A Modal Sequent Calculus for Propositional Separation Logic

Neelakantan R. Krishnaswami [1]

Computer Science Department
Carnegie Mellon University
Pittsburgh, USA

Abstract

In this paper, we give a sequent calculus for separation logic. Unlike the logic of bunched implications, this calculus does not have a tree-shaped context – instead, we use labelled deduction to control when hypotheses can and cannot be used. We prove that cut-elimination holds for this calculus, and show that it is sound with respect to the provability semantics of separation logic.

Keywords: Separation logic, sequent calculus, cut-elimination, hybrid logic, labelled deduction

1 Introduction

Separation logic [11] is an extension of Hoare logic, designed to make it easier to reason about the behavior of programs making use of aliased mutable state.

In ordinary Hoare logic, a predicate describes a set of program states (in our case, heaps), and a conjunction like $A \wedge B$ holds of a state when that state holds of A and also holds of B. Unfortunately, aliasing is quite difficult to treat – if x and y are pointer variables, we need to explicitly state whether they alias or not. So as the number of variables in a program grows, the number of aliasing conditions grows quadratically. Worse still, this defeats modular proof, since as soon as we put a subprogram into a larger one, we need to add aliasing assertions describing possible interference between the subprogram and the larger program.

The key innovation in separation logic is to extend the logic of pre- and post-conditions with the *spatial* connectives $A * B$ and $A -\!\!* B$. Intuitively, we take $A * B$ to hold of a program state when the state can be divided into two *disjoint* parts, one of which holds of A and the other of which holds of B. Since the meaning of the connective enforces disjointness, we do not need to write aliasing conditions

[1] Email: neelk@cs.cmu.edu

Propositions	$A ::= \top \mid A \wedge B \mid A \to B \mid \bot \mid A \vee B$ $\mid I \mid A * B \mid A -\!\!* B \mid P$
Worlds	$\omega ::= \alpha \mid \epsilon \mid \omega \cdot \omega$
World Contexts	$\Omega ::= \cdot \mid \Omega, \alpha$
Equality Contexts	$\Xi ::= \cdot \mid \Xi, \omega = \omega'$
Hypothetical Contexts	$\Gamma ::= \cdot \mid \Gamma, A[\omega]$

Fig. 1. Syntax

explicitly. As in ordinary Hoare logic, separation logic has a rule of consequence:

$$\frac{P \vdash P' \qquad \{P'\}c\{Q'\} \qquad Q \vdash Q'}{\{P\}c\{Q\}}$$

However, the fact that we have a novel logic means that the entailment relation $P \vdash P'$ is also novel – so we need rules to reason about the entailment relation. This is most commonly done in a Hilbert-style deduction system, where axiom schemata are given that allow direct reasoning about entailment, without context-changing operations. However, such schemes are somewhat cumbersome to work with in practice, and it is desirable to have a sequent calculus or natural deduction system.

Our contributions in this paper are:

- First, we present a sequent calculus for separation logic that does not use bunched contexts. Instead, we interpret separation logic as a modal logic, and give a labelled deduction system that uses hybrids/labels to control when hypotheses can be used.
- Second, we prove that cut is an admissible rule for this calculus.
- Third, we show that this calculus is sound with respect to the semantics of separation logic – that is, any tautology provable in this calculus is true in the model.

2 The Sequent Calculus

Our logic is the propositional fragment of separation logic. We have $\top$ as truth, $A \wedge B$ as conjunction, $A \to B$ as implication, $\bot$ as falsehood, $A \vee B$ as disjunction, $A * B$ as separating conjunction, I as the unit to the separating conjunction, and $A -\!\!* B$ as the magic wand (i.e., adjoint to separating conjunction). We do not include the points-to connective $e \mapsto e'$, but we do add atomic formulas P. The grammar of propositions is given in Figure 1.

