbb{U}) \nrightarrow F$ if and only if $\mathfrak{M}$ is of sub-class IU and $\mathfrak{M}, x \nVdash_\delta F$.

Let us now prove the contrapositive of the inclusion $\mathsf{BBI}_K \subseteq \mathsf{BBI}_{\mathrm{PD+IU}}$. Let us consider a formula F such that $F \notin \mathsf{BBI}_{\mathrm{PD+IU}}$ and let us show $F \notin \mathsf{BBI}_K$. Let us first establish $(\mathbb{I} \wedge \mathbb{U}) \nrightarrow F \notin \mathsf{BBI}_{\mathrm{PD+SU}}$. Since the sub-class $\mathrm{PD} + \mathrm{IU}$ is closed under slicing, by Theorem 1 we have $F \notin \mathsf{BBI}_{\mathrm{PD+SU+IU}}$. Hence there exists a counter-model $\mathfrak{M}$ of F in sub-class $\mathrm{PD} + \mathrm{SU} + \mathrm{IU}$. From the previous remark on $\mathbb{U}$, we deduce that $\mathfrak{M}$ is also a counter-model of $(\mathbb{I} \wedge \mathbb{U}) \nrightarrow F$. As $\mathfrak{M}$ also belongs to sub-class $\mathrm{PD} + \mathrm{SU}$, we deduce $(\mathbb{I} \wedge \mathbb{U}) \nrightarrow F \notin \mathsf{BBI}_{\mathrm{PD+SU}}$.

We apply Theorem 2 and we obtain a counter-model of $(\mathbb{I} \wedge \mathbb{U}) \nrightarrow F$ of the form $\mathfrak{M}_\sim$ where $\sim$ is a simple PME. Since $\mathfrak{M}_\sim$ is of subclass SU, we deduce that $\mathfrak{M}_\sim$ is of subclass IU and $\mathfrak{M}_\sim$ is a counter-model of F (see previous remark on $\mathbb{U}$). Hence $\mathfrak{M}_\sim$ is of sub-class $\mathrm{PD} + \mathrm{SU} + \mathrm{IU}$. Thus by Proposition 3, $\sim$ is closed under rule $\langle iu \rangle$. Hence by Theorem 3, the simple PME $\sim$ is closed under rules $\langle ca \rangle$ and $\langle di \rangle$. By Proposition 3, $\mathfrak{M}_\sim$ is a counter-model of F of sub-class $\mathrm{PD} + \mathrm{SU} + \mathrm{CA} + \mathrm{IU} + \mathrm{DI}$ and we conclude $F \notin \mathsf{BBI}_K$.

Remark: unlike IU, DI is not axiomatizable in BBI [4] thus we cannot have $\mathsf{BBI}_{\mathrm{DI}} = \mathsf{BBI}_{\mathrm{IU}}$. Hence the strict inclusion $\mathsf{BBI}_{\mathrm{IU}} \subsetneq \mathsf{BBI}_{\mathrm{DI}}$ by Proposition 1. Let us now discuss and develop the proof of Theorem 3, our core result.

6 Invertibility, group-PMEs and squares

In this section, we study the properties of the extension $\sim + \{\epsilon \nrightarrow m\}$ and how they impact invertible letters/words. We introduce the notion of group-PME.

Definition 13. *A* group-PME *over L is a* PME $\sim$ *such that $\mathcal{A}_\sim = \mathcal{I}_\sim$ where $\mathcal{I}_\sim = \{\mathsf{c} \in L \mid \epsilon \sim \mathsf{c}\beta$ holds for some $\beta \in L^\star\}$ is the set of* invertible letters *of $\sim$.*

The operator $\sim \mapsto \mathcal{I}_\sim$ is monotonic. By rule $\langle p_r \rangle$, the inclusion $\mathcal{I}_\sim \subseteq \mathcal{A}_\sim$ holds for any PME. We may write $\mathcal{I}_\mathcal{C}$ for $\mathcal{I}_{\sim_\mathcal{C}}$; this should not lead to any ambiguity. We introduce a set of derived rules related to invertible words (in $\mathcal{I}^\star_\sim$) and we analyze the relations between $\sim$ and invertible words. Appart from the letter α which serves as a parameter for (primary) extensions, we ease the reading by denoting invertible words with greek letters β, γ, ... in place of x, y, ...

