Modular Tableaux Calculi for Separation Theories

Simon Docherty[1] and David Pym[2]

University College London[1,2] and The Alan Turing Institute[2],
London, UK
{simon.docherty.14,d.pym}@ucl.ac.uk

Abstract. In recent years the key principles behind Separation Logic have been generalized to generate formalisms for a number of verification tasks in program analysis via the formulation of 'non-standard' models utilizing notions of separation distinct from heap disjointness. These models can typically be characterized by a *separation theory*, a collection of first-order axioms in the signature of the model's underlying ordered monoid. While all separation theories are interpreted by models that instantiate a common mathematical structure, many are undefinable in Separation Logic and determine different classes of valid formulae, leading to incompleteness for existing proof systems. Generalizing systems utilized in the proof theory of bunched logics, we propose a framework of tableaux calculi that are generically extendable by rules that correspond to separation theories axiomatized by coherent formulas. This class covers all separation theories in the literature — both classical and intuitionistic — as well as axioms for a number of related formalisms appropriate for reasoning about complex systems, security, and concurrency. Parametric soundness and completeness of the framework is proved by a novel representation of tableaux systems as coherent theories, suggesting a strategy for implementation and a tentative first step towards a new logical framework for non-classical logics.

Keywords: Bunched logic; Coherent logic; Kripke semantics; Proof theory; Separation Logic; Separation theories; Substructural logic; Tableaux

1 Introduction

Separation Logic [44], introduced by Ishtiaq & O'Hearn [36], Reynolds [50] and Yang & O'Hearn [55], is a Hoare-style program logic suitable for reasoning about programs that mutate data structures. In its original formulation, the assertion language of Separation Logic is based on a model of O'Hearn & Pym's logic of bunched implications [45] formulated by considering heaps as possible worlds with internal structure that allows their decomposition into separate pieces of memory. This decomposition is witnessed in the logic by the *separating conjunction* $*$, with $\phi * \psi$ informally read as 'the heap can be split into *separate* parts; one satisfying ϕ and the other satisfying ψ'.

Calcagno, O'Hearn & Yang [14] abstract the details of the heap model to a structure called a *separation algebra*, a partial-deterministic and cancellative monoid model of the Boolean logic of bunched implications (BBI), which can be used to generate bespoke separation logics suitable for program analysis tasks beyond that of the original formalism. Conflicting definitions of separation algebra have since been given by adding/removing first-order properties or strengthening/weakening the monoid properties [11, 15, 23, 26]. These mutually exclusive definitions can be encompassed in a framework of *separation theories* [11], collections of first-order axioms (*separation properties*) common to separation logic models which the definition of (B)BI model can be extended by. All separation logics in the literature can be seen to be models of separation theories, while the frameworks Views [23] and Iris [38] explicitly implement the idea of generating program logics parametrically by separation theory.

Recent work has revealed an expressivity gap between the logic of bunched implications and common separation theories in the literature, however. Brotherston & Villard [11] and Larchey-Wendling & Galmiche [41] have shown that separation properties like indivisibility of units and partial deterministic composition determine distinct sets of valid BBI formulae, leading to the incompleteness of standard proof systems with respect to typical classes of memory models. To make matters worse, Brotherston & Villard additionally show that many separation properties (among them partial determinism) are undefinable in BBI, and thus cannot be axiomatized by the logic. Similar arguments can be made for BI [48], the intuitionistic logic of bunched implications. This is an increasingly relevant issue given the growing number of intuitionistic separation logics, most prominent amongst them Iris, a framework that utilizes a 'later' modality [42] that can only be nontrivially defined in intuitionistic systems.

This expressivity gap is a significant problem for Separation Logic. A theorem prover for deriving assertions satisfied by the underlying model is a necessary component of any implementation of a separation logic, with the deployable proof theory of the standard formalism crucial for its scalability to large code bases [13, 55]. Standard implementations are model-specific, however, and only suitable for the heap model. In order to account for the large numbers of bespoke separation logics, as well as Views/Iris-style frameworks, we require tools that support parametrization by separation theory.

Technical Approach. The present work generalizes methods pioneered on tableaux systems for a range of logics including and related to BI and BBI [21, 22, 24, 29, 31, 39] to specify modular tableaux calculi for the breadth of classical and intuitionistic separation theories in the literature, proved sound and complete uniformly and parametrically in choice of separation theory. While previous systems implicitly implement a systematic method for constructing tableaux proof theory for bunched logics, subtle but signficant changes must be made to additionally capture separation theories. Past systems can be formulated as particular instances of our framework, thus making the systematic method explicit.

First, we specify tableaux proof systems for BI and BBI, the propositional basis for Separation Logic. The key difference between our calculi and tableaux

systems previously given in the literature is that we do not outsource any part of the derivation of proofs to an algebra of labels or auxilliary proof system for constraints. Instead, we utilize *frame expansion rules* that are of the same form as the standard *logical expansion rules* of the system. These rules capture the same structural properties (and more) but can also be added/removed in a modular fashion. Crucially, this ensures separation properties — for example, partial determinism — are not hard-coded into the basic systems via the structure of labels, and facilitates the parametricity of our completeness theorem.

We extend these systems with a rule schema for separation properties axiomatized by *coherent formulae*; a subset of first-order formulae with a special syntactic form. This set contains every separation property that can be found in the literature and is expressive enough to include virtually any axiom that might be utilized in future. The strength of this statement can be justified by a folklore result recently reconstructed by Dyckhoff & Negri [27] that shows that *every* first-order axiom can be reconstructed as an equivalent system of coherent formulae . We thus obtain a modular framework of $(B)BI+\Sigma$-tableaux systems, where Σ is an arbitrary collection of coherent axioms.

In order to prove soundness and completeness of the system, we utilize a novel representation of labelled tableaux systems as theories of coherent logic. The key insight here is that the translation of coherent formulae into tableaux rules is not one way: tableaux rules can naturally be seen as coherent formulae in a signature augmented with special predicate symbols. The parametric soundness and completeness of the framework can then be reduced to proving the soundness and completeness of Tarskian truth for coherent logic with respect to a meta-tableaux method, a problem positively resolved by Bezem & Coquand [4]. To our knowledge, the application of this technique to labelled tableaux is new, although, in the aforementioned work, Bezem & Coquand show how to encode the tableaux method for first-order classical logic as a coherent theory, and trace the idea of abbreviating formulae with predicate symbols to Skolem [52].

Contributions. We identify three principal contributions.

1. An exhaustive, sound and complete proof theory for the full breadth of separation theories in the literature. Notably, this includes intuitionistic separation theories that have never been considered proof theoretically.
2. A new technique for constructing proof systems for essentially any logic interpreted on Kripke structures that are axiomatized by coherent theories.
3. The identification of tableaux systems with theories of coherent logic.

On points 2 and 3, we believe many prefixed/labelled tableaux systems in the literature (e.g., [28]) are subsumed by this method, with their respective 'Hintikka set' completeness proofs actually localized instances of the parametric completeness theorem given here. This suggests coherent logic is a natural mathematical foundation for Kripke semantics and opens up the possibility of a logical framework for non-classical logics via the representation of tableaux systems as coherent theories. As Bezem & Coquand [4] mention, reasoning in coherent logic is constructive and proof objects can easily be produced from derivations. We discuss these possibilities in more detail in Section 6.

Related Work. While much work has been done on the proof theory of BI and BBI [9, 31, 34, 46], as well as proof systems for the concrete heap model of Separation Logic [5, 30, 33], very little exists for separation theories. A key exception to this is Hóu et al.'s [35] labelled sequent calculi for propositional abstract separation logic. There, a labelled sequent calculus for BBI is extended with rules corresponding to the most common separation properties – *partial determinism, cancellativity, indivisible unit* and *disjointness* – and completeness and cut elimination is proved. In Hóu's PhD dissertation [32] the properties *cross-split* and *splittability* are additionally handled, although completeness for these new rules requires 'non-trivial changes' to the previous proofs.

The classes of model captured by our systems strictly extend those of Hóu et al. — in particular, by additionally considering classes of BI models that are appropriate for intuitionistic separation logics — and our calculi are proved complete uniformly. Our systems are also generically extendable according to a rule schema, meaning the framework should be suitable for new separation theories devised in the future. A deficiency of our approach with respect to Hóu et al's is a lack of implementation, though we note that the representation of our systems as theories of coherent logic suggests off-the-shelf coherent logic provers could be used to give naive implementations of our framework.