The main idea in this calculus is to move from a judgement of truth to a judgement that determines truth at a particular world. So our judgement does not provide a proof that A is true, but rather a proof that $A[\omega]$, which shows that A

World Well-formedness	$\Omega \vdash \omega : \mathsf{world}$
Equality Context Well-formedness	$\Omega \vdash \Xi\ \mathsf{ok}$
Context Well-formedness	$\Omega \vdash \Gamma\ \mathsf{ok}$
World Equality	$\Omega; \Xi \vdash \omega \equiv \omega'$
Proposition Provability	$\Omega; \Xi; \Gamma \vdash A[\omega]$

Fig. 2. Catalog of Judgements

$$\frac{\omega \equiv \omega' \in \Xi \qquad \Omega \vdash \Xi\ \mathsf{ok}}{\Omega; \Xi \vdash \omega \equiv \omega'}\ \textsc{EHyp} \qquad \frac{\Omega; \Xi \vdash \omega \equiv \omega'}{\Omega; \Xi \vdash \omega' \equiv \omega}\ \textsc{ESym}$$

$$\frac{\Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \Xi\ \mathsf{ok}}{\Omega; \Xi \vdash \omega \equiv \omega}\ \textsc{ERefl} \qquad \frac{\Omega; \Xi \vdash \omega \equiv \omega' \qquad \Omega; \Xi \vdash \omega' \equiv \omega''}{\Omega; \Xi \vdash \omega \equiv \omega''}\ \textsc{ETrans}$$

$$\frac{\Omega; \Xi \vdash \omega_1 \equiv \omega_2 \qquad \Omega; \Xi \vdash \omega_1' \equiv \omega_2'}{\Omega; \Xi \vdash \omega_1 \cdot \omega_2 \equiv \omega_1' \cdot \omega_2'}\ \textsc{ECat} \qquad \frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world}}{\Omega; \Xi \vdash \omega \cdot \epsilon \equiv \omega}\ \textsc{EUnit}$$

$$\frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \omega' : \mathsf{world}}{\Omega; \Xi \vdash \omega \cdot \omega' \equiv \omega' \cdot \omega}\ \textsc{EComm}$$

$$\frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \omega' : \mathsf{world} \qquad \Omega \vdash \omega'' : \mathsf{world}}{\Omega; \Xi \vdash \omega \cdot (\omega' \cdot \omega'') \equiv (\omega \cdot \omega') \cdot \omega}\ \textsc{EAssoc}$$

Fig. 3. World Equality

holds at a world ω. Likewise, we change the context from a multiset $A_1, \ldots, A_n$ to a multiset of located hypotheses $\Gamma = A_1[\omega_1], \ldots, A_n[\omega_n]$.

The world annotations themselves are not structureless. They are expressions formed from world variables α, concatenation $\omega \cdot \omega'$, and unit ϵ. We give an equality judgement for worlds $\Omega; \Xi \vdash \omega \equiv \omega'$ in Figure 3. This axiomatizes an equivalence relation (i.e., reflexive, transitive, symmetric) which makes the concatenation $\omega \cdot \omega'$ into an associative and commutative operation that has ϵ as a unit. The free world variables are in Ω, and a novelty of this equality judgement is that it allows the use of the hypothetical equalities found in the context Ξ. Ω is a set of variables, and Ξ is a multiset of equality hypotheses.

Finally, we come to the primary judgement of this calculus, the provability judgement $\Omega; \Xi; \Gamma \vdash A[\omega]$. This can be read as, "in a world variable context Ω, when the equations in Ξ hold, then A is provable at a world ω, under the hypotheses in Γ."

We catalog all the judgements of the system in Figure 2, and give the auxilliary well-formedness judgments in Figure 4.

Below, we give the inference rules for our separation logic calculus. The hypothesis rule Hyp allows us to conclude that an atomic proposition P holds at ω when

P can be found at ω' in the context, and the two worlds are equal.

The intuitionistic rules for $\top$, $A \wedge B$, $A \to B$, $\bot$, and $A \vee B$ all exactly follow the structure of the usual rules of the intuitionistic sequent calculus – the only difference is that we push around an extra world annotation ω. This corresponds to the fact that in the Kripke semantics of separation logic (given at the start of section 4), we never look at the exact shapes of a heap, except in the semantics of the spatial connectives.