Definition 14 (Squares and invertible squares). *We say that a word $\alpha \in L^\star$ is* square-free *if $\forall \mathsf{c} \in L, \mathsf{cc} \not\sim \alpha$. We say that the* PME $\sim$ *be over L* has invertible squares *if $\forall \mathsf{c} \in L, \mathsf{cc} \sim \mathsf{cc} \Rightarrow \mathsf{c} \in \mathcal{I}_\sim$ (i.e. any squarable letter is invertible).*

Proposition 5. *Let $\sim$ be a* PME *over L. If $\sim$ has invertible squares then for any word $k \in L^\star$, if $kk \sim kk$ holds then $k \in \mathcal{I}^\star_\sim$ holds.*

Proposition 6. PMEs *are closed under rules $\langle \epsilon_c, i_\uparrow, i_c, i_s, i_\leftarrow, i_\rightarrow \rangle$:*

$$\frac{\epsilon \nrightarrow \gamma \quad \epsilon \nrightarrow \beta}{\epsilon \nrightarrow \gamma\beta}\,\langle \epsilon_c \rangle \qquad \frac{x \nrightarrow y \quad \epsilon \nrightarrow \gamma\beta}{\gamma x \nrightarrow \gamma y}\,\langle i_c \rangle \qquad \frac{x \nrightarrow \beta y \quad \epsilon \nrightarrow \gamma\beta}{\gamma x \nrightarrow y}\,\langle i_\leftarrow \rangle$$

$$\frac{\epsilon \nrightarrow \gamma\beta \quad \epsilon \nrightarrow \gamma\beta'}{\beta \nrightarrow \beta'}\,\langle i_\uparrow \rangle \qquad \frac{\gamma x \nrightarrow \gamma y \quad \epsilon \nrightarrow \gamma\beta}{x \nrightarrow y}\,\langle i_s \rangle \qquad \frac{\gamma x \nrightarrow y \quad \epsilon \nrightarrow \gamma\beta}{x \nrightarrow \beta y}\,\langle i_\rightarrow \rangle$$

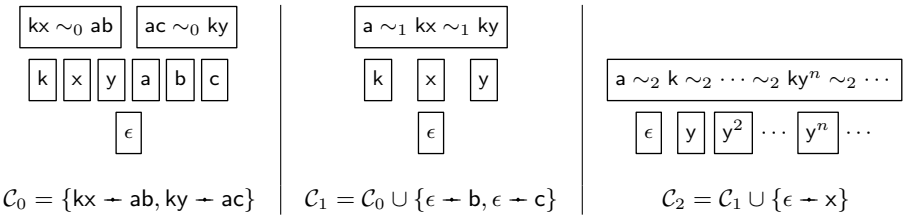

Fig. 2. The partial equivalence classes of $\sim_0 = \overline{\mathcal{C}_0}$, $\sim_1 = \overline{\mathcal{C}_1}$ and $\sim_2 = \overline{\mathcal{C}_2}$

Proposition 7. *Let $\sim$ be a* PME *over L and $x, y \in L^\star$ and $\gamma \in \mathcal{I}^\star_\sim$. We have: (a) $x \in \mathcal{I}^\star_\sim$ iff $\exists \beta\ \epsilon \sim x\beta$; (b) $x \sim y$ iff $\gamma x \sim \gamma y$; (c) the inclusion $\mathcal{I}^\star_\sim \subseteq \mathcal{L}_\sim$ holds; (d) if $x \sim y$ then $x \in \mathcal{I}^\star_\sim \Leftrightarrow y \in \mathcal{I}^\star_\sim$.*

In any group-PME $\sim$, every defined letter is invertible and from Proposition 7 (c), we obtain the identity $\mathcal{L}_\sim = \mathcal{I}^\star_\sim$.[13] Proposition 8 makes explicit a sufficient condition under which extensions do not change invertible letters: no new invertible letter appears in $\sim + \{x \rightharpoonup y\}$ unless either $x \in \mathcal{I}^\star_\sim$ or $y \in \mathcal{I}^\star_\sim$.

Proposition 8. *Let $\sim$ be a* PME *and $\mathcal{C}$ be a set of constraints such that for any $x \rightharpoonup y \in \mathcal{C}$ the identity $\{x, y\} \cap \mathcal{I}^\star_\sim = \emptyset$ holds. Then the identity $\mathcal{I}_{\sim+\mathcal{C}} = \mathcal{I}_\sim$ holds.*

7 No direct inductive proof of cancellativity for basic PMEs

We argue that it is not possible to prove cancellativity of basic PMEs by a direct induction on the length of the sequence defining them. This justifies the involved development that lies ahead. We present an example where the extensions $\sim + \{\epsilon \rightharpoonup m\}$ break cancellativity and introduce non-invertible squares.[14]