Brotherston & Villard [11] deal with the undefinability of separation theories by defining a conservative extension of BBI called HyBBI, extending the syntax with nominals, satisfaction operators and binders. This extra expressivity leads to the axiomatizability of the undefinable separation properties. This work is not specifically concerned with proof theory, giving only a Hilbert-style system for HyBBI, and has the defect of requiring modifications to the syntax of Separation Logic. In addition, a significant theoretical reformulation would be required to capture intuitionistic separation theories this way. In contrast, in our work the necessary machinery is internalized within the proof system and both Boolean and intuitionistic cases are taken care of uniformly.

Finally, we connect our work to a recent line of research in proof theory investigating the generation of proof rules from coherent theories. Simpson [51] and Braüner [8] have used this technique to produce natural deduction rules, while Negri [43] has extensively developed it to generate systems of labelled sequent rules from frame conditions axiomatized by generalized coherent formulae. To our knowledge the present work is the first application of these ideas to the tableaux method. In addition, we believe the encoding of the proof systems themselves as coherent theories is novel.

2   Preliminaries

The Logics of Bunched Implications. We first recall O'Hearn & Pym's *logics of bunched implications* BI and BBI [45], the propositional basis of Separation Logic's assertion language. BI and BBI are archetypal examples of *bunched logics*; systems given by combining the standard *additives* of classical or intuitionistic propositional logic with the *multiplicatives* of a substructural logic. This idea

$$\frac{\xi \vdash \phi \quad \eta \vdash \psi}{\xi * \eta \vdash \phi * \psi} \qquad \frac{\eta * \phi \vdash \psi}{\eta \vdash \phi \twoheadrightarrow \psi} \qquad \frac{\xi \vdash \phi \twoheadrightarrow \psi \quad \eta \vdash \phi}{\xi * \eta \vdash \psi}$$

$$\overline{(\phi * \psi) * \xi \vdash \phi * (\psi * \xi)} \quad \overline{\phi * \psi \vdash \psi * \phi} \qquad \overline{\phi * \mathrm{I} \dashv\vdash \phi}$$

Fig. 1. Rules for the multiplicative fragment of (B)BI.

has been developed to give logics for reasoning about concurrency [25] and the layering structure of complex systems [18, 19, 24], Hennessey-Milner-style process logics for reasoning about security and systems modelling [1] and modal and epistemic systems for reasoning about reachability/knowledge subject to the availability of resources [22, 29].

Let Prop be a set of atomic propositions, ranged over by p. The set of all formulae of (B)BI is generated by the following grammar:

$$\phi ::= \mathrm{p} \mid \top \mid \bot \mid \mathrm{I} \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \to \phi \mid \phi * \phi \mid \phi \twoheadrightarrow \phi.$$

For BI, the standard connectives are interpreted intuitionistically; in BBI, classically. Negation is defined by $\neg \phi := \phi \to \bot$. Figure 1 gives Hilbert rules for the multiplicative fragment of the logics.

A *BI frame* is given by a tuple $\mathcal{X} = (X, \leq, \circ, E)$, where $(X, \leq)$ is a partial order, $\circ : X^2 \to \mathcal{P}(X)$ a binary composition (where $\mathcal{P}(X)$ denotes the power set of X) and $E \subseteq X$ a unary relation. This structure must satisfy the following axioms, where the outermost universal quantification is left implicit:

(Comm) $z \in x \circ y \to z \in y \circ x$ (Up) $e \in E \wedge e \leq e' \to e' \in E$
 (Weak) $\exists e \in E(x \in x \circ e)$ (Contr) $x \in y \circ e \wedge e \in E \to y \leq x$
 (Assoc) $t' \geq t \in x \circ y \wedge w \in t' \circ z \to \exists s, s', w'(s' \geq s \in y \circ z \wedge w \geq w' \in x \circ s')$.

The axioms formalize intuitive ideas about the composition of generic resources: for example, that the composition satisfies a generalized associativity that is compatible with the comparison order. This analysis is known as *resource semantics*.

A sound interpretation of BI is given by extending the standard poset semantics for propositional intuitionistic logic. This requires a *persistent* valuation: a map $\mathcal{V} : \mathrm{Prop} \to \mathcal{P}(X)$ such that $x \in \mathcal{V}(\mathrm{p})$ and $x \leq y$ entail $y \in \mathcal{V}(\mathrm{p})$. We call a BI frame $\mathcal{X}$ together with a persistent valuation $\mathcal{V}$ a *Kripke BI model*. The satisfaction relation $\vDash_{\mathcal{V}}$ is given in Fig 2. As standard for intuitionistic logics, persistence extends to all formulae of BI. *Kripke BBI models* and their associated semantics are given by the special case of the definitions for BI when the partial order $\leq$ is equality.

Coherent Logic. Coherent logic is the fragment of first-order logic consisting of formulae of the form $A_1(\vec{x}) \wedge \cdots \wedge A_n(\vec{x}) \to \exists \vec{y_1} B_1(\vec{x}, \vec{y_1}) \vee \cdots \vee \exists \vec{y_m} B_m(\vec{x}, \vec{y_m})$, for $n, m \geq 0$, where each A_i is an atomic formula involving only variables from the vector $\vec{x}$, and each B_i is the conjunction of atomic formulae involving only variables from the vectors $\vec{x}$ and $\vec{y_i}$. In a coherent formula, the variables $\vec{x}$

$r \vDash$	p	iff $r \in \mathcal{V}(\mathrm{p})$	$r \vDash$	$\top$	$r \nvDash \bot$

$$r \vDash \quad \mathrm{p} \quad \text{iff } r \in \mathcal{V}(\mathrm{p}) \qquad\qquad\qquad r \vDash \quad \top \qquad\qquad r \nvDash \bot$$
$$r \vDash \quad \phi \wedge \psi \quad \text{iff } r \vDash \phi \text{ and } r \vDash \psi \qquad\qquad r \vDash \quad \phi \vee \psi \ \text{ iff } r \vDash \phi \text{ or } r \vDash \psi$$
$$r \vDash \quad \phi \rightarrow \psi \ \text{ iff for all } r' \geq r, \ r' \vDash \phi \text{ implies } r' \vDash \psi; \quad r \vDash \quad \mathrm{I} \quad \text{ iff } r \in E$$
$$r \vDash \quad \phi * \psi \quad \text{iff there exists } r', s, t \text{ such that } r \geq r' \in s \circ t, \ s \vDash \phi \text{ and } t \vDash \psi$$
$$r \vDash \quad \phi \mathbin{-\!\!*} \psi \ \text{ iff for all } r', s, t \text{ such that } r \leq r', \ t \in r' \circ s, \ s \vDash \phi \text{ implies } t \vDash \psi$$

Fig. 2. Satisfaction for **(B)BI**. **BBI** is the case where $\leq$ is substituted with $=$.

are implicitly universally quantified (with scope the whole formula) and both $\vec{x}$ and $\overrightarrow{y_i}$ may be empty. The case $n = 0$ is a consequent that is always true — $\top \rightarrow \exists \overrightarrow{y_1} B_1(\vec{x}, \overrightarrow{y_1}) \vee \cdots \vee \exists \overrightarrow{y_m} B_m(\vec{x}, \overrightarrow{y_m})$ — similarly, the case $m = 0$ is an antecedent that is always false: $A_1(\vec{x}) \wedge \cdots \wedge A_n(\vec{x}) \rightarrow \bot$. The case $m = 1$ with empty $\overrightarrow{y_1}$ gives the *Horn clause* fragment of first-order logic utilized in logic programming and first-order theorem provers based on the resolution method.

We call a set of coherent formulae Φ a *coherent theory*. Models of coherent theories are given in a way standard for first-order logic: a *Tarskian model of Φ* is a non-empty set X together with an interpretation $\mathcal{I}$, which assigns to every n-ary relation symbol R in the signature a set $R^{\mathcal{I}} \subseteq X^n$ such that for each coherent formulae in Φ, for all $\vec{x} \in X$, the consequent $\exists \overrightarrow{y_1} \in X(B^{\mathcal{I}}(\vec{x}, \overrightarrow{y_1})) \vee \cdots \vee \exists \overrightarrow{y_m} \in X(B^{\mathcal{I}}(\vec{x}, \overrightarrow{y_m}))$ is true whenever the antecedent $A_1^{\mathcal{I}}(\vec{x}) \wedge \cdots \wedge A_n^{\mathcal{I}}(\vec{x})$ is true.

Many common mathematical structures are axiomatized by coherent theories. For example, algebraic structures like groups, rings, lattices and fields, as well as total, partial, and linear orders. Further examples are found in the theory of confluence for term rewriting systems [4, 53]. Of interest for our purposes, (B)BI frames are axiomatized by coherent theories. As we will see, virtually every separation property in the literature is given directly as a coherent axiom.