The world annotations start to come into play with the spatial connectives. For example, in the EmpR rule, we are allowed to introduce I at ω, whenever we can show that ω equals the empty world ϵ. Likewise, reading the left rule from bottom to top, the hypothesis that $I[\omega]$ holds lets us add the assumption that $\omega \equiv \epsilon$.

$$\frac{\Omega; \Xi \vdash \omega \equiv \omega' \qquad \Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \Gamma\ \mathsf{ok}}{\Omega; \Xi; \Gamma, P[\omega] \vdash P[\omega']}\ \textsc{Hyp}$$

$$\frac{\Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \Gamma\ \mathsf{ok}}{\Omega; \Xi; \Gamma \vdash \top[\omega]}\ \textsc{TrueR} \qquad \text{(No TrueL)}$$

$$\frac{\Omega; \Xi; \Gamma \vdash A_1[\omega] \qquad \Omega; \Xi; \Gamma \vdash A_2[\omega]}{\Omega; \Xi; \Gamma \vdash A_1 \wedge A_2[\omega]}\ \textsc{AndR} \qquad \frac{\Omega; \Xi; \Gamma, A[\omega], B[\omega] \vdash C[\omega']}{\Omega; \Xi; \Gamma, A \wedge B[\omega] \vdash C[\omega']}\ \textsc{AndL}$$

$$\frac{\Omega; \Xi; \Gamma, A[\omega] \vdash B[\omega]}{\Omega; \Xi; \Gamma \vdash A \to B[\omega]}\ \textsc{ImpR}$$

$$\frac{\Omega; \Xi; \Gamma, A \to B[\omega] \vdash A[\omega] \qquad \Omega; \Xi; \Gamma, A \to B[\omega], B[\omega] \vdash C[\omega']}{\Omega; \Xi; \Gamma, A \to B[\omega] \vdash C[\omega']}\ \textsc{ImpL} \qquad \text{(No FalseR)}$$

$$\frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \Gamma, \bot[\omega]\ \mathsf{ok} \qquad \Omega \vdash \omega' : \mathsf{world}}{\Omega; \Xi; \Gamma, \bot[\omega] \vdash C[\omega']}\ \textsc{FalseL} \qquad \frac{\Omega; \Xi; \Gamma \vdash A[\omega]}{\Omega; \Xi; \Gamma \vdash A \vee B[\omega]}\ \textsc{OrR1}$$

$$\frac{\Omega; \Xi; \Gamma \vdash B[\omega]}{\Omega; \Xi; \Gamma \vdash A \vee B[\omega]}\ \textsc{OrR2} \qquad \frac{\Omega; \Xi; \Gamma, A[\omega] \vdash C[\omega'] \qquad \Omega; \Xi; \Gamma, B[\omega] \vdash C[\omega']}{\Omega; \Xi; \Gamma, A \vee B[\omega] \vdash C[\omega']}\ \textsc{OrL}$$

$$\frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \Gamma\ \mathsf{ok} \qquad \Omega; \Xi \vdash \epsilon \equiv \omega}{\Omega; \Xi; \Gamma \vdash I[\omega]}\ \textsc{EmpR} \qquad \frac{\Omega; \Xi, \epsilon \equiv \omega; \Gamma, I[\omega] \vdash C[\omega']}{\Omega; \Xi; \Gamma, I[\omega] \vdash C[\omega']}\ \textsc{EmpL}$$

$$\frac{\Omega; \Xi; \Gamma \vdash A[\omega_1] \qquad \Omega; \Xi; \Gamma \vdash B[\omega_2] \qquad \Omega; \Xi \vdash \omega \equiv \omega_1 \cdot \omega_2}{\Omega; \Xi; \Gamma \vdash A * B[\omega]}\ \textsc{StarR}$$

$$\frac{\Omega, \alpha, \beta; \Xi, \omega = \alpha \cdot \beta; \Gamma, A * B[\omega], A[\alpha], B[\beta] \vdash C[\omega']}{\Omega; \Xi; \Gamma, A * B[\omega] \vdash C[\omega']}\ \textsc{StarL}$$

$$\frac{\Omega, \alpha; \Xi; \Gamma, A[\alpha] \vdash B[\omega'] \qquad \Omega, \alpha; \Xi \vdash \omega \cdot \alpha \equiv \omega'}{\Omega; \Xi; \Gamma \vdash A \mathrel{-\!\!*} B[\omega]}\ \textsc{WandR}$$

$$\frac{\begin{array}{c}\Omega; \Xi; \Gamma, A \mathrel{-\!\!*} B[\omega] \vdash A[\omega''] \\ \Omega; \Xi \vdash \omega \cdot \omega'' \equiv \omega_1 \qquad \Omega; \Xi; \Gamma, A \mathrel{-\!\!*} B[\omega], B[\omega_1] \vdash C[\omega']\end{array}}{\Omega; \Xi; \Gamma, A \mathrel{-\!\!*} B[\omega] \vdash C[\omega']}\ \textsc{WandL}$$

The rules for $A * B$ are similar, but a little more complicated. In the StarR rule, we can show that $A * B$ holds at ω whenver we can find a world ω_1 that A holds in, and a world ω_2 that B holds in, such that ω equals their concatenation – exactly in analogy to the Kripke semantics for the separating conjunction.

