Modal BI and Separation Logic (DRAFT)

Noam Zeilberger

June 8, 2005

Abstract

We present modal BI and show that the necessary propositions are exactly the "pure" propositions, in the sense of separation logic. We demonstrate the use of modal BI for reasoning with axioms and by induction, and also relate $\Box$ to the exponential modality $!$.

1 Introduction

Separation logic [10] is an extension of Hoare logic that was developed for reasoning about programs with shared mutable data. At its heart is a novel logical operation called the "separating" conjunction $*$, which coexists with the ordinary conjunction $\wedge$. The basic intuition is that the assertion $p * q$ holds in a given state only if the heap at that state can be split into disjoint parts, one in which p holds and the other in which q holds—the extra condition of disjointness allows one to express non-aliasing of pointers much more concisely than in ordinary Hoare Logic and thus prove correctness of programs using mutable store with only "local" reasoning. In [4], Ishtiaq and O'Hearn noted a correspondence between separation logic and O'Hearn and Pym's logic of bunched implications (BI) [6], a substructural logic that combines a multiplicative implication $-\!*$ with an intuitionistic implication $\rightarrow$ to obtain "resource sensitivity" in a manner very different from Girard's linear logic [3] [9]. It turns out that separation logic can be viewed as a model of Boolean BI (where $\rightarrow$ is classical), in which the atomic propositions are pointer assertions $e_1 \mapsto e_2$ ("the location denoted by e_1 contains the value denoted by e_2"). Hence much of separation logic can be axiomatized as BI together with a few axioms about the $\mapsto$ relation and arithmetic.

However, the correspondence is not perfect—real proofs in separation logic often require additional reasoning principles. For example, the proof of correctness of a garbage collector done in [2] took from [10] and [11] a catalogue of special classes of assertions, along with specialized axiom schemata for manipulating them. One such class that Reynolds defines is the "pure" assertions: an assertion p is said to be *pure* if for any store (assignment to variables), p is independent of the heap. Another important class is the "precise" assertions: an assertion p is *precise* if for any heap, there is at most one subheap that satisfies p. Additionally, the proof in [2] and others (e.g. [12]) make use of abstract data structures such as lists and sets, with their own set of axioms.

In this paper we take a step towards the formalization of separation logic by presenting *modal* BI. It turns out that purity can be characterized exactly in terms of S4 necessity. Moreover, the pure modality seems to be essential for reasoning from axioms or with inductive hypotheses, and hence for formalizing the use of data structures in separation logic or programming with inductive types in a programming language. This is related to recent work by Biering, Birkedal and Torp-Smith [1], in which they attempt to provide a semantic foundation for all of separation logic by defining the notion of a BI hyperdoctrine and higher-order separation logic. However, whereas they give a quite general semantics, we give a less general but conceptually very simple proof system that could serve as the basis (via Curry-Howard) for a BI programming language or type theory.

2 Modal BI: Syntax

2.1 BI overview

We begin by reviewing the natural deduction presentation of standard (intuitionistic) BI, adapted from [6] and [8]. Formulas are built out of propositional atoms P using the additive connectives $\wedge, \vee, \rightarrow$, the multiplicative connectives $*$ and $\mathrel{-\!*}$, the additive units $\top, \bot$, and the multiplicative unit I. Contexts are not sets or multisets but rather "bunches", given by the following grammar:

$$\Delta ::= A \mid \emptyset_a \mid (\Delta;\Delta') \mid \emptyset_m \mid (\Delta,\Delta')$$

A structural equivalence $\equiv$ is defined on bunches by taking the commutative monoid equations on ; and , with units $\emptyset_a$ and $\emptyset_m$ respectively, together with the congruence induced by equivalence on sub-bunches. Structural equivalence is reflected in the structural rule $\equiv$:

$$\frac{\Delta \vdash A \quad \Delta \equiv \Delta'}{\Delta' \vdash A}\ \equiv$$

The structural operators $\emptyset_a$ and ; correspond to the additives $\top$ and $\wedge$, and obey weakening and contraction through explicit structural rules:

$$\frac{\Delta \vdash A}{\Delta;\Delta' \vdash A}\ w \qquad \frac{\Delta;\Delta \vdash A}{\Delta \vdash A}\ c$$