3   Modular Tableaux Calculi for Separation Theories

The Base Tableaux Systems. We begin with tableaux systems designed for the semantics of (B)BI as outlined in Section 2. As is standard for tableaux systems, derivations in our calculi are implicit attempts to construct a countermodel for the formula ϕ to be proved. This is done via the derivation of syntactic expressions that give partial specifications of a (B)BI model that can be realized as a real model if the formula is invalid. If every possible countermodel construction (i.e., every branch of a tableau) results in a contradiction, then we may conclude that no countermodel exists and call such a tableau a proof of ϕ.

A *labelled formula* $\mathbb{S}\phi : x$ is given by a sign $\mathbb{S} \in \{\mathbb{T}, \mathbb{F}\}$ together with a (B)BI formula ϕ and a *label* $x \in \{c_i \mid i \in \mathbb{N}\}$. A labelled formula states that a (B)BI formula ϕ is true ($\mathbb{T}$) or false ($\mathbb{F}$) at the state represented by the label x. A *constraint* is a syntactic expression of the form $x \sim y$, $R_* xyz$ or Ex, where $x, y, z \in \{c_i \mid i \in \mathbb{N}\}$. Constraints are partial specifications of the structure of a (B)BI frame corresponding to a partial order $\leq$, composition $\circ$, or unit set E respectively. Unlike other bunched logic tableaux systems, we only utilize atomic

Logical expansion rules

$\langle\mathbb{T}\wedge\rangle$ $$\frac{\mathbb{T}\phi\wedge\psi:x\in\mathcal{F}}{\langle\{\mathbb{T}\phi:x,\mathbb{T}\psi:x\},\emptyset\rangle}$$ $\langle\mathbb{F}\wedge\rangle$ $$\frac{\mathbb{F}\phi\wedge\psi:x\in\mathcal{F}}{\langle\{\mathbb{F}\phi:x\},\emptyset\rangle\mid\langle\{\mathbb{F}\psi:x\},\emptyset\rangle}$$

$\langle\mathbb{T}\vee\rangle$ $$\frac{\mathbb{T}\phi\vee\psi:x\in\mathcal{F}}{\langle\{\mathbb{T}\phi:x\},\emptyset\rangle\mid\langle\{\mathbb{T}\psi:x\},\emptyset\rangle}$$ $\langle\mathbb{F}\vee\rangle$ $$\frac{\mathbb{F}\phi\vee\psi:x\in\mathcal{F}}{\langle\{\mathbb{F}\phi:x,\mathbb{F}\psi:x\},\emptyset\rangle}$$

$\langle\mathbb{T}\mathrm{I}\rangle$ $$\frac{\mathbb{T}\mathrm{I}:x\in\mathcal{F}}{\langle\emptyset,\{Ex\}\rangle}$$

Frame expansion rules

$\langle\mathrm{Ref}\rangle$ $$\frac{Expr(x)\in\mathcal{C}\cup\mathcal{F}}{\langle\emptyset,\{x\sim x\}\rangle}$$ $\langle\mathrm{Trans}\rangle$ $$\frac{x\sim y,y\sim z\in\mathcal{C}}{\langle\emptyset,\{x\sim z\}\rangle}$$

$\langle\mathrm{Cong}\rangle$ $$\frac{x\sim y,y\sim x,Expr(x)\in\mathcal{C}}{\langle\emptyset,\{Expr(y/x)\}\rangle}$$ $\langle\mathrm{Com}\rangle$ $$\frac{R_*xyz\in\mathcal{C}}{\langle\emptyset,\{R_*yxz\}\rangle}$$

$\langle\mathrm{Weak}\rangle$ $$\frac{Expr(x)\in\mathcal{F}\cup\mathcal{C}}{\langle\emptyset,\{Ec_i,R_*xc_ix\}\rangle}$$ $\langle\mathrm{Contr}\rangle$ $$\frac{R_*xyz,Ey\in\mathcal{C}}{\langle\emptyset,\{x\sim z\}\rangle}$$

with c_i a fresh label, $Expr(x)$ any expression in which x occurs.

Fig. 3. Shared rules for the tableaux systems.

labels, as opposed to a monoidal algebra of labels that encodes properties of the multiplicative connectives. New constraints are derived only by *frame expansion rules*, rather than by using the properties of the algebra of labels and a separate proof system for constraints. A *constrained set of statements* (CSS) is a pair $\langle\mathcal{F},\mathcal{C}\rangle$, where $\mathcal{F}$ is a set of labelled formulae and $\mathcal{C}$ is a set of constraints. It is finite if $\mathcal{F}$ and $\mathcal{C}$ are.

Informally, tableaux are trees annotated with finite CSSs. Each branch determines a CSS $\langle\mathcal{F},\mathcal{C}\rangle$ where $\mathcal{F}$ (respectively $\mathcal{C}$) is the union of the formula (constraint) sets that occur on the branch. Figures 3 and 4 give rules dictating the expansion of tableaux: Figure 3 gives rules shared by both the BI and BBI systems, while Figure 4 gives rules specific to each system. While c_i,c_j,c_k denote concrete fresh labels, x,y,z etc. are *label variables*. An instance of a rule is triggered for a branch CSS when a concrete substitution instance of the premiss holds of it, and the same label substitutions carry through to the (branching) CSS(s) that the conclusion dictates are added to the tree. We now define (B)BI tableaux formally, with $\oplus$ giving concatenation of lists.

Definition 1 (Tableau). *A* (B)BI tableau *for a finite CSS* $\langle\mathcal{F}_0,\mathcal{C}_0\rangle$ *is a list of CSSs, called* branches, *built inductively according to the following rules:*

1. *The one branch list* $[\langle\mathcal{F}_0,\mathcal{C}_0\rangle]$ *is a tableau for* $\langle\mathcal{F}_0,\mathcal{C}_0\rangle$;
2. *If the list* $\mathcal{T}_m\oplus[\langle\mathcal{F},\mathcal{C}\rangle]\oplus\mathcal{T}_n$ *is a tableau for* $\langle\mathcal{F}_0,\mathcal{C}_0\rangle$ *and*

$$\frac{Premiss}{\langle\mathcal{F}_1,\mathcal{C}_1\rangle\mid\ldots\mid\langle\mathcal{F}_k,\mathcal{C}_k\rangle}$$

is a (B)BI expansion rule from Figures 3 or 4 for which a concrete instance of Premiss is fulfilled by $\langle\mathcal{F},\mathcal{C}\rangle$, *then the list* $\mathcal{T}_m\oplus[\langle\mathcal{F}\cup\mathcal{F}_1,\mathcal{C}\cup\mathcal{C}_1\rangle;\ldots;\langle\mathcal{F}\cup\mathcal{F}_k,\mathcal{C}\cup\mathcal{C}_k\rangle]\oplus\mathcal{T}_n$ *is a tableau for* $\langle\mathcal{F}_0,\mathcal{C}_0\rangle$.

Logical expansion rules for BI

$\langle \mathbb{T} \to \rangle$ $\dfrac{\mathbb{T}\phi \to \psi : x \in \mathcal{F} \text{ and } x \sim y \in \mathcal{C}}{\langle \{\mathbb{F}\phi : y\}, \emptyset \rangle \mid \langle \{\mathbb{T}\psi : y\}, \emptyset \rangle}$
  $\langle \mathbb{F} \to \rangle$ $\dfrac{\mathbb{F}\phi \to \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\phi : c_i, \mathbb{F}\psi : c_i\}, \{x \sim c_i\} \rangle}$

$\langle \mathbb{T}* \rangle$ $\dfrac{\mathbb{T}\phi * \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\phi : c_i, \mathbb{T}\psi : c_j\}, \{R_* c_i c_j c_k, c_k \sim x\} \rangle}$
  $\langle \mathbb{F}* \rangle$ $\dfrac{\mathbb{F}\phi * \psi : x \in \mathcal{F} \text{ and } R_* yzw, w \sim x \in \mathcal{C}}{\langle \{\mathbb{F}\phi : y\}, \emptyset \rangle \mid \langle \{\mathbb{F}\psi : z\}, \emptyset \rangle}$

$\langle \mathbb{T}{-\!\!*} \rangle$ $\dfrac{\mathbb{T}\phi {-\!\!*} \psi : x \in \mathcal{F} \text{ and } x \sim w, R_* wyz \in \mathcal{C}}{\langle \{\mathbb{F}\phi : y\}, \emptyset \rangle \mid \langle \{\mathbb{T}\psi : z\}, \emptyset \rangle}$
  $\langle \mathbb{F}{-\!\!*} \rangle$ $\dfrac{\mathbb{F}\phi {-\!\!*} \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\phi : c_j, \mathbb{F}\psi : c_k\}, \{x \sim c_i, R_* c_i c_j c_k\} \rangle}$