The left rule for separating conjunction is the most complex rule in this calculus. If we have $A * B$ as a hypothesis at ω in the conclusion, then in the premise we can extend the context with two new worlds α and β, such that A holds at α, B holds at β, and that $\alpha \cdot \beta \equiv \omega$. The analogy to the Kripke semantics is interesting. In the Kripke semantics, if a heap h satisfies $A * B$, then there is a splitting of h into h_1 and h_2 such that h_1 satisfies A and h_2 satisfies B. Note that h_1 and h_2 are existentially quantified in the Kripke semantics. Because we have a separating conjunction as a hypothesis, we have this existential on the left-hand side of an implication. So we can essentially treat the existential as a universal, via the equivalence $(\exists x.P(x)) \supset Q \ \equiv \ \forall x.\ P(x) \supset Q$.

Finally we come to the right and left rules for the magic wand $A \mathrel{-\!\!*} B$. The right rule WandR tells us that we can prove that $A \mathrel{-\!\!*} B$ holds at ω, whenever we can show that if A holds at a new world α, then B holds at a world equivalent to $\omega \cdot \alpha$. This is in exact analogy to the Kripke semantics. The left rule tells us that if have a wand hypothesis $A \mathrel{-\!\!*} B$ at ω, and can find a proof that A holds at ω', then we can also assume that B holds at a world equivalent to $\omega \cdot \omega'$ while proving C.

$$\frac{\alpha \in \Omega}{\Omega \vdash \alpha : \mathsf{world}}\ \textsc{WHyp} \qquad \frac{}{\Omega \vdash \epsilon : \mathsf{world}}\ \textsc{WEps} \qquad \frac{\Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \omega' : \mathsf{world}}{\Omega \vdash \omega \cdot \omega' : \mathsf{world}}\ \textsc{WCat}$$

$$\frac{}{\Omega \vdash \cdot\ \mathsf{ok}}\ \textsc{EqOkNil} \qquad \frac{\Omega \vdash \Xi\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world} \qquad \Omega \vdash \omega' : \mathsf{world}}{\Omega \vdash Xi, \omega \equiv \omega'\ \mathsf{ok}}\ \textsc{EqOkCons}$$

$$\frac{}{\Omega \vdash \cdot\ \mathsf{ok}}\ \textsc{CtxOkNil} \qquad \frac{\Omega \vdash \Gamma\ \mathsf{ok} \qquad \Omega \vdash \omega : \mathsf{world}}{\Omega \vdash \Gamma, A[\omega]\ \mathsf{ok}}\ \textsc{CtxOkCons}$$

Fig. 4. Auxilliary Judgements

3 Proof Theory

Since we only allow the hypothesis rule at atomic propositions, we need to prove that the identity principle holds for this calculus.

Theorem 3.1 (Identity) *If* $\Omega \vdash \Xi\ \mathsf{ok}$, $\Omega \vdash \Gamma\ \mathsf{ok}$, *and* $\Omega; \Xi \vdash \omega \equiv \omega'$, *then* $\Omega; \Xi; \Gamma, A[\omega] \vdash A[\omega']$.

The proof is a straightforward induction on the proposition A.

Next, we can show that weakening holds for this calculus. Equivalent weakening rules hold (when they make sense) for all of the other judgements. However, for concision we will only state the theorems for the case of the main provability judgement.

Theorem 3.2 (Weakening) *We have that:*

(i) *If* $\Omega; \Xi; \Gamma \vdash A[\omega'']$, *then* $\Omega, \alpha; \Xi; \Gamma \vdash A[\omega'']$.

(ii) *If* $\Omega; \Xi; \Gamma \vdash A[\omega'']$ *and* $\Omega \vdash \omega : \mathsf{world}$, *and* $\Omega \vdash \omega' : \mathsf{world}$ *then we have that* $\Omega; \Xi, \omega \equiv \omega'; \Gamma \vdash A[\omega'']$.