The structural operators $\emptyset_m$ and , correspond to the multiplicatives I and $*$, and do *not* have weakening or contraction. The rest of the system is defined by the identity axiom $A \vdash A$, together with the logical rules given below. Note that in the notation $\Delta'(\Delta)$, Δ' stands for a meta-context, i.e. a context with a hole for a context, which is filled in by Δ.

$$\frac{\Delta_1 \vdash A \quad \Delta_2 \vdash B}{\Delta_1,\Delta_2 \vdash A * B}\ {*I} \qquad \frac{\Delta \vdash A * B \quad \Delta'(A,B) \vdash C}{\Delta'(\Delta) \vdash C}\ {*E} \qquad \frac{\Delta, A \vdash B}{\Delta \vdash A \mathrel{-\!*} B}\ {\mathrel{-\!*}I} \qquad \frac{\Delta \vdash A \mathrel{-\!*} B \quad \Delta' \vdash B}{\Delta,\Delta' \vdash B}\ {\mathrel{-\!*}E}$$

$$\frac{}{\emptyset_m \vdash I}\ II \qquad \frac{\Delta \vdash I \quad \Delta'(\emptyset_m) \vdash C}{\Delta'(\Delta) \vdash C}\ IE$$

$$\frac{\Delta_1 \vdash A \quad \Delta_2 \vdash B}{\Delta_1;\Delta_2 \vdash A \wedge B}\ {\wedge I} \qquad \frac{\Delta \vdash A \wedge B \quad \Delta'(A;B) \vdash C}{\Delta'(\Delta) \vdash C}\ {\wedge E} \qquad \frac{\Delta; A \vdash B}{\Delta \vdash A \rightarrow B}\ {\rightarrow I} \qquad \frac{\Delta \vdash A \rightarrow B \quad \Delta' \vdash B}{\Delta;\Delta' \vdash B}\ {\rightarrow E}$$

$$\frac{}{\emptyset_a \vdash \top}\ {\top I} \qquad \frac{\Delta \vdash \top \quad \Delta'(\emptyset_a) \vdash C}{\Delta'(\Delta) \vdash C}\ {\top E}$$

$$\frac{\Delta \vdash A}{\Delta \vdash A \vee B}\ {\vee I_1} \qquad \frac{\Delta \vdash B}{\Delta \vdash A \vee B}\ {\vee I_2} \qquad \frac{\Delta \vdash A \vee B \quad \Delta(A) \vdash C \quad \Delta(B) \vdash C}{\Delta'(\Delta) \vdash C}\ {\vee E}$$

$$\frac{\Delta \vdash \bot}{\Delta \vdash C}\ {\bot E}$$

It is possible to derive the following rules for identity and the intuitionistic connectives, which build in weakening and contraction:

$$\frac{}{\Delta; A \vdash A}\ id'$$

$$\frac{\Delta \vdash A \quad \Delta \vdash B}{\Delta \vdash A \wedge B}\ {\wedge I'} \qquad \frac{\Delta \vdash A \rightarrow B \quad \Delta \vdash B}{\Delta \vdash B}\ {\rightarrow E'} \qquad \frac{}{\Delta \vdash \top}\ {\top I'}$$

Note though that while these rules are derivable, we cannot directly use them in place of the system with explicit structural rules—we would have to modify the introduction and elimination rules for the multiplicative connectives as well to admit weakening and contraction, which results in a somewhat clunky system: see the discussion in [5, §3.4].