Frame expansion rules for BI

$\langle \text{Assoc} \rangle$ $\dfrac{t \sim t', R_* xyt, R_* t' zw \in \mathcal{C}}{\langle \emptyset, \{c_i \sim c_j, c_k \sim w, R_* yzc_i, R_* xc_j c_k\} \rangle}$
  $\langle \text{Up} \rangle$ $\dfrac{Ex, x \sim y \in \mathcal{C}}{\langle \emptyset, \{Ey\} \rangle}$

Logical expansion rules for BBI

$\langle \mathbb{T}\neg \rangle$ $\dfrac{\mathbb{T}\neg\phi : x \in \mathcal{F}}{\langle \{\mathbb{F}\phi : x\}, \emptyset \rangle}$
  $\langle \mathbb{F}\neg \rangle$ $\dfrac{\mathbb{F}\neg\phi : x \in \mathcal{F}}{\langle \{\mathbb{T}\phi : x\}, \emptyset \rangle}$

$\langle \mathbb{T} \to \rangle$ $\dfrac{\mathbb{T}\phi \to \psi : x \in \mathcal{F}}{\langle \{\mathbb{F}\phi : x\}, \emptyset \rangle \mid \langle \{\mathbb{T}\psi : x\}, \emptyset \rangle}$
  $\langle \mathbb{F} \to \rangle$ $\dfrac{\mathbb{F}\phi \to \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\phi : x, \mathbb{F}\psi : x\}, \emptyset \rangle}$

$\langle \mathbb{T}* \rangle$ $\dfrac{\mathbb{T}\phi * \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\phi : c_i, \mathbb{T}\psi : c_j\}, \{R_* c_i c_j x\} \rangle}$
  $\langle \mathbb{F}* \rangle$ $\dfrac{\mathbb{F}\phi * \psi : x \in \mathcal{F} \text{ and } R_* yzx \in \mathcal{C}}{\langle \{\mathbb{F}\phi : y\}, \emptyset \rangle \mid \langle \{\mathbb{F}\psi : z\}, \emptyset \rangle}$

$\langle \mathbb{T}{-\!\!*} \rangle$ $\dfrac{\mathbb{T}\phi {-\!\!*} \psi : x \in \mathcal{F} \text{ and } R_* xyz \in \mathcal{C}}{\langle \{\mathbb{F}\phi : y\}, \emptyset \rangle \mid \langle \{\mathbb{T}\psi : z\}, \emptyset \rangle}$
  $\langle \mathbb{F}{-\!\!*} \rangle$ $\dfrac{\mathbb{F}\phi {-\!\!*} \psi : x \in \mathcal{F}}{\langle \{\mathbb{T}\phi : c_i, \mathbb{F}\psi : c_j\}, \{R_* xc_i c_j\} \rangle}$

Frame expansion rules for BBI

$\langle \text{Assoc} \rangle$ $\dfrac{R_* xyt, R_* tzw \in \mathcal{C}}{\langle \emptyset, \{R_* yzc_i, R_* xc_i w\} \rangle}$
  $\langle \text{Sym} \rangle$ $\dfrac{x \sim y \in \mathcal{C}}{\langle \emptyset, \{y \sim x\} \rangle}$

with c_i, c_j, c_k fresh labels, $Expr(x)$ any expression in which x occurs.

Fig. 4. Tableaux rules for (B)BI

A (B)BI tableau for ϕ is a (B)BI tableau for $\langle \{\mathbb{F}\phi : c_0\}, \emptyset \rangle$. □

Definition 2 (Closed tableau/proof). *A CSS $\langle \mathcal{F}, \mathcal{C} \rangle$ is closed if one of the following closure conditions holds: (1) $\mathbb{T}\phi : x \in \mathcal{F}$, $\mathbb{F}\phi : y \in \mathcal{F}$ and $x \sim y \in \mathcal{C}$; (2) $\mathbb{F}\top : x \in \mathcal{F}$; (3) $\mathbb{T}\bot : x \in \mathcal{F}$; (4) $\mathbb{F}I : x \in \mathcal{F}$ and $Ex \in \mathcal{C}$. A CSS is open iff it is not closed. A tableau is closed iff all its branches are closed. A proof for a formula ϕ is a closed tableau for ϕ.* □

We note that we could simply add $\langle \mathbb{T}\neg \rangle, \langle \mathbb{F}\neg \rangle$, and $\langle \text{Sym} \rangle$ to the BI system and obtain one for BBI. However, this causes a significant amount of redundancy in the production of labels and constraints while requiring many more derivation steps in proofs, something that does not arise with the BBI rules given.

Extension with Coherent Axioms. Figure 5 gives a number of separation properties taken from across the Separation Logic literature [11, 14, 15, 26]. A *separation theory* is a collection Σ of axioms from Figure 5. All of the separation properties given are axiomatized as coherent formulae and we now show how to translate them into tableaux expansion rules and closure conditions. First, each

Partial Determinism	$z \in x \circ y \wedge z' \in x \circ y \rightarrow z = z'$
Total	$\exists z(z \in x \circ y)$
Cancellativity	$z \in x \circ y \wedge z \in x \circ y' \rightarrow y = y'$
Single Unit	$x \in E \wedge x' \in E \rightarrow x = x'$
Indivisible Units	$x \in y \circ z \wedge x \in E \rightarrow y \in E$
Disjointness	$x \in y \circ y \rightarrow y \in E$
Splittability	$x \in \overline{E} \wedge x \in E \rightarrow \bot, x \in \overline{E} \vee x \in E, x \in \overline{E} \rightarrow \exists y, z(y \in \overline{E} \wedge z \in \overline{E} \wedge x \in y \circ z)$
Cross-Split	$x \in t \circ u \wedge x \in v \circ w \rightarrow \exists a, b, c, d(t \in a \circ b \wedge u \in c \circ d \wedge v \in a \circ c \wedge w \in b \circ d)$
Upwards-Closed	$z \in x \circ y \wedge z \leq z' \rightarrow \exists x', y'(z' \in x' \circ y' \wedge x \leq x' \wedge y \leq y')$
Downwards-Closed	$z \in x \circ y \wedge x' \leq x \wedge y' \leq y \rightarrow \exists z'(z' \in x' \circ y' \wedge z' \leq z)$
Non-Branching	$x \leq y \wedge x \leq y' \rightarrow y \leq y' \vee y' \leq y$
Always-Joins	$x \leq y \wedge x \leq y' \rightarrow \exists z(y \leq z \wedge y' \leq z)$
Increasing	$z \in x \circ y \rightarrow y \leq z$
Unit Self Joining	$Ex \rightarrow x \in x \circ x$
Normal Increasing	$z \in x \circ y \wedge Ez \rightarrow x \leq z$

Fig. 5. Separation properties.

first-order atomic formula is translated into constraints: $Tr(z \in x \circ y) = R_* xyz$, $Tr(x \in E) = Ex$, $Tr(x \leq y) = x \sim y$ and $Tr(x = x') = x \sim x', x' \sim x$. Given $A_1(\vec{x}) \wedge \cdots \wedge A_n(\vec{x}) \rightarrow \exists \vec{y_1} B_1(\vec{x}, \vec{y_1}) \vee \cdots \vee \exists \vec{y_m} B_m(\vec{x}, \vec{y_m})$ with $n, m \neq 0$, we obtain the frame expansion rule

$$\frac{Tr(A_1(\vec{x})), \ldots, Tr(A_n(\vec{x})) \in \mathcal{C}}{\langle \emptyset, \mathcal{C}_1 \rangle \mid \ldots \mid \langle \emptyset, \mathcal{C}_m \rangle},$$

where each $\mathcal{C}_i$ is the set of constraints translated from the conjuncts of B_i, using fresh labels $\vec{c_i}$ in place of the previously quantified $\vec{y_i}$. For example, the separation properties Cross-Split and Non-Branching are translated to the rules

$$\frac{R_* tux, R_* vwx \in \mathcal{C}}{\langle \emptyset, \{R_* c_i c_j t, R_* c_k c_l u, R_* c_i c_k v, R_* c_j c_l w\} \rangle} \text{ and } \frac{x \sim y, x \sim y' \in \mathcal{C}}{\langle \emptyset, \{y \sim y'\} \rangle \mid \langle \emptyset, \{y' \sim y\} \rangle},$$

where c_i, c_j, c_k, c_l are fresh labels. The special case $n = 0$ gives a rule with premiss $Expr_1(x_1), \ldots, Expr_p(x_p) \in \mathcal{F} \cup \mathcal{C}$, where each $Expr_i(x_i)$ is *any* expression in which x_i occurs and the x_i are the universally quantified variables in the original formula. The case $m = 0$ gives a new closure condition consisting of the conjunction of constraints translated from the antecedent of the original formula.