Let $\mathsf{k}, \mathsf{x}, \mathsf{y}, \mathsf{a}, \mathsf{b}, \mathsf{c} \in L$ be six different letters. Let us consider the following PME $\sim_0 = \sim_{\mathcal{C}_0}$ where $\mathcal{C}_0 = \{\mathsf{kx} \rightharpoonup \mathsf{ab}, \mathsf{ky} \rightharpoonup \mathsf{ac}\}$. In Figure 2, we represent the corresponding set of partial equivalence classes of $\sim_0$. It is left to the reader to check that these are indeed the partial equivalence classes of the closure of $\mathcal{C}_0$: we have $L^\star/{\sim_0} = \{[\epsilon], [\mathsf{k}], [\mathsf{x}], [\mathsf{y}], [\mathsf{a}], [\mathsf{b}], [\mathsf{c}], [\mathsf{kx}], [\mathsf{ky}]\}$ with $[\alpha] = \{\alpha\}$ for $\alpha \in \{\epsilon, \mathsf{k}, \mathsf{x}, \mathsf{y}, \mathsf{a}, \mathsf{b}, \mathsf{c}\}$ and $[\mathsf{kx}] = \{\mathsf{kx}, \mathsf{ab}\}$ and $[\mathsf{ky}] = \{\mathsf{ky}, \mathsf{ac}\}$. We check that $\sim_0$ is cancellative and has invertible squares (it contains no square except ϵ).

Now we consider the extension $\mathcal{C}_1 = \mathcal{C}_0 \cup \{\epsilon \rightharpoonup \mathsf{b}, \epsilon \rightharpoonup \mathsf{c}\}$ and $\sim_1 = \sim_0 + \{\epsilon \rightharpoonup \mathsf{b}, \epsilon \rightharpoonup \mathsf{c}\}$. Let us denote $E = \mathsf{b}^\star\mathsf{c}^\star = \{\mathsf{b}^i\mathsf{c}^j \mid i, j \in \mathbb{N}\}$. Then $L^\star/{\sim_1} = \{[\epsilon], [\mathsf{k}], [\mathsf{x}], [\mathsf{y}], [\mathsf{a}]\}$ where $[\alpha] = \alpha E$ for $\alpha \in \{\epsilon, \mathsf{k}, \mathsf{x}, \mathsf{y}\}$ and $[\mathsf{a}] = (\mathsf{a} \mid \mathsf{kx} \mid \mathsf{ky})E$. The PME $\sim_1$ is not cancellative anymore. Indeed, $\mathsf{kx} \sim_1 \mathsf{ky}$ but $\mathsf{x} \not\sim_1 \mathsf{y}$. Hence we have an example that shows that the extension $\sim + \{\epsilon \rightharpoonup m\}$ does not preserve cancellativity. But still $\sim_1$ has invertible squares; check that $\mathcal{I}_{\sim_1} = \{\mathsf{b}, \mathsf{c}\}$.

[13] In that case, $\sim$ is a congruence over $\mathcal{I}^\star_\sim$ and the quotient $\mathcal{I}^\star_\sim/{\sim}$ is an Abelian group.
[14] i.e. some kk with $kk \sim kk$ and $k \notin \mathcal{I}^\star_\sim$; see Definition 14.

Finally we consider the extension $\mathcal{C}_2 = \mathcal{C}_1 \cup \{\epsilon \rightharpoonup \mathsf{x}\}$ and $\sim_2 = \sim_1 + \{\epsilon \rightharpoonup \mathsf{x}\}$. Let us denote $E = \mathsf{b}^\star\mathsf{c}^\star\mathsf{x}^\star$. Then $L^\star/\sim_2 = \{[\mathsf{y}^n] \mid n \geqslant 0\} \cup \{[\mathsf{a}]\}$ with $[\mathsf{y}^n] = \mathsf{y}^n E$ and $[\mathsf{a}] = (\mathsf{a} \mid \mathsf{k})\mathsf{y}^\star E$. Like $\sim_1$, the PME $\sim_2$ is not cancellative. Moreover it has squares like y^2 where y is not an invertible letter; check $\mathcal{I}_{\sim_2} = \{\mathsf{b}, \mathsf{c}, \mathsf{x}\}$. Hence $\sim_2$ contains non-invertible squares.

We see that the extension $\sim + \{\epsilon \rightharpoonup m\}$ preserves neither cancellativity nor the invertibility of squares. Therefore it is not possible to show that basic PMEs have these properties by direct induction on the basic sequence.

8 Basic PMEs are primary extensions of group-PMEs

We define the notion of primary extension and use the equations in Lemma 3 to show that cancellativity and invertible squares are preserved by primary extensions. We then prove that basic PMEs are primary extensions of group-PMEs.