BI has intuitionistic logic (IL) and multiplicative intuitionistic linear logic (MILL) as independent fragments, but the interesting cases arise when they interact. For example, $*$ is (only) semidistributive over $\wedge$, in that $(A \wedge B) * C \vdash (A * C) \wedge (B * C)$ is valid but $(A * C) \wedge (B * C) \vdash (A \wedge B) * C$ is not. The following is a proof of the first fact:

$$\dfrac{\dfrac{\dfrac{}{(A\wedge B)*C\vdash(A\wedge B)*C}\ \mathit{id} \qquad \dfrac{\dfrac{}{A;B\vdash A}\ \mathit{id}' \quad \dfrac{}{C\vdash C}\ \mathit{id}}{(A;B),C\vdash A*C}\ *I}{(A\wedge B)*C\vdash A*C}\ \wedge E,*E \qquad \dfrac{\text{...symmetric...}}{(A\wedge B)*C\vdash B*C}}{(A\wedge B)*C\vdash(A*C)\wedge(B*C)}\ \wedge I'$$

2.2 BI + $\Box$

We now extend standard propositional BI with the S4 necessity operator $\Box$. It may seem like we are setting up a technical nightmare by adding modalities to a logic that already tests the limits of proof theory, but it turns out that the extension can be made in a completely modular fashion. Pfenning and Davies showed in [7] that a dual-zone judgment—with one context of true assumptions and a separate context of necessary ones—can elegantly represent intuitionistic S4. Let us recall their presentation. After defining a truth judgment $A\ \mathit{true}$, extending it to a hypothetical judgment $\Delta \vdash A\ \mathit{true}$ (where Δ is a set of *true* assumptions), and giving introduction and elimination rules for the various logical connectives, they then define what it means for a proposition to be necessary, or *valid*: $A\ \mathit{valid}$ holds if and only if $A\ \mathit{true}$ can be proved from no assumptions, i.e. $\cdot \vdash A\ \mathit{true}$. This then motivates a two zone judgment $\Gamma; \Delta \vdash A\ \mathit{true}$ where Γ is a set of *valid* assumptions, and three new rules: one for using valid assumptions to make conclusions about truth, and introduction and elimination rules for $\Box$ to internalize the validity judgment:

$$\dfrac{}{A\ \mathit{valid}, \Gamma; \Delta \vdash A\ \mathit{true}}\ \mathit{hyp}'$$

$$\dfrac{\Gamma; \cdot \vdash A\ \mathit{true}}{\Gamma; \Delta \vdash \Box A\ \mathit{true}}\ \Box I \qquad \dfrac{\Gamma; \Delta \vdash \Box A\ \mathit{true} \quad A\ \mathit{valid}, \Gamma; \Delta \vdash C}{\Gamma; \Delta \vdash C\ \mathit{true}}\ \Box E$$

Modal BI is constructed by simply importing this structure. We define validity by saying that $A\ \mathit{valid}$ if and only if A can be proved from the empty additive context, i.e. $\emptyset_a \vdash A$. Note this is a restriction of the definition of a BI "theorem" from [8], which is any formula that can be proved from *either* $\emptyset_a$ or $\emptyset_m$ (and proving from $\emptyset_m$ is strictly easier)—we will have more to say about this in Section 4. We then extend the BI hypothetical judgment $\Delta \vdash A$ to a dual-zone judgment $\Gamma \mid \Delta \vdash A$, where Γ is a flat context of valid assumptions (we write $\mid$ instead of ; to avoid confusion with the BI structural operator). The previously defined rules simply carry Γ through, and we have a rule *pure* for applying valid assumptions (why this is called "pure" will be explained in Section 3):

$$\dfrac{}{A, \Gamma \mid \emptyset_a \vdash A}\ \mathit{pure}$$

Finally, introduction and elimination rules for $\Box$ internalize validity:

$$\dfrac{\Gamma \mid \emptyset_a \vdash A}{\Gamma \mid \emptyset_a \vdash \Box A}\ \Box I \qquad \dfrac{\Gamma \mid \Delta \vdash \Box A \quad A, \Gamma \mid \Delta'(\emptyset_a) \vdash C}{\Gamma \mid \Delta'(\Delta) \vdash C}\ \Box E$$