(iii) *If* $\Omega; \Xi; \Gamma \vdash A[\omega'']$ *and* $\Omega \vdash \omega : \mathsf{world}$, *then* $\Omega; \Xi; \Gamma, B[\omega'] \vdash A[\omega'']$.

Next, we give a contraction principle for this calculus. As before, a similar contraction principle holds for the other judgements.

Theorem 3.3 (Contraction) *We have that:*

(i) *If* $\Omega; \Xi, \omega \equiv \omega', \omega \equiv \omega'; \Gamma \vdash C[\omega'']$, *then* $\Omega; \Xi, \omega \equiv \omega'; \Gamma \vdash C[\omega'']$.

(ii) *If* $\Omega; \Xi; \Gamma, A[\omega], A[\omega'] \vdash C[\omega'']$ *and* $\Omega; \Xi \vdash \omega \equiv \omega'$, *then* $\Omega, \alpha; \Xi; \Gamma, A[\omega] \vdash C[\omega'']$.

We do not give explicit theorems for Exchange, because we have been treating the contexts as multisets.

Finally, we can show that the cut rule is admissible in this calculus. We have two substitution principles for the world variable and world equation contexts, and a true cut principle for the provability judgement. (And once again, we elide the substitution principles for the other judgements in this calculus.)

Theorem 3.4 (Admissibility of Cut) *We have that:*

(i) *If* $\Omega \vdash \omega : \mathsf{world}$ *and* $\Omega, \alpha; \Xi; \Gamma \vdash C[\omega'']$, *then* $\Omega; \Xi[\omega/\alpha]; \Gamma[\omega/\alpha] \vdash C[\omega''[\omega/\alpha]]$.

(ii) *If* $\Omega; \Xi \vdash \omega \equiv \omega'$ *and* $\Omega; \Xi, \omega \equiv \omega'; \Gamma \vdash C[\omega'']$, *then* $\Omega; \Xi; \Gamma \vdash C[\omega'']$.

(iii) *If* $\Omega; \Xi; \Gamma \vdash A[\omega]$, *and* $\Omega; \Xi; \Gamma, A[\omega'] \vdash C[\omega'']$, *and* $\Omega; \Xi \vdash \omega \equiv \omega'$, *then* $\Omega; \Xi; \Gamma \vdash C[\omega'']$

The first two cases are just structural inductions over the derivation. The interesting case is the third case, which we prove with a structural cut admissibility argument in the style of Pfenning [8]. We do a induction on the size of the type A, lexicographically prior to a simultaneous induction on the sizes of the two provability derivations.

4 Soundness of the Calculus

In this section, we show that our sequent calculus is sound with respect to the Kripke semantics of separation logic, in the sense that the provable tautologies of our calculus are all equal to true in the semantics.

First, recall the Kripke semantics of separation logic. We write h for a heap (a finite function from locations to values; the whole set of heaps is written H) [2]; the

[2] In fact, the following section does not depend specifically on heaps. The algebraic structure we need is a

predicate $h\#h'$ holds when the domains of h and h' are disjoint; e is the empty heap; and $h \cdot h'$ is the union of two heaps, which is defined when the domains are disjoint. Since we include atoms in our propositional language, this satisfaction relation is also indexed by a function $\gamma \in \text{Atom} \to \mathcal{P}(H)$ to interpret the atoms.

$$
\begin{array}{ll}
h \models_\gamma \top & \text{iff always} \\
h \models_\gamma A \wedge B & \text{iff } h \models_\gamma A \text{ and } h \models_\gamma B \\
h \models_\gamma A \to B & \text{iff if } h \models_\gamma A \text{ then } h \models_\gamma B \\
h \models_\gamma \bot & \text{iff never} \\
h \models_\gamma A \vee B & \text{iff } h \models_\gamma A \text{ or } h \models_\gamma B \\
h \models_\gamma I & \text{iff } h = e \\
h \models_\gamma A * B & \text{iff } \exists h_1, h_2. h = h_1 \cdot h_2 \text{ and } h_1 \models_\gamma A \text{ and } h_2 \models_\gamma B \\
h \models_\gamma A -\!\!* B & \text{iff } \forall h'. \text{ if } h' \models_\gamma A \text{ and } h\#h' \text{ then } h \cdot h' \models_\gamma B \\
h \models_\gamma P & \text{iff } h \in \gamma(P)
\end{array}
$$