Definition 15 (Primary PME). *Let $\sim$ be a* PME *over L and $\alpha, m \in L^\star$ be two words such that $m \sim m$, $\alpha \neq \epsilon$, $\mathcal{A}_\sim \cap \mathcal{A}_\alpha = \emptyset$ and α is square-free. A* type-1 extension of $\sim$ *is of the form $\sim + \{\alpha \rightharpoonup m\}$; A* type-2 extension of $\sim$ *is of the form $\sim + \{\alpha m \rightharpoonup \mathsf{b}\}$ with $\mathsf{b} \in L \setminus (\mathcal{A}_\sim \cup \mathcal{A}_\alpha)$. A* primary extension of $\sim$ *is a type-1 or a type-2 extension of $\sim$. The class of* primary PMEs *is the least class containing group-*PMEs *and closed under primary extensions.*

We show that the properties of "cancellativity" and "invertible squares" hold for group-PMEs and are preserved by primary extensions.

Lemma 2. *Every group-*PME *is cancellative and has invertible squares.*

Lemma 3. *Let $\sim$ be a* PME *over L and $m, \alpha \in L^\star$ be such that $m \sim m$, $\alpha \neq \epsilon$ and $\mathcal{A}_\alpha \cap \mathcal{A}_\sim = \emptyset$. Then the two following identities hold:*

$$\sim + \{\alpha \rightharpoonup m\} = \{\delta\alpha^u x \rightharpoonup \delta\alpha^v y \mid \exists i,\ m^u x \sim m^v y, m^{i+u} x \sim m^{i+v} y \text{ and } \delta \prec \alpha^i\}$$
$$\sim + \{\alpha m \rightharpoonup \alpha m\} = \sim \cup \{\delta x \rightharpoonup \delta y \mid x \sim y, \epsilon \neq \delta \prec \alpha \text{ and } \exists q\ xq \sim m\}$$

Moreover, if $\sim$ is cancellative then both $\sim + \{\alpha \rightharpoonup m\}$ and $\sim + \{\alpha m \rightharpoonup \alpha m\}$ are cancellative; and if $\sim$ has invertible squares and α is square-free then both $\sim + \{\alpha \rightharpoonup m\}$ and $\sim + \{\alpha m \rightharpoonup \alpha m\}$ have invertible squares.

Corollary 1. *Primary* PMEs *are cancellative and have invertible squares.*

The proof of Lemma 3 is long/technical but not too difficult (once you have the equations). We now prove our core result: basic PMEs are primary PMEs; in particular, they are cancellative and have invertible squares.

Theorem 5. *Basic* PMEs *are primary* PMEs.

Proof. Let us consider a basic PME $\sim$. By Definition 12, there exists a basic sequence of constraints $(x_i \rightharpoonup y_i)_{i<k}$ such that $\sim\ =\ \sim_{\mathcal{H}}$, with $k < \infty$ and $\mathcal{H} = \{x_0 \rightharpoonup y_0, \ldots, x_{k-1} \rightharpoonup y_{k-1}\}$. For any $q \leqslant k$, we denote $\mathcal{H}_q = \{x_i \rightharpoonup y_i \mid i < q\}$.

The extension $\sim_{\mathcal{H}_q} + \{x_q \nrightarrow y_q\}$ is basic for any $q < k$. We recall the notation $\mathcal{I}_\sim = \mathcal{I}_\mathcal{H}$ for the set of invertible letters of $\sim = \sim_\mathcal{H}$.

From $x_i \nrightarrow y_i \in \mathcal{H}$, we deduce $x_i \sim y_i$ and by Proposition 7 (d), we have $x_i \in \mathcal{I}_\sim^\star$ iff $y_i \in \mathcal{I}_\sim^\star$ for any $i < k$. Hence we obtain a partition $[0,k[= C \uplus D$ with $C = \{i < k \mid \{x_i, y_i\} \subseteq \mathcal{I}_\sim^\star\}$ and $D = \{i < k \mid \{x_i, y_i\} \cap \mathcal{I}_\sim^\star = \emptyset\}$. Let us denote $\mathcal{C} = \{x_i \nrightarrow y_i \mid i \in C\}$ and $\mathcal{D} = \{x_i \nrightarrow y_i \mid i \in D\}$.