The complete formal system is summarized in Figure 1. Notice that it contains intuitionistic S4 (minus $\Diamond$) as a fragment—in fact, if we forget that the contexts are bunched and ignore the multiplicative connectives, the system *is* the Pfenning-Davies presentation of modal logic, modulo the explicit structural rules—and the following rules that implicitly maintain weakening and contraction are derivable:

$$\dfrac{}{A, \Gamma \mid \Delta \vdash A}\ \mathit{pure}'$$

$$\dfrac{\Gamma \mid \emptyset_a \vdash A}{\Gamma \mid \Delta \vdash \Box A}\ \Box I' \qquad \dfrac{\Gamma \mid \Delta \vdash \Box A \quad A, \Gamma \mid \Delta \vdash C}{\Gamma \mid \Delta \vdash C}\ \Box E'$$

formulas

$$\begin{array}{lll} A, B & ::= & P \mid A * B \mid A \mathrel{-\!\!*} B \mid I \mid A \wedge B \mid A \to B \mid \top \mid A \vee B \mid \bot \mid \Box A \end{array}$$

contexts

$$\begin{array}{lll} \Gamma & ::= & \cdot \mid A, \Gamma \\ \Delta & ::= & A \mid \emptyset_a \mid (\Delta; \Delta') \mid \emptyset_m \mid (\Delta, \Delta') \end{array}$$

$$\boxed{\text{structural}}$$

$$\frac{\Gamma \mid \Delta \vdash A \quad \Delta \equiv \Delta'}{\Gamma \mid \Delta' \vdash A}\ \equiv \qquad \frac{\Gamma \mid \Delta \vdash A}{\Gamma \mid \Delta; \Delta' \vdash A}\ w \qquad \frac{\Gamma \mid \Delta; \Delta \vdash A}{\Gamma \mid \Delta \vdash A}\ c$$

$$\frac{}{\Gamma \mid A \vdash A}\ id \qquad \frac{}{A, \Gamma \mid \emptyset_a \vdash A}\ pure$$

$$\boxed{\text{multiplicative}}$$

$$\frac{\Gamma \mid \Delta_1 \vdash A \quad \Gamma \mid \Delta_2 \vdash B}{\Gamma \mid \Delta_1, \Delta_2 \vdash A * B}\ {*I} \qquad \frac{\Gamma \mid \Delta \vdash A * B \quad \Gamma \mid \Delta'(A, B) \vdash C}{\Gamma \mid \Delta'(\Delta) \vdash C}\ {*E}$$

$$\frac{\Gamma \mid \Delta, A \vdash B}{\Gamma \mid \Delta \vdash A \mathrel{-\!\!*} B}\ {\mathrel{-\!\!*}I} \qquad \frac{\Gamma \mid \Delta \vdash A \mathrel{-\!\!*} B \quad \Gamma \mid \Delta' \vdash B}{\Gamma \mid \Delta, \Delta' \vdash B}\ {\mathrel{-\!\!*}E}$$

$$\frac{}{\Gamma \mid \emptyset_m \vdash I}\ II \qquad \frac{\Gamma \mid \Delta \vdash I \quad \Gamma \mid \Delta'(\emptyset_m) \vdash C}{\Gamma \mid \Delta'(\Delta) \vdash C}\ IE$$

$$\boxed{\text{additive}}$$

$$\frac{\Gamma \mid \Delta_1 \vdash A \quad \Gamma \mid \Delta_2 \vdash B}{\Gamma \mid \Delta_1; \Delta_2 \vdash A \wedge B}\ {\wedge I} \qquad \frac{\Gamma \mid \Delta \vdash A \wedge B \quad \Gamma \mid \Delta'(A; B) \vdash C}{\Gamma \mid \Delta'(\Delta) \vdash C}\ {\wedge E}$$