Note that the property Splittability is defined by a *system* of coherent axioms. This axiomatization additionally requires a new type of constraint to be added to the tableaux system for their translated rules: $\overline{E}$, for the complement of E.

Given a separation theory Σ, a *(B)BI + Σ-tableau/proof* is defined in the same way as Definitions 1 and 2, except that a tableau can also be expanded by translated Σ-rules, and any new closure properties obtained from Σ can factor into the closure of a tableau and thus into proofs.

We give an example of a tableau proof in Figure 6. The formula $(\neg I \twoheadrightarrow \bot) \rightarrow I$ is valid in BBI models satisfying Total, but not in all BBI models [40, 48], and Figure 6 — written, for clarity, using the traditional representation of tableaux

(1)	$\langle \{\mathbb{F}(\neg I \mathbin{-\!\!*} \bot) \to I : c_0\}, \emptyset \rangle$	Premiss
(2)	$\langle \{\mathbb{T}\neg I \mathbin{-\!\!*} \bot : c_0, \mathbb{F}I : c_0\}, \emptyset \rangle$	$\langle \mathbb{F} \to \rangle$, from (1)
(3)	$\langle \emptyset, \{R_* c_0 c_0 c_1\} \rangle$	Total, from (1)

(4)	$\langle \{\mathbb{F}\neg I : c_0\}, \emptyset \rangle$	$\langle \{\mathbb{T}\bot : c_1\}, \emptyset \rangle$	$\langle \mathbb{T}\mathbin{-\!\!*} \rangle$, from (2), (3)
(5)	$\langle \{\mathbb{T}I : c_0\}, \emptyset \rangle$	$\otimes$	$\langle \mathbb{F}\neg \rangle$, from (4)
(6)	$\langle \emptyset, \{c_0 \sim c_0\} \rangle$		$\langle \text{Ref} \rangle$, from (5)
	$\otimes$		

Fig. 6. Tableau proof of $(\neg I \mathbin{-\!\!*} \bot) \to I$ in the BBI + Total system.

and using $\otimes$ to denote closed branches — shows that the tableaux system for BBI + Total proves it. The left-hand branch is closed because both $\mathbb{F}I : c_0$, $\mathbb{T}I : c_0$ and $c_0 \sim c_0$ occur, while the right is closed because $\mathbb{T}\bot : c_1$ occurs.

4 Applications to Separation Logics

The construction principles guiding the wide variety of separation logics in the literature are described in Jensen [37]: a *separation logic* is determined by a programming language, an assertion logic to describe machine state — a first-order theory of (B)BI generated by validity in a concrete model of (B)BI + Σ for some separation theory Σ — and a specification logic to describe computations — typically a logic of Hoare triples $\{\phi\}C\{\psi\}$, where ϕ and ψ are formulas of the assertion language and C a program. Soundness of the *frame rule*,

$$\frac{\{\,\phi\,\}\,C\,\{\,\psi\,\}}{\{\,\phi * \chi\,\}\,C\,\{\,\psi * \chi\,\}},$$

where χ does not include any free variables modified by the program C, witnesses the coherence of these different aspects, and facilitates Separation Logic's characteristic 'local reasoning', which allows conclusions about a program's effect on the global state to be derived from reasoning on just the resource it accesses.

To demonstrate the wide applicability of our framework we now give a number of separation logic models satisfying separation theories captured by our tableaux systems. Because of space constraints this selection is demonstrative rather than exhaustive. Other examples include Petri nets [14]; step-indexed models for storable locks [12] and the Iris framework [38]; separation logics incorporating named [47] and fractional [7] permissions; and separation logics designed for message passing [54] and amortized resource analysis [3].

Heaps. Our first example is given by the standard memory models of Separation Logic [36]. A *heap* is a partial function $h : \mathbb{N} \to \mathbb{Z}$, representing an allocation of memory addresses to values. Given heaps h, h', $h \# h'$ denotes that $dom(h) \cap dom(h') = \emptyset$; $h \cdot h'$ denotes the union of functions with disjoint domains, which is defined iff $h \# h'$. The *empty heap*, $[]$, is defined nowhere.

Let H denote the set of all heaps. Then $\mathrm{Heap}_{\mathrm{BBI}} = (H, \cdot, \{[]\})$ is a BBI frame. Letting $h \sqsubseteq h'$ denote that h' extends h, $\mathrm{Heap}_{\mathrm{BI}} = (H, \sqsubseteq, \cdot, H)$ defines a

(1)	$\langle \{ \mathbb{F} \phi * \psi \to \psi : c_0 \}, \emptyset \rangle$	Premiss
(2)	$\langle \{ \mathbb{T} \phi * \psi : c_1, \, \mathbb{F} \psi : c_1 \}, \{ c_0 \sim c_1 \} \rangle$	$\langle \mathbb{F} \to \rangle$, from (1)
(3)	$\langle \{ \mathbb{T} \phi : c_3, \, \mathbb{T} \psi : c_4 \}, \{ R_* c_3 c_4 c_2, \, c_2 \sim c_1 \} \rangle$	$\langle \mathbb{T} * \rangle$, from (2)
(4)	$\langle \emptyset, \{ c_4 \sim c_2 \} \rangle$	Increasing, from (3)
(5)	$\langle \emptyset, \{ c_4 \sim c_1 \} \rangle$	$\langle \text{Trans} \rangle$, from (2), (3)

$$\otimes$$

Fig. 7. Tableau proof of $\phi * \psi \to \psi$ in the BI + Increasing system.

BI frame. These frames generate the standard classical and intuitionistic models of Separation Logic. Heap_{BBI} satisfies Partial Determinism, Cancellativity, Single Unit, Indivisible Units, Cross-Split and Unit Self Joining; Heap_{BI} additionally satisfies Splittability, Upwards-Closed, Downwards-Closed, Increasing and Normal Increasing while dropping Single Unit and Unit Self Joining.

One of the key properties distinguishing the standard memory models is that weakening for $*$ (i.e., $\phi * \psi \to \psi$) is valid in the intuitionistic heap model but not the classical. Cao et al. [15] show that this corresponds to the separation property Increasing. Figure 7 — again, written using the traditional representation of tableaux — shows a single branch tableaux proof of $\phi * \psi \to \psi$ for $BI+$Increasing, closed because $\mathbb{T} \psi : c_4$, $\mathbb{F} \psi : c_1$ and $c_4 \sim c_1$ occur.

Permissions. Permissions are incorporated into variants of separation logics that are designed to reason about certain kinds of concurrent algorithms and more fine-grained notions of memory disjointness: for example, disjointness modulo shared read permission. Hóu [32] reports a schema of Clouston that encompasses many such models: we recall it, with two concrete instances.

Let V be a set of values and $\star : V^2 \to V$ an associative and commutative partial function. Denote by H_V the set of V-valued heaps $h : \mathbb{N} \to V$. Then $\text{Heap}_V = (H_V, \circ_\star, \{[]\})$ is a BBI frame, where $\circ_\star$ is defined by

$$h_1 \circ_\star h_2(n) = \begin{cases} h_1(n) \star h_2(n) & \text{if } n \in dom(h_1) \cap dom(h_2) \text{ and } h_1(n) \star h_2(n) \downarrow \\ h_1(n) & \text{if } n \in dom(h_1) \setminus dom(h_2) \\ h_2(n) & \text{if } n \in dom(h_2) \setminus dom(h_1) \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Hóu defines Bornat et al.'s [6] *counting permissions model* with $V = \mathbb{Z}^2$ and

$$(x, i) \star (y, j) = \begin{cases} (x, i + j) & \text{if } x = y, i < 0 \text{ and } j < 0 \\ (x, i + j) & \text{if } x = y, i + j \geq 0 \text{ and } (i < 0 \text{ or } j < 0) \\ \text{undefined} & \text{otherwise.} \end{cases}$$

This frame satisfies Partial Determinism, Cancellativity, Indivisible Units, Single Unit, Cross-Split and Unit Self Joining.

Hóu defines Dockins et al.'s [26] *binary tree model* by considering the set T of non-empty binary trees with leaves labelled $\top$ or $\bot$ that are quotiented by the smallest congruence that identifies any subtree in which all leaves have the same

label with a single leaf carrying that label. Then $V = \mathbb{Z} \times T$, and $\star$ is defined, where $\vee$ ($\wedge$) denotes pointwise disjunction (conjunction) of equivalent trees, by

$$(x, [t]) \star (y, [t']) = \begin{cases} (x, [t \vee t']) & \text{if } x = y \text{ and } [t \wedge t'] = [\bot] \\ \text{undefined} & \text{otherwise.} \end{cases}$$

This frame satisfies Partial Determinism, Cancellativity, Single Unit, Indivisible Units, Disjointness, Splittability, Cross-Split and Unit Self Joining.