Now, we can give interpretation functions for the world expressions and the propositions. We will take a world expression as denoting a particular heap, and since world expressions may have free variables the interpretation will be a mapping from the free world variables to a heap. This can just follow the structure of the world expression – note that since heap concatenation is partial, the interpretation function for worlds is also necessarily partial. We will write $\omega \downarrow \eta$ to mean that the interpretation of ω is defined under the substitution η.

$$
\begin{aligned}
[\![\epsilon]\!]\eta &= e \\
[\![\alpha]\!]\eta &= \eta(\alpha) \\
[\![\omega \cdot \omega']\!]\eta &= [\![\omega]\!]\eta \cdot [\![\omega']\!]\eta
\end{aligned}
$$

We will also need an interpretation of propositions, which we will take to be the set of heaps satisfying the proposition.

$$[\![A]\!]\gamma = \{h \mid h \models_\gamma A\}$$

To show soundness, we first show that the equality judgement is sound.

Lemma 4.1 (Soundness of Equality) *If we have that:*

- $\Omega; \Xi \vdash \omega \equiv \omega'$,
- $\omega_i \downarrow \eta$, *and* $\omega_i' \downarrow \eta$, *and* $[\![\omega_i]\!]\eta = [\![\omega_i']\!]\eta$ *for every* $\omega_i \equiv \omega_i'$ *in* Ξ, *and*
- $\omega \downarrow \eta$ *or* $\omega' \downarrow \eta$

then we know that $\omega \downarrow \eta$ *and* $\omega' \downarrow \eta$ *and* $[\![\omega]\!]\eta = [\![\omega']\!]\eta$

The proof is a routine induction on the equality judgement. Armed with this lemma, we can give a soundness theorem for the sequent calculus:

---

separation algebra [3], which is just a partial commutative monoid.

Theorem 4.2 (Soundness of the Sequent Calculus) *If we have that:*

- $\Omega; \Xi; \Gamma \vdash A[\omega]$,
- $\eta \in \Omega \to H$,
- $\gamma \in Atom \to \mathcal{P}(H)$
- $\omega_i \downarrow \eta$, *and* $\omega_i' \downarrow \eta$, *and* $[\![\omega_i]\!]\eta = [\![\omega_i']\!]\eta$ *for every* $\omega_i \equiv \omega_i'$ *in* Ξ, *and*
- $\omega_j \downarrow \eta$ *and* $[\![\omega_j]\!]\eta \in [\![A_j]\!]\gamma$ *for every* $A_j[\omega_j]$ *in* Γ,

then we can conclude that if $\omega \downarrow \eta$, *then* $[\![\omega]\!]\eta \in [\![A]\!]\gamma$ *holds.*

The proof follows from an induction on the structure of the derivation. As an immediate corollary, it follows that if we can derive $\alpha; \cdot; \cdot \vdash A[\alpha]$, then A is a true proposition of separation logic.

4.1 (In)Completeness

While our calculus is sound, it is not even remotely complete with respect to the semantics. First, the set of heaps forms a boolean algebra, which means that the semantics validates the law of the excluded middle. Since we have an intuitionistic calculus, we cannot prove this. This problem might be rectified by extending the sequent calculus with multiple conclusions, to support classical reasoning.

However, this is not sufficient. Our equality judgement only allows us to make positive judgements about equality – and for completeness, we will need some way to reason from *inequality*. Concretely, suppose we add the points-to assertion $e \mapsto v$, which asserts that we have a one-element heap with location e pointing to value v. Now, consider the separation logic assertion $(x \mapsto -) * (x \mapsto -)$. This formula must entail false, because we know that the same pointer cannot be in two disjoint heaps and hence the formula is unsatisfiable. Such a deduction is not possible unless we have a way of deducing inequalities from world expressions.

5 Future and Related Work

5.1 Future Work

There are a number of directions to proceed from here. First, it would be interesting to add support for the points-to predicate, perhaps by extending the language of worlds to refer more explicitly to the contents of a heap. This is an interesting question even though it is known [4] that the points-to predicate and equality are sufficient to make judging validity undecidable – there might still be proof-theoretically well-behaved systems (in the sense of admitting cut-elimination) that contain points-to.