$$\frac{\Gamma \mid \Delta; A \vdash B}{\Gamma \mid \Delta \vdash A \to B}\ {\to I} \qquad \frac{\Gamma \mid \Delta \vdash A \to B \quad \Gamma \mid \Delta' \vdash B}{\Gamma \mid \Delta; \Delta' \vdash B}\ {\to E}$$

$$\frac{}{\Gamma \mid \emptyset_a \vdash \top}\ {\top I} \qquad \frac{\Gamma \mid \Delta \vdash \top \quad \Gamma \mid \Delta'(\emptyset_a) \vdash C}{\Gamma \mid \Delta'(\Delta) \vdash C}\ {\top E}$$

$$\frac{\Gamma \mid \Delta \vdash A}{\Gamma \mid \Delta \vdash A \vee B}\ {\vee I_1} \qquad \frac{\Gamma \mid \Delta \vdash B}{\Gamma \mid \Delta \vdash A \vee B}\ {\vee I_2} \qquad \frac{\Gamma \mid \Delta \vdash A \vee B \quad \Gamma \mid \Delta(A) \vdash C \quad \Gamma \mid \Delta(B) \vdash C}{\Gamma \mid \Delta'(\Delta) \vdash C}\ {\vee E}$$

$$\frac{\Gamma \mid \Delta \vdash \bot}{\Gamma \mid \Delta \vdash C}\ {\bot E}$$

$$\boxed{\text{modal}}$$

$$\frac{\Gamma \mid \emptyset_a \vdash A}{\Gamma \mid \emptyset_a \vdash \Box A}\ {\Box I} \qquad \frac{\Gamma \mid \Delta \vdash \Box A \quad A, \Gamma \mid \Delta'(\emptyset_a) \vdash C}{\Gamma \mid \Delta'(\Delta) \vdash C}\ {\Box E}$$

Figure 1: Natural deduction for modal BI

Thus the usual validities of S4 are provable in modal BI, e.g. $\Box(A \to B) \vdash \Box A \to \Box B$, $\Box A \vdash \Box\Box A$, etc. (We are writing $\Delta \vdash C$ as shorthand for $\cdot \mid \Delta \vdash C$.) Again, however, more interesting is the interaction of $\Box$ with the multiplicative connectives. For example, we have $\Box A * \Box B \vdash \Box(A * B)$ but not conversely, and $\Box A \wedge (B * C) \vdash (\Box A \wedge B) * C$, as shown by the following derivations (we omit applications of $\equiv$, and some initial steps of eliminating connectives):

$\boxed{\Box A * \Box B \vdash \Box(A * B)}$

$$\dfrac{\dfrac{}{\cdot \mid \Box A \vdash \Box A}\,\mathit{id} \quad \dfrac{\dfrac{}{A \mid \Box B \vdash \Box B}\,\mathit{id} \quad \dfrac{\dfrac{\dfrac{}{A, B \mid \emptyset_a \vdash A}\,\mathit{pure} \quad \dfrac{}{A, B \mid \emptyset_m \vdash B}\,\mathit{pure}'}{A, B \mid \emptyset_a \vdash A * B}\,{*I}}{A, B \mid \emptyset_a, \emptyset_a \vdash \Box(A * B)}\,\Box I'}{A \mid \emptyset_a, \Box B \vdash \Box(A * B)}\,\Box E}{\cdot \mid \Box A, \Box B \vdash \Box(A * B)}\,\Box E$$