Crash Hoare Logic. Chen et al. [17] use a separation logic to verify that the FSCQ file system meets its specification and secures its data under any sequence of crashes. Cao et. al. [15] give the underlying model as the following BI frame. Let V^+ be the set of non-empty lists over a set V and ϵ the empty list. Buffer heaps are defined to be heaps $h : \mathbb{N} \to V^+$. Let H_{buff} be the set of all buffer heaps. Then $Heap_{\text{buff}} = (H_{\text{buff}}, \leq, \cdot, \{[]\})$ is a BI frame, where $\cdot$ is the usual heap composition, and $h_1 \leq h_2$ iff $dom(h_1) = dom(h_2)$ and $\forall x \in \mathbb{N}, \exists l \in V^+ \cup \{\epsilon\}$ such that $h_1(x) = l \oplus h_2(x)$. This frame satisfies Partial Determinism, Cancellativity, Single Unit, Indivisible Units, Cross-Split, Upwards-Closed, Downwards-Closed, Always-Joins, Non-Branching, Unit Self Joining, and Normal Increasing.

Typed Heaps. Cao et al. [15] give an example derived from the handling of multibyte locks in Appel's [2] Verified System Toolchain separation logic for CompCert C. Let a *typed heap* be a partial map $h : \mathbb{N} \to \{\text{char}, \text{short}_1, \text{short}_2\}$ such that $h(n) = \text{short}_1$ implies $h(n+1) = \text{short}_2$. Let H_{typ} denote the set of all typed heaps. Then $\text{Heap}_{\text{Typ}} = (H_{\text{typ}}, \leq, \circ, H_{\text{typ}})$ is a BI frame, where $h_1 \leq h_2$ iff, for all $n \in dom(h_1)$ either $n \in dom(h_2)$ and $h_1(n) = h_2(n)$ or $h_1(n) = \text{char}$, and $h \in h_1 \circ h_2$ iff $h_1 \cdot h_2 \leq h$. This frame satisfies Indivisible Units, Disjointness, Splittability, Cross-Split, Upwards-Closed, Downwards-Closed, Non-Branching, Increasing, and Normal Increasing.

5   Metatheory

Tableaux Systems as Coherent Theories. Just as coherent formulae yield tableaux rules, tableaux rules yield coherent formulae, allowing a complete specification of our calculi as coherent theories. Our framework determines a first-order signature: for each formula ϕ of (B)BI, we have unary relation symbols $\mathbb{T}\phi$ and $\mathbb{F}\phi$, together with the unary relation symbol E, the binary relation symbol $\sim$ and the ternary relation symbol R_*.

Given a rule premiss '$\mathbb{S}\phi : x \in \mathcal{F}$ and $A_1 x_1^1 \ldots x_{k_1}^1, \ldots, A_m x_1^m \ldots x_{k_m}^m \in \mathcal{C}$' we obtain the coherent antecedent $C(\vec{x}) \equiv \mathbb{S}\phi(x) \wedge \bigwedge_i A_i x_1^i \ldots x_{k_i}^i$. For the $j - th$ conclusion $\langle \mathcal{F}_j, \mathcal{C}_j \rangle$ of the rule we obtain $\exists \overrightarrow{y_j} C_j(\vec{x}, \overrightarrow{y_j})$, where C_j is the conjunction of atomic formulae translated from the constraints in $\mathcal{F}_j \cup \mathcal{C}_j$, with any fresh labels $\vec{c}$ that occurred substituted with $\overrightarrow{y_j}$. The translated rule is thus $C(\vec{x}) \to \exists \overrightarrow{y_1} C_1(\vec{x}, \overrightarrow{y_1}) \vee \cdots \vee \exists \overrightarrow{y_n} C_n(\vec{x}, \overrightarrow{y_n})$. For example, the instance of the BI rule $\langle \mathbb{F} \ast \rangle$ for $\phi \mathbin{-\!\!*} \psi$ becomes $\mathbb{F}\phi \mathbin{-\!\!*} \psi(x) \to \exists y_1, y_2, y_3(\mathbb{T}\phi(y_2) \wedge \mathbb{F}\psi(y_3) \wedge x \sim y_1 \wedge R_* y_1 y_2 y_3)$.

There are some special cases to pay attention to. For tableaux rules with premiss $\text{Expr}(x) \in \mathcal{F} \cup \mathcal{C}$ the antecedent of the translated coherent formula

is $\top$. This is not the case for rules with premiss $\mathrm{Expr}(x) \in \mathcal{C}$: these must be translated into a separate rule for each of the finitely many ways x can occur in each constraint. Finally, each closure condition '$\mathbb{S}_1\phi_1 : x_1, \ldots, \mathbb{S}_n\phi_n : x_n,$ $A_1 y_1^1 \ldots y_{k_1}^1, \ldots,$ and $A_m y_1^m \ldots y_{k_m}^m$' gives $\bigwedge_i \mathbb{S}_i\phi_i(x_i) \wedge \bigwedge_i A_i y_1^i \ldots y_{k_i}^i \to \bot$.

Given a (B)BI formula ϕ, the finite coherent theory $\Phi_\phi^{(B)BI+\Sigma}$ is given by the translated $(B)BI + \Sigma$-frame expansion rules, the translated closure conditions and the instances of translated logical expansion rules for subformulae of ϕ. We note that we could specify the whole tableaux system for $(B)BI + \Sigma$ as an infinite coherent theory (similar to the axiomatization of a Hintikka set in standard tableaux completeness proofs), but finiteness is required for our argument.

Soundness and Completeness. We now prove soundness and completeness of the tableaux method via an analogous result for the Tarskian semantics of coherent logic. First, we show that the existence of a Kripke $(B)BI + \Sigma$-model with a state that doesn't satisfy ϕ is equivalent to the existence of a Tarskian model of $\Phi_\phi^{(B)BI+\Sigma} \cup \{\exists x.\mathbb{F}\phi(x)\}$.

Definition 3 (Induced Kripke Model of $\mathcal{M}$). *Given a Tarskian model $\mathcal{M}$ of $\Phi_\phi^{(B)BI+\Sigma}$, define $[a] = \{b \mid a \sim^{\mathcal{I}} b, b \sim^{\mathcal{I}} a\}$ and $X_\mathcal{M} = \{[a] \mid a \in X\}$. Then $[a] \leq_\mathcal{M} [b]$ iff $a \sim^{\mathcal{I}} b$, $[c] \in [a] \circ_\mathcal{M} [b]$ iff $R_*^{\mathcal{I}} abc$, and $E_\mathcal{M} = \{[a] \mid E^{\mathcal{I}} a\}$. $\mathcal{V}_\mathcal{M}(\mathrm{p}) = \{[a] \mid \exists b(b \sim^{\mathcal{I}} a$ and $\mathbb{T}\mathrm{p}^{\mathcal{I}}(b))\}$.*

1. *If $\mathcal{M}$ is a model of $\Phi_\phi^{BI+\Sigma}$, the induced Kripke frame is given by $\mathcal{X}_\mathcal{M} = (X_\mathcal{M}, \leq_\mathcal{M}, \circ_\mathcal{M}, E_\mathcal{M})$; the induced Kripke model is given by $(\mathcal{X}_\mathcal{M}, \mathcal{V}_\mathcal{M})$.*
2. *If $\mathcal{M}$ is a model of $\Phi_\phi^{BBI+\Sigma}$, the induced Kripke frame is given by $\mathcal{X}_\mathcal{M} = (X_\mathcal{M}, \circ_\mathcal{M}, E_\mathcal{M})$; the induced Kripke model is given by $(\mathcal{X}_\mathcal{M}, \mathcal{V}_\mathcal{M})$.*

The induced Kripke frame is a well-defined structure because of the frame tableaux rules, with $[-]$ forming equivalence classes and $\leq_\mathcal{M}$, $\circ_\mathcal{M}$, and $E_\mathcal{M}$ independent from the choice of representatives due to $\langle\mathrm{Cong}\rangle$. The $(B)BI + \Sigma$-frame properties for the induced frame follow from their correspondent rules in the tableaux and the valuation $\mathcal{V}_\mathcal{M}$ is independent of choice of representative and persistent for induced Kripke $BI + \Sigma$-models.