Let us enumerate $D = \{\sigma_0 < \cdots < \sigma_{d-1}\}$ in strictly increasing order with $d = \mathrm{card}(D) \leqslant k$ and $\sigma : [0,d[\longrightarrow [0,k[$. For $q \leqslant d$, let us denote $D_q = \{\sigma_i \mid i < q\}$. We show the inclusion $[0,\sigma_q[\subseteq C \cup D_q$: indeed, let us consider $j < \sigma_q$ and let us prove $j \in C \cup D_q$. From $\sigma_q < k$, we deduce $j \in [0,k[= C \uplus D$. In case $j \in C$, we have finished. In case $j \in D = \{\sigma_0 < \cdots < \sigma_{d-1}\}$, then $j = \sigma_r$ for some $r < d$. If $q \leqslant r$ then $\sigma_q \leqslant \sigma_r = j$ which contradicts $j < \sigma_q$. Hence we must have $r < q$ and we conclude $j = \sigma_r \in D_q$. Let us denote $\mathcal{D}_q = \{x_{\sigma_i} \nrightarrow y_{\sigma_i} \mid i < q\}$ for $q \leqslant d$. From $D_q \subseteq [0,\sigma_q[$ we derive $\mathcal{D}_q \subseteq \mathcal{H}_{\sigma_q}$.

Let us prove the identities $\mathcal{A}_\mathcal{C} = \mathcal{I}_\mathcal{C} = \mathcal{I}_\sim$. Since $\mathcal{H} = \mathcal{C} \cup \mathcal{D}$, we get $\sim_\mathcal{H} = \sim_\mathcal{C} + \mathcal{D}$. Moreover, every constraint of $\mathcal{D}$ is of the form $x \nrightarrow y$ with $\{x,y\} \cap \mathcal{I}_\sim^\star = \emptyset$. As $\mathcal{I}_\mathcal{C} \subseteq \mathcal{I}_\mathcal{H} = \mathcal{I}_\sim$ we deduce $\{x,y\} \cap \mathcal{I}_\mathcal{C}^\star = \emptyset$ for every constraint $x \nrightarrow y \in \mathcal{D}$. Thus, by Proposition 8, we have $\mathcal{I}_{\sim_\mathcal{C}+\mathcal{D}} = \mathcal{I}_{\sim_\mathcal{C}}$ and thus $\mathcal{I}_\mathcal{C} = \mathcal{I}_{\sim_\mathcal{C}} = \mathcal{I}_{\sim_\mathcal{C}+\mathcal{D}} = \mathcal{I}_{\sim_\mathcal{H}} = \mathcal{I}_\sim$. Also, for any $x \nrightarrow y \in \mathcal{C}$ we have $\{x,y\} \subseteq \mathcal{I}_\sim^\star$ and thus $\mathcal{A}_\mathcal{C} \subseteq \mathcal{I}_\sim$. We conclude $\mathcal{A}_\mathcal{C} = \mathcal{I}_\mathcal{C} = \mathcal{I}_\sim$. In particular, $\sim_\mathcal{C}$ is a group-PME.

Let us define $\mathcal{E}_q = \mathcal{C} \cup \mathcal{D}_q$ for $q \leqslant d$. As $\mathcal{C} \subseteq \mathcal{E}_q \subseteq \mathcal{E}_d = \mathcal{C} \cup \mathcal{D}_d = \mathcal{C} \cup \mathcal{D} = \mathcal{H}$, we deduce $\mathcal{I}_\sim = \mathcal{I}_\mathcal{C} \subseteq \mathcal{I}_{\mathcal{E}_q} \subseteq \mathcal{I}_\mathcal{H} = \mathcal{I}_\sim$ and thus $\mathcal{I}_{\mathcal{E}_q} = \mathcal{I}_\sim$ for any $q \leqslant d$. Let us establish the inclusions $\mathcal{H}_{\sigma_q} \subseteq \mathcal{E}_q$ and $\mathcal{A}_{\mathcal{E}_q} \setminus \mathcal{A}_{\mathcal{H}_{\sigma_q}} \subseteq \mathcal{I}_\sim$. The first inclusion follows from $[0,\sigma_q[\subseteq C \cup D_q$ and the definitions of $\mathcal{H}_{\sigma_q}$ and $\mathcal{E}_q$. For the second inclusion, starting with $\mathcal{D}_q \subseteq \mathcal{H}_{\sigma_q}$ we derive $\mathcal{E}_q = \mathcal{C} \cup \mathcal{D}_q \subseteq \mathcal{C} \cup \mathcal{H}_{\sigma_q}$ and thus $\mathcal{A}_{\mathcal{E}_q} \subseteq \mathcal{A}_\mathcal{C} \cup \mathcal{A}_{\mathcal{H}_{\sigma_q}} = \mathcal{I}_\sim \cup \mathcal{A}_{\mathcal{H}_{\sigma_q}}$. Hence the inclusion $\mathcal{A}_{\mathcal{E}_q} \setminus \mathcal{A}_{\mathcal{H}_{\sigma_q}} \subseteq \mathcal{I}_\sim$.