$\boxed{\Box A \wedge (B * C) \vdash (\Box A \wedge B) * C}$

$$\dfrac{\dfrac{}{\cdot \mid \Box A \vdash \Box A}\,\mathit{id} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{A \mid \emptyset_a \vdash A}\,\mathit{pure}}{A \mid \emptyset_a \vdash \Box A}\,\Box I \quad \dfrac{}{A \mid B \vdash B}\,\mathit{id}}{A \mid B \vdash \Box A \wedge B}\,\wedge I \quad \dfrac{}{A \mid C \vdash C}\,\mathit{id}}{A \mid B, C \vdash (\Box A \wedge B) * C}\,{*I}}{\cdot \mid \Box A; (B, C) \vdash (\Box A \wedge B) * C}\,\Box E$$

2.3 Axiomatic reasoning in modal BI

Our first demonstration of the use of modal BI is for reasoning in BI with additional axioms. We borrow from [9] (who in turn borrow from Hoare) the example of buying chocolates and candy from a vending machine. There are three basic propositions *coin*, *choc*, and *candy*, interpreted as follows:

- *coin*: I have one coin in my pocket
- *choc*: I have enough to buy a chocolate
- *candy*: I have enough to buy a candy

The fact that a candy costs one coin and a chocolate costs two is encoded by the following axioms:

$$\begin{array}{rcl} \mathit{coin} & \vdash & \mathit{candy} \\ \mathit{coin} * \mathit{coin} & \vdash & \mathit{choc} \end{array}$$

With this set of axioms and the rules of BI, it is possible to prove, for example, that $\mathit{coin} \vdash \mathit{coin} \mathrel{-\!\!*} \mathit{choc}$, i.e. if I have one coin in my pocket, then with one more I can buy a chocolate.

Now, in ordinary predicate calculus it is straightforward to translate reasoning from axioms into hypothetical reasoning, by converting each axiom into an additional assumption. But bunched contexts destroy this property. For suppose we encode the two axioms as hypotheses $\mathit{coin} \to \mathit{candy}$ and $\mathit{coin} * \mathit{coin} \to \mathit{choc}$: how do we combine these hypotheses with the context *coin* so as to be able to prove $\mathit{coin} \mathrel{-\!\!*} \mathit{choc}$? We might try combining them intuitionistically: we let $\Delta_a = (\mathit{coin} \to \mathit{candy}); (\mathit{coin} * \mathit{coin} \to \mathit{choc})$, and try to prove $\Delta_a; \mathit{coin} \vdash \mathit{coin} \mathrel{-\!\!*} \mathit{choc}$. But this sequent is *not* provable—the following is an attempt:

$$\dfrac{\dfrac{\dfrac{\Delta_a \vdash \mathit{coin} * \mathit{coin} \to \mathit{choc} \quad \mathit{coin}, \mathit{coin} \vdash \mathit{coin} * \mathit{coin}}{\Delta_a; (\mathit{coin}, \mathit{coin}) \vdash \mathit{choc}}\,{\to}E}{(\Delta_a; \mathit{coin}), \mathit{coin} \vdash \mathit{choc}}\,???}{\Delta_a; \mathit{coin} \vdash \mathit{coin} \mathrel{-\!\!*} \mathit{choc}}\,{-\!\!*}I$$

$$\begin{array}{lll}
s, h \vDash e = e' & \text{iff} & [\![e]\!]\ s = [\![e']\!]\ s \\
s, h \vDash e \mapsto e_1, e_2 & \text{iff} & \mathrm{dom}\, h = \{[\![e_1]\!]\ s\} \text{ and } h([\![e_1]\!]\ s) = \langle [\![e_1]\!]\ s, [\![e_2]\!]\ s\rangle \\
\\
s, h \vDash A \mathrel{-\!\!*} B & \text{iff} & \forall h_0 \perp h.\ s, h_0 \vDash A \text{ implies } s, h \circ h_0 \vDash B \\
s, h \vDash A * B & \text{iff} & \exists h_1, h_2.\ h = h_1 \circ h_2 \text{ and } s, h_1 \vDash A \text{ and } s, h_2 \vDash B \\
s, h \vDash I & \text{iff} & h = \emptyset \\
\\
s, h \vDash A \rightarrow B & \text{iff} & s, h \vDash A \text{ implies } s, h \vDash B \\
s, h \vDash A \wedge B & \text{iff} & s, h \vDash A \text{ and } s, h \vDash B \\
s, h \vDash A \vee B & \text{iff} & s, h \vDash A \text{ or } s, h \vDash B \\
s, h \vDash \top & \text{iff} & \text{always} \\
s, h \vDash \perp & \text{iff} & \text{never} \\
s, h \vDash \exists x.A & \text{iff} & \exists v \in Val.[s|x \mapsto v], h \vDash A
\end{array}$$