Lemma 1. *Given a Tarskian model $\mathcal{M}$ of $\Phi_\phi^{(B)BI+\Sigma}$, the induced Kripke model $\mathcal{X}_\mathcal{M}$ is a Kripke $(B)BI + \Sigma$-model.* □

The significance of this model is that satisfiability of subformulae ψ of ϕ is determined by the interpretation of the relation symbols $\mathbb{S}\psi$ in the original Tarskian model. A simple proof by induction yields the next lemma.

Lemma 2. *Let $\mathcal{M}$ be a Tarskian model of the coherent theory $\Phi_\phi^{(B)BI+\Sigma}$, ψ a subformula of ϕ and $a \in X$. 1. If $\mathbb{T}\psi^{\mathcal{I}}(a)$ holds in $\mathcal{M}$, then $[a] \vDash_{\mathcal{V}_\mathcal{M}} \psi$; 2. If $\mathbb{F}\psi^{\mathcal{I}}(a)$ holds in $\mathcal{M}$, then $[a] \nvDash_{\mathcal{V}_\mathcal{M}} \psi$.* □

We can also induce Tarskian models from Kripke models. Let $(\mathcal{X}, \mathcal{V})$ be a Kripke $(B)BI + \Sigma$-model. We define the induced Tarskian model by taking X to be the carrier, and defining the interpretation $\mathcal{I}$ by $\sim^{\mathcal{I}} = \leq$, $R_*^{\mathcal{I}} = \{(a, b, c) \mid c \in a \circ b\}$, $E^{\mathcal{I}} = E$, $\mathbb{T}\psi^{\mathcal{I}} = \{x \mid x \vDash_\mathcal{V} \psi\}$ and $\mathbb{F}\psi^{\mathcal{I}} = \{x \mid x \nvDash_\mathcal{V} \psi\}$.

Lemma 3.   *Every Kripke $(B)BI{+}\Sigma$-model $(\mathcal{X},\mathcal{V})$ with a state x (not) satisfying ϕ induces a model of $\Phi_\phi^{(B)BI+\Sigma} \cup \{\exists x.\mathbb{T}\phi(x)\}$ $(\Phi_\phi^{(B)BI+\Sigma} \cup \{\exists x.\mathbb{F}\phi(x)\})$.*   □

We now connect the existence of a closed tableaux to Bezem & Coquand's [4] *breadth-first forward reasoning* proof system for coherent logic. In their system, judgments of the form $X \Vdash^\Phi D$ are derived, where X is a set of atomic first-order sentences, Φ a finite coherent theory and D a *closed coherent disjunction*; a first-order sentence with the same syntactic shape as the consequent of a coherent formula. The derivation of the judgment $X \Vdash^\Phi D$ is defined inductively:

1. (Base) $X \Vdash^\Phi D$ holds if for one of the disjuncts $\exists \vec{y}.C$ of D, there are constants $\vec{a}$ such that all conjuncts of $C[\vec{y} := \vec{a}]$ occur in X;
2. (Inductive Step) Consider all closed instances $C_i \to D_i$ of Φ-axioms such that the conjuncts of C_i occur in X but the conjuncts of no disjunct $C_{i,j}$ of D_i do. There exist finitely many, with their consequents thus enumerated $D_0,\dots,D_n$. Let $\exists \overrightarrow{y_{i,j}}.C_{i,j}$ denote the j-th of the m_i disjuncts of D_i, and denote by $\overline{C_{i,j}}$ the substitution of $\overrightarrow{y_{i,j}}$ with fresh constants. Infer $X \Vdash^\Phi D$ from $\forall j_0 \in \{1,\dots,m_0\},\dots,\forall j_n \in \{1,\dots,m_n\}(X,\overline{C_{0,j_0}},\dots,\overline{C_{n,j_n}} \Vdash^\Phi D)$. Importantly, if a D_i is $\bot$, then $m_i = 0$, and $X \Vdash^\Phi D$ is trivially inferred.

A derivation can be seen as a kind of tableau, branching at each stage by adding every possible consequence of Φ obtainable from the atomic first-order sentences at the current node. A semi-decidable procedure is given to systematically search for a derivation of $X \Vdash^\Phi D$. First check the base case. If it doesn't hold, apply the inductive step to any Φ-axioms fireable from X. If there are none, X forms an Herbrand countermodel of Φ against D. If the inductive step can be applied, apply the search procedure recursively to all premises. Bezem & Coquand show that successful termination corresponds to Tarskian truth.

Theorem 1 ([4]).   *$X \Vdash^\Phi D$ is derivable iff the search procedure successfully terminates for $X \Vdash^\Phi D$ iff D is true in all Tarskian models of X,Φ.*

It is straightforward that the search procedure for $\{\mathbb{F}\phi(a)\} \Vdash^{\Phi_\phi^{(B)BI+\Sigma}} \bot$ corresponds precisely to an exhaustive search for a closed tableau for ϕ.

Lemma 4.   *There exists a closed $(B)BI+\Sigma$-tableaux for ϕ iff the search procedure for $\{\mathbb{F}\phi(a)\} \Vdash^{\Phi_\phi^{(B)BI+\Sigma}} \bot$ successfully terminates.*   □

Hence if a closed $(B)BI+\Sigma$-tableaux does not exist for ϕ, there exists a Tarskian model $\mathcal{M}$ of $\Phi_\phi^{(B)BI+\Sigma} \cup \{\exists x.\mathbb{F}\phi(x)\}$. By Lemma 2, the induced Kripke model $\mathcal{X}_\mathcal{M}$ has a state $[a]$ such that $[a] \nVdash_{\mathcal{V}_\mathcal{M}} \phi$, establishing that ϕ fails to be valid for Kripke $(B)BI+\Sigma$-models. Conversely, if a closed tableaux does exist, then there is no Tarskian model of $\mathcal{M}$ of $\Phi_\phi^{(B)BI+\Sigma} \cup \{\exists x.\mathbb{F}\phi(x)\}$. By Lemma 3, ϕ is valid in Kripke $(B)BI+\Sigma$-models, as otherwise any countermodel would generate a Tarskian model $\mathcal{M}$ of $\Phi_\phi^{(B)BI+\Sigma} \cup \{\exists x.\mathbb{F}\phi(x)\}$, a contradiction.

Theorem 2 (Soundness & Completeness for $(B)BI{+}\Sigma$-Tableaux). *ϕ is valid in Kripke $(B)BI{+}\Sigma$-models iff ϕ is provable in the $(B)BI{+}\Sigma$-tableaux system.*   □

6   Conclusions and Further Work

We have given a framework of tableaux systems that exhaustively captures the breadth of separation theories in the literature. Our framework is proven sound and complete parametrically by a novel representation of tableaux systems as coherent theories that allows us to apply existing theory from coherent logic. This resolves the expressivity gap between the logics of bunched implications and the separation logics defined upon them, and provides proof theory for the assertion languages of a wide array of program logics.

The completeness of tableaux systems is usually proved by defining a notion of a *Hintikka set*: a saturated set of (labelled) formulae (and possibly constraints) that can be transformed into a term model of the logic. It is then shown that the uncloseability of a tableau generates a Hintikka set that can be used as a countermodel, thus entailing invalidity of any formula without a tableau proof. Our method can be seen as a generalization of this idea, implemented parametrically by choice of tableaux system. While we have focused on Separation Logic, this technique is adaptable to virtually any logic interpreted on relational structures, including the breadth of bunched and modal logics. That this can all be performed in the setting of coherent logic suggests the significance of the fragment extends beyond the generation of proof rules for frame conditions. We aim to investigate the possibility of using coherent logic as a logical framework for non-classical logics more generally in work to be presented.

The implementation of our systems is of principal importance for future work. Our tableaux representation suggests existing coherent logic provers (see [49] for a survey) may already be suitable, though tactics designed specifically for tableaux coherent theories may have to be developed to make this efficient. A closely related goal is the development of Separation Logic implementations that utilize our systems as assertion language provers; if such an implementation could be done parametrically it would be very powerful indeed. Finally, our results suggest interesting theoretical work. Coherent logic has close connections to topos theory, and Caramello [16] has developed techniques to transfer results between mathematical fields via bridges between the classifying topoi of coherent theories. We wish to investigate if any results of logical interest can be found by utilizing the representation of tableaux as coherent theories.

References

1. G. Anderson and D. Pym. A Calculus and Logic of Bunched Resources and Processes. *Theoret. Comput. Sci.*, 614:63–96, 2016.
2. A. W. Appel. *Program Logics for Certified Compilers*. CUP, 2014.
3. R. Atkey. Amortised Resource Analysis with Separation Logic. *Log. Meth. Comput. Sci.*, 2(17):1–33, 2011.
4. M. Bezem and T. Coquand. Automating Coherent Logic. In *Proc. LPAR 2005*, LNCS 3836:246–260, 2005.
5. J. Berdine, C. Calcagno, and P. W. O'Hearn. Smallfoot: Modular automatic assertion checking with separation logic. In *Proc. FMCO 2005*, LNCS 4111:115–137, 2005.