Let us show by induction on $q \leqslant d$ that $\sim_{\mathcal{E}_q}$ is a primary PME. First the ground case. We have $\mathcal{D}_0 = \emptyset$ and thus the identity $\sim_{\mathcal{E}_0} = \sim_\mathcal{C}$ holds. As a consequence, $\sim_{\mathcal{E}_0}$ is a group-PME and thus is a primary PME. Then the induction step. We assume that $\sim_{\mathcal{E}_q}$ is a primary PME and we show that $\sim_{\mathcal{E}_{q+1}} = \sim_{\mathcal{E}_q} + \{x_{\sigma_q} \nrightarrow y_{\sigma_q}\}$ is also a primary PME. For this aim, we show that $\sim_{\mathcal{E}_q} + \{x_{\sigma_q} \nrightarrow y_{\sigma_q}\}$ is identical to a primary extension of $\sim_{\mathcal{E}_q}$. We remind that the constraint $x_{\sigma_q} \nrightarrow y_{\sigma_q}$ is basic w.r.t. $\sim_{\mathcal{H}_{\sigma_q}}$. We proceed by case analysis on that fact (see Definition 11):

- if $x_{\sigma_q} \nrightarrow y_{\sigma_q} = \mathsf{ab} \nrightarrow m$ with $m \sim_{\mathcal{H}_{\sigma_q}} m$ and $\mathsf{a} \neq \mathsf{b} \in L \setminus \mathcal{A}_{\mathcal{H}_{\sigma_q}}$. From $\mathcal{H}_{\sigma_q} \subseteq \mathcal{E}_q$ we deduce $m \sim_{\mathcal{E}_q} m$. We establish the relation $\{\mathsf{a},\mathsf{b}\} \not\subseteq \mathcal{A}_{\mathcal{E}_q}$: if $\{\mathsf{a},\mathsf{b}\} \subseteq \mathcal{A}_{\mathcal{E}_q}$ holds then we have $\{\mathsf{a},\mathsf{b}\} \subseteq \mathcal{A}_{\mathcal{E}_q} \setminus \mathcal{A}_{\mathcal{H}_{\sigma_q}} \subseteq \mathcal{I}_\sim$ and as a consequence $\mathsf{ab} \in \mathcal{I}_\sim^\star$. But from $\sigma_q \in D$, we get $\mathsf{ab} = x_{\sigma_q} \notin \mathcal{I}_\sim^\star$ which leads to a contradiction.
  In case $\{\mathsf{a},\mathsf{b}\} \cap \mathcal{A}_{\mathcal{E}_q} = \emptyset$ then $\mathcal{A}_\mathsf{ab} \cap \mathcal{A}_{\mathcal{E}_q} = \emptyset$, $\mathsf{ab} \neq \epsilon$ is square-free and $m \sim_{\mathcal{E}_q} m$. Hence, $\sim_{\mathcal{E}_q} + \{\mathsf{ab} \nrightarrow m\}$ is a type-1 primary extension of $\sim_{\mathcal{E}_q}$.
  In case $\mathsf{a} \in \mathcal{A}_{\mathcal{E}_q}$ and $\mathsf{b} \notin \mathcal{A}_{\mathcal{E}_q}$ then $\mathsf{a} \in \mathcal{A}_{\mathcal{E}_q} \setminus \mathcal{A}_{\mathcal{H}_{\sigma_q}} \subseteq \mathcal{I}_\sim = \mathcal{I}_{\mathcal{E}_q}$ and hence we have $\epsilon \sim_{\mathcal{E}_q} \mathsf{a}\beta$ for some β. The identity $\sim_{\mathcal{E}_q} + \{\mathsf{ab} \nrightarrow m\} = \sim_{\mathcal{E}_q} + \{\mathsf{b} \nrightarrow m\beta\}$ holds by direct application of rules $\langle i_\leftarrow \rangle$ and $\langle i_\rightarrow \rangle$. We verify that $\sim_{\mathcal{E}_q} + \{\mathsf{b} \nrightarrow m\beta\}$ is a type-1 primary extension of $\sim_{\mathcal{E}_q}$: $\mathsf{b} \neq \epsilon$ is square-free, $\mathcal{A}_\mathsf{b} \cap \mathcal{A}_{\mathcal{E}_q} = \emptyset$, $m\beta \sim_{\mathcal{E}_q} m\beta$ (because $m \sim_{\mathcal{E}_q} m$, $\epsilon \sim_{\mathcal{E}_q} \mathsf{a}\beta$ and rule $\langle i_c \rangle$). Hence $\sim_{\mathcal{E}_q} + \{\mathsf{ab} \nrightarrow m\}$ is identical to a type-1 primary extension of $\sim_{\mathcal{E}_q}$.