Adding first-order quantifiers would also be of interest beyond the practical utility, because in conjunction with the simplest formulation of points-to, it would introduce an interaction between the quantified variables and the hybrid labels. For example, consider the formula $\exists x.\ x \mapsto 5$ – here, the location of the pointer is existentially hidden!

Finally, in program proofs using separation logic, it is typical to identify and make use of special classes of formulas (such as the pure propositions, whose truth

does not depend on the heap; or the precise propositions, which unambiguously identify a piece of state) which satisfy additional axioms. It would be interesting to see if we can extend this calculus with modalities corresponding to those classes.

5.2 Related Work

Pym's original work on bunched implications [9,7] includes a natural deduction and sequent calculus for BI with a branching, tree-structured context. Even though the metatheory is very elegant, actually writing proofs in this calculus is quite complicated, which motivated us to seek an alternative proof theory.

This is also a problem Bean [1] sought to address, by giving a Fitch-style presentation of natural deduction for BI, called the ribbon calculus. This calculus extends the scoping rules of the regular Fitch style into the second dimension, with a (literally!) spatial scoping principle for the $*$ and $-\!\!*$ connectives.

Agostino and Gabbay [5] proposed labelled deduction as a general methodology for extending the methods for classical theorem proving to cope with intuitionistic and substructural logics. In his doctoral thesis, Simpson [12] shows how to use a labelled calculus to give a proof theory for modal logic, in which the labels are drawn from the Kripke semantics of modal logic.

Galmiche and Mery [6] describe a tableaux method for theorem proving in propositional BI. This work contains the key idea of using monoidal labels to control where BI formulas can and cannot be used. However, they must enrich this structure with an extra preorder structure in order to prevent the provability of formulas like $(A \wedge I) \to (A * A)$, which is not a valid formula of BI. However, we observed that all such anamolies are true theorems of separation logic, which permits us to leave out this preorder structure and simplify our calculus.

Braüner and de Paiva [2] present a natural deduction system for a hybrid propositional logic with a satisfaction operator $a : A$, which is a proposition that asserts that A holds at the world a. Reed [10] integrates a hybrid logic with monoidal labels into the dependent type theory LF. His system can express many substructural types, including a substantial fragment of bunched logic, including the magic wand but not the separating conjunction. This is because his system does not include explicit equality hypotheses in order to simplify type checking. (In our system, only the StarL rule introduces new hypothetical equalities.)

References

[1] Julian Michael Lewis Bean. *Ribbon Proofs – A Proof System for the Logic of Bunched Implications*. PhD thesis, Queen Mary University of London, January 2006.

[2] Torben Braüner and Valeria de Paiva. Intuitionistic hybrid logic. *Journal of Applied Logic*, 4(3):231–255, 2006.

[3] Cristiano Calcagno, Peter W. O'Hearn, and Hongseok Yang. Local action and abstract separation logic. In *LICS*, pages 366–378. IEEE Computer Society, 2007.

[4] Cristiano Calcagno, Hongseok Yang, and Peter W. O'Hearn. Computability and complexity results for a spatial assertion language for data structures. In *APLAS*, pages 289–300, 2001.

[5] Marcello D'Agostino and Dov M. Gabbay. A generalization of analytic deduction via labelled deductive systems. part i: Basic substructural logics. *J. Autom. Reasoning*, 13(2):243–281, 1994.

[6] Didier Galmiche and Daniel Méry. Semantic labelled tableaux for propositional bi. *J. Log. Comput.*, 13(5):707–753, 2003.

[7] Peter W. O'Hearn and David J. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.

[8] Frank Pfenning. Structural cut elimination: I. intuitionistic and classical logic. *Inf. Comput.*, 157(1-2):84–141, 2000.

[9] D.J. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002. Errata and Remarks maintained at: http://www.cs.bath.ac.uk/~pym/BI-monograph-errata.pdf.

[10] Jason Reed. Hybridizing a logical framework. *Electronic Notes in Theoretical Computer Science*, 174(6):135–148, 2007.

[11] John C. Reynolds. Separation logic: A logic for shared mutable data structures. In *LICS*, pages 55–74. IEEE Computer Society, 2002.

[12] Alex Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, December 1993.