6. R. Bornat, C. Calcagno, P. O'Hearn, and M. Parkinson. Permission Accounting in Separation Logic. In *Proc. POPL 2005*, ACM, 259–270, 2005.
7. J. Boyland. Checking interference with fractional permissions. In *Proc. SAS 2003*, LNCS 2694:55–72, 2003.
8. T. Braüner. *Hybrid Logic and its Proof-Theory*. Applied Logic Series 37, Springer Netherlands, 2011.
9. J. Brotherston. Bunched Logics Displayed. *Studia Logica* 100(6):1223–1254, 2012.
10. J. Brotherston and M. Kanovich. Undecidability of Propositional Separation Logic and Its Neighbours. *J. ACM*, 61(2):`https:doi.org/10.1145/2542667`, 2014.
11. J. Brotherston and J. Villard. Parametric Completeness for Separation Theories. In *Proc. POPL 2014*, ACM, 453–464, 2014.
12. A. Buisse, L. Birkedal, and K. Støvring. A Step-Indexed Kripke Model of Separation Logic for Storable Locks. In *Proc. MFPS 2011*, ENTCS 276:121–143, 2011.
13. C. Calcagno, D. Distefano, P. O'Hearn, and H. Yang. Compositional Shape Analysis by Means of Bi-abduction. *J. ACM*, 58(6), 2011.
14. C. Calcagno, P. O'Hearn, and H. Yang. Local Action and Abstract Separation Logic. In *Proc. LICS 2007*, IEEE, 366–378, 2007.
15. Q. Cao, S. Cuellar, and A. Appel. Bringing Order to the Separation Logic Jungle In *Proc. APLAS 2017*, LNCS, to appear.
16. O. Caramello. *Theories, Sites, Toposes: Relating and studying mathematical theories through topos-theoretic 'bridges'*. OUP, 2017.
17. H, Chen, D. Ziegler, T. Chajed, A. Chlipala, M. F. Kaashoek and N. Zeldovich. Using Crash Hoare Logic for Certifying the FSCQ File System. In *Proc. SOSP 2015*, ACM, 18–37, 2015.
18. M. Collinson, K. McDonald, and D. Pym. A Substructural Logic for Layered Graphs. *J. Logic Comput.*, 24(4):953–988, 2014.
19. M. Collinson, K. McDonald, and D. Pym. Layered Graph Logic as an Assertion Language for Access Control Policy Models. *J. Logic Comput.*, 27(1):41–80, 2017.
20. M. Collinson and D. Pym. Algebra and logic for resource-based systems modelling. *Math. Struct. Comput. Sci.* , 19:959–1027, 2009.
21. J.-R. Courtault and D. Galmiche. A Modal BI Logic for Dynamic Resource Properties. In *Proc. LFCS 2013*, Springer Berlin Heidelberg, 134–138, 2013.
22. J.-R. Courtault, D. Galmiche, and D. Pym. A Logic of Separating Modalities. *Theoret. Comput. Sci.*, 637:30–58, 2016.
23. T. Dinsdale-Young, L. Birkedal, P. Gardner, M. Parkinson, H. Yang. Views: compositional reasoning for concurrent programs. In *Proc. POPL 2013*, ACM, 287–300, 2013.
24. S. Docherty and D. Pym. Intuitionistic Layered Graph Logic. In *Proc. IJCAR 2016*, LNAI 9706:469–486, 2016.
25. S. Docherty and D. Pym. Stone-Type Dualities for Separation Logics. Submitted.
26. R. Dockins, A. Hobor, and A.W. Appel. A Fresh Look at Separation Algebras and Share Accounting. In *Proc. APLAS 2009*, LNCS 5904:161–177, 2009.
27. R. Dyckhoff and S. Negri. Geometrisation of First-Order Logic. *Bull. Symb. Log.*, 21(2):123–163, 2015.
28. M. Fitting. Tableau Methods of Proof for Modal Logics. *Notre Dame J. Form. Log.*, 13(2):237–247, 1972.
29. D. Galmiche, P. Kimmel, and D. Pym. A Substructural Epistemic Resource Logic. In *Proc. ICLA 2017*, LNCS 10119:106–122, 2017.
30. D. Galmiche and D. Méry. Tableaux and resource graphs for separation logic. J. Logic Comput., 20(1):189–231, 2007.
31. D. Galmiche, D. Méry, and D. Pym. The Semantics of BI and Resource Tableaux. *Math. Struct. Comput. Sci.*, 15:1033–1088, 2005.

32. Z. Hóu. Labelled Sequent Calculi and Automated Reasoning for Assertions in Separation Logic. PhD thesis, The Australian National University, 2015.
33. Z. Hóu, A. Tiu, and R. Goré. Automated Theorem Proving for Assertions in Separation Logic with All Connectives. In *Proc. CADE 25*, LNCS, 501–516, 2015.
34. Z. Hóu, A. Tiu, and R. Goré. A Labelled Sequent Calculus for BBI: Proof Theory and Proof Search. In *Proc. TABLEAUX 2013*, LNCS 8123:172–187, 2013.
35. Z. Hóu, R. Clouston, A. Tiu, and R. Goré. Proof Search for Propositional Abstract Separation Logics via Labelled Sequents In *Proc. POPL 2014*, ACM, 465–476, 2014.
36. S. Ishtiaq and P. O'Hearn. BI as an Assertion Language for Mutable Data Structures. In *Proc. POPL 2001*, ACM, 14–26, 2001.
37. J. Jensen. Enabling Concise and Modular Specifications in Separation Logic. PhD dissertation, IT University of Copenhagen, 2014.
38. R. Jung, R. Krebbers, J.-H. Jourdan, A. Bizjak, L. Birkedal, and D. Dreyer. Iris from the ground up: A modular foundation for higher-order concurrent separation logic. under consideration for publication in *J. Functional Programming*, 2017.
39. D. Larchey-Wendling. The Formal Strong Completeness of Partial Monoidal Boolean BI. *J. Log. Comput.*, 26(2):605–640, 2016.
40. D. Larchey-Wendling and D. Galmiche. The Undecidability of Boolean BI Through Phase Semantics. In *Proc. LICS 2010*, IEEE Computer Soc. Press, 140–149, 2010.
41. D. Larchey-Wendling and D. Galmiche. Looking at Separation Algebras with Boolean BI-eyes. In *Proc. TCS 2014*, LNCS 8705:326–340, 2014.
42. H. Nakano. A Modality for Recursion. In *Proc. LICS 2000*, IEEE Computer Soc. Press, 255–266, 2000.
43. S. Negri. Proof analysis beyond geometric theories: from rule systems to systems of rules. *J. Logic Comput.*, 26(2): 513–537, 2016.
44. P. O'Hearn. A Primer on Separation Logic. *Software Safety and Security; Tools for Analysis and Verification. NATO Science for Peace and Security Series* 33:286–318, 2012.
45. P. O'Hearn and D. Pym. The Logic of Bunched Implications. *Bull. Symb. Log.*, 5(2):215–244, June 1999.
46. J. Park, J. Seo, and S. Park. A Theorem Prover for BBI. In *Proc. POPL 2013*, ACM, 219–232, 2013.
47. M. Parkinson. Local Reasoning for Java. PhD thesis, Univ. of Cambridge, 2005.
48. D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications.* Applied Logic Series 26, Springer Netherlands, 2002.
49. A. Polonsky. Proofs, Types, and Lambda Calculus. PhD thesis, University of Bergen, 2012.
50. J. Reynolds. Separation Logic: A Logic for Shared Mutable Data Structures. In *Proc. LICS 2002*, IEEE Computer Soc. Press, 55–74, 2002.
51. A. Simpson. The Proof Theory and Semantics of Intuitionistic Modal Logic. PhD Thesis, University of Edinburgh, 1994.
52. Th. Skolem. Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit und Beweisbarkeit mathematischen Sätze nebst einem Theoreme über dichte Mengen, Skrifter I, 4: 1–36, Det Norske Videnskaps-Akademi, 1920.
53. Terese. *Term Rewriting Systems.* Cambridge University Press, 2003.
54. J. Villard, É. Lozes and C. Calcagno. Proving Copyless Message Passing. In *Proc. APLAS 2009*, LNCS 5904:194–209, 2009.
55. H. Yang and P. O'Hearn. A Semantic Basis for Local Reasoning. In *Proc. FOSSACS 2002*, LNCS 2303:402–416, 2002.