The case $\mathsf{b} \in \mathcal{A}_{\mathcal{E}_q}$ and $\mathsf{a} \notin \mathcal{A}_{\mathcal{E}_q}$ can be treated in a symmetric way. In any of these three cases, we have proved that the PME $\sim_{\mathcal{E}_q} + \{\mathsf{ab} \rightarrowtail m\}$ can be expressed as a type-1 primary extension of $\sim_{\mathcal{E}_q}$;

- if $x_{\sigma_q} \rightarrowtail y_{\sigma_q} = \mathsf{a}m \rightarrowtail \mathsf{b}$ with $m \sim_{\mathcal{H}_{\sigma_q}} m$ and $\mathsf{a} \neq \mathsf{b} \in L \setminus \mathcal{A}_{\mathcal{H}_{\sigma_q}}$. From $\sigma_q \in D$, we have $\mathsf{b} = y_{\sigma_q} \notin \mathcal{I}^\star_\sim$ and thus $\mathsf{b} \notin \mathcal{I}_\sim$. From the inclusion $\mathcal{H}_{\sigma_q} \subseteq \mathcal{E}_q$, we deduce $m \sim_{\mathcal{E}_q} m$. We further have $\mathsf{b} \notin \mathcal{A}_{\mathcal{E}_q}$ (otherwise we would have $\mathsf{b} \in \mathcal{A}_{\mathcal{E}_q} \setminus \mathcal{A}_{\mathcal{H}_{\sigma_q}} \subseteq \mathcal{I}_\sim$ contradicting $\mathsf{b} \notin \mathcal{I}_\sim$). We consider the two cases $\mathsf{a} \notin \mathcal{A}_{\mathcal{E}_q}$ and $\mathsf{a} \in \mathcal{A}_{\mathcal{E}_q}$.
  In case $\mathsf{a} \notin \mathcal{A}_{\mathcal{E}_q}$ then we check that $\sim_{\mathcal{E}_q} + \{\mathsf{a}m \rightarrowtail \mathsf{b}\}$ is a type-2 primary extension: $\mathsf{a} \neq \epsilon$ is square-free, $\mathcal{A}_\mathsf{a} \cap \mathcal{A}_{\mathcal{E}_q} = \emptyset$, $m \sim_{\mathcal{E}_q} m$ and $\mathsf{b} \notin \mathcal{A}_{\mathcal{E}_q} \cup \mathcal{A}_\mathsf{a}$.
  In case $\mathsf{a} \in \mathcal{A}_{\mathcal{E}_q}$ then $\mathsf{a} \in \mathcal{A}_{\mathcal{E}_q} \setminus \mathcal{A}_{\mathcal{H}_{\sigma_q}} \subseteq \mathcal{I}_\sim = \mathcal{I}_{\mathcal{E}_q}$. Hence there exists β such that $\epsilon \sim_{\mathcal{E}_q} \mathsf{a}\beta$. The identity $\sim_{\mathcal{E}_q} + \{\mathsf{a}m \rightarrowtail \mathsf{b}\} = \sim_{\mathcal{E}_q} + \{\mathsf{b} \rightarrowtail \mathsf{a}m\}$ holds by rule $\langle s \rangle$. Let us check that $\sim_{\mathcal{E}_q} + \{\mathsf{b} \rightarrowtail \mathsf{a}m\}$ is a type-1 primary extension of $\sim_{\mathcal{E}_q}$: $\mathsf{b} \neq \epsilon$ is square-free and $\mathcal{A}_\mathsf{b} \cap \mathcal{A}_{\mathcal{E}_q} = \emptyset$ holds. $\mathsf{a}m \sim_{\mathcal{E}_q} \mathsf{a}m$ is the last remaining condition, obtained from $m \sim_{\mathcal{E}_q} m$ and $\epsilon \sim_{\mathcal{E}_q} \mathsf{a}\beta$ using rule $\langle i_c \rangle$.
  In any of these two cases, we have proved that the PME $\sim_{\mathcal{E}_q} + \{\mathsf{a}m \rightarrowtail \mathsf{b}\}$ can be expressed as a type-1 or as type-2 primary extension of $\sim_{\mathcal{E}_q}$;
- if $x_{\sigma_q} \rightarrowtail y_{\sigma_q} = \epsilon \rightarrowtail m$ with $m \sim_{\mathcal{H}_{\sigma_q}} m$. Then we have $x_{\sigma_q} = \epsilon \in \mathcal{I}^\star_\sim$ which directly contradicts $\{x_{\sigma_q}, y_{\sigma_q}\} \cap \mathcal{I}^\star_\sim = \emptyset$. Hence this case is not possible.

Hence, by induction on $q \leqslant d$, the PME $\sim_{\mathcal{E}_q}$ is primary. In particular $\sim_{\mathcal{E}_d} = \sim_{\mathcal{H}} = \sim$ is a primary PME.

Corollary 2. *Basic and simple* PME*s are cancellative and have invertible squares.*

Corollary 3. *Simple* PME*s closed under rule $\langle iu \rangle$ are also closed under rule $\langle di \rangle$.*

9 Conclusion

In this paper, we prove that validity in Boolean BI does not distinguish between some of the different notions of separation algebras commonly found in the literature. This result is obtained by an in-depth examination of the syntactic properties of basic/simple PMEs which are the counter-models that are generated by tableaux proof-search. We show that these models are cancellative and that the only squares they allow are composed of invertible letters using a detour via the notion of primary PME. From the cancellativity of simple PMEs and the strong completeness theorem, we derive equivalence results for cancellative partial monoids. We relate indivisibility of units to the disjointness property.

We propose some perspectives. First, we could investigate more properties of basic/simple PMEs to enrich the graph of known relations between the family $(\mathsf{BBI}_X)_X$. In particular, we expect a full characterization of basic PMEs that could lead to finer properties of simple PMEs. Another track of research would be to find a constructive proof of the results of this paper. There is little hope to succeed by using the strong completeness which is inescapably non-constructive; but we could for instance approach the problem by eliminating the cancellativity rule in the proofs of the sequent calculus [9]. Another way to tackle the problem would be to design bisimulations or at least Kripke semantics preserving relations between cancellative and non-cancellative models.

References

1. Brotherston, J.: Bunched Logics Displayed. Studia Logica **100**(6) (2012) 1223–1254
2. Brotherston, J., Kanovich, M.: Undecidability of Propositional Separation Logic and Its Neighbours. In: LICS, IEEE Computer Society (2010) 130–139
3. Brotherston, J., Kanovich, M.: Undecidability of Propositional Separation Logic and its Neighbours. Journal of the ACM **61**(2) (2014)
4. Brotherston, J., Villard, J.: Parametric Completeness for Separation Theories. In: POPL, ACM (2014) 453–464
5. Calcagno, C., O'Hearn, P.W., Yang, H.: Local Action and Abstract Separation Logic. In: LICS, IEEE Computer Society (2007) 366–378
6. Dinsdale-Young, T., Birkedal, L., Gardner, P., Parkinson, M.J., Yang, H.: Views: compositional reasoning for concurrent programs. In: POPL, ACM (2013) 287–300
7. Dockins, R., Hobor, A., Appel, A.W.: A Fresh Look at Separation Algebras and Share Accounting. In: APLAS. Volume 5904 of Lecture Notes in Computer Science., Springer (2009) 161–177
8. Galmiche, D., Larchey-Wendling, D.: Expressivity properties of Boolean BI through Relational Models. In: FSTTCS. Volume 4337 of Lecture Notes in Computer Science., Springer (2006) 358–369
9. Hóu, Z., Clouston, R., Goré, R., Tiu, A.: Proof search for propositional abstract separation logics via labelled sequents. In: POPL, ACM (2014) 465–476
10. Hóu, Z., Tiu, A., Goré, R.: A Labelled Sequent Calculus for BBI: Proof Theory and Proof Search. In: TABLEAUX. Volume 8123 of Lecture Notes in Computer Science., Springer (2013) 172–187
11. Ishtiaq, S.S., O'Hearn, P.W.: BI as an Assertion Language for Mutable Data Structures. In: POPL, London, UK (2001) 14–26
12. Larchey-Wendling, D.: The formal strong completeness of partial monoidal Boolean BI. J. Logic. Comput. (2014) doi:10.1093/logcom/exu031.
13. Larchey-Wendling, D., Galmiche, D.: Exploring the relation between Intuitionistic BI and Boolean BI: an unexpected embedding. Mathematical Structures in Computer Science **19**(3) (2009) 435–500
14. Larchey-Wendling, D., Galmiche, D.: The Undecidability of Boolean BI through Phase Semantics. In: LICS, IEEE Computer Society (2010) 140–149
15. Larchey-Wendling, D., Galmiche, D.: Nondeterministic Phase Semantics and the Undecidability of Boolean BI. ACM ToCL **14**(1) (2013) 6
16. Park, J., Seo, J., Park, S.: A theorem prover for Boolean BI. In: POPL, ACM (2013) 219–232
17. Pym, D.: The Semantics and Proof Theory of the Logic of Bunched Implications. Volume 26 of Applied Logic Series. Kluwer Academic Publishers (2002)
18. Reynolds, J.C.: Separation logic: A logic for shared mutable data structures. In: LICS, IEEE Computer Society (2002) 55–74