Figure 2: Separation logic assertion semantics (fragment)

The pseudo-derivation illustrates the essential problem: we want to apply the axiom *coin* $*$ *coin* $\rightarrow$ *choc* in Δ_a not on the original hypothesis *coin*, but on the larger context created after $-\!\!*$ introduction—yet for this we need the (in general) unsound reasoning principle marked by ???. Nor can this problem be fixed by combining the hypotheses multiplicatively. Instead, if we look more closely at what is going on in the axiomatic system, we see that axioms are hypotheses that can be invoked *anywhere*, so to speak; that is, $\Delta \vdash coin * coin \rightarrow choc$ holds for arbitrary bunches Δ. Now, this is precisely the role that *valid* assumptions play. Hence we can obtain a faithful translation of the axiomatic reasoning by replacing the axioms by a flat context $\Gamma_a = coin \rightarrow candy, coin * coin \rightarrow choc$ of valid assumptions, and proving $\Gamma_a \mid coin \vdash coin \mathrel{-\!\!*} choc$:

$$\dfrac{\dfrac{\Gamma_a \mid \emptyset_a \vdash coin * coin \rightarrow choc \quad \Gamma_a \mid coin, coin \vdash coin * coin}{\Gamma_a \mid coin, coin \vdash choc}\ \rightarrow E}{\Gamma_a \mid coin \vdash coin \mathrel{-\!\!*} choc}\ \mathrel{-\!\!*} I$$

3 Pure assertions and modal separation logic

As described in the introduction, proofs in separation logic typically require definitions of various special classes of assertions, with their own set of reasoning principles beyond entailment in ordinary BI. In [10], Reynolds defines "pure" assertions as those which, given any store, are independent of the heap. In terms of the separation logic forcing relation $s, h \vDash A$ (for reference included in Figure 2) this says that:

$$\forall s. \forall h_1, h_2.\ s, h_1 \vDash A \ \text{ iff } \ s, h_2 \vDash A \tag{$*$}$$

From the semantic definition ($*$), it is possible to prove a collection of useful validities for assertions involving pure subformulas: Reynolds gives an axiom schemata, which is shown in Figure 3. Moreover, as he notes, it is easy to syntactically define a conservative subclass of the pure assertions by restricting to those not containing I (**emp** in the usual notation of separation logic) or $\mapsto$. But this rules out many pure assertions. Trivial examples are $(x \mapsto 7) \rightarrow (x \mapsto 7)$ and $\perp \mathrel{-\!\!*} I$, but more interestingly, consider the inductive definition of a relation List α (i, j), asserting that there is a list segment from i to j representing the sequence α:

$$\begin{array}{rcl}
\text{List } \epsilon\ (i, j) & = & I \wedge i = j \\
\text{List } a \cdot \alpha\ (i, k) & = & \exists j. i \mapsto a, j * \text{List } \alpha\ (j, k)
\end{array}$$

From this definition it is possible to prove, e.g., that List $\alpha \cdot \beta$ $(i, k) \leftrightarrow \exists j.$List α $(i, j) *$ List β (j, k) is valid [10]. But if the assertion List $\alpha \cdot \beta$ $(i, k) \leftrightarrow \exists j.$List α $(i, j) *$ List β (j, k) is valid, i.e. satisfied in *every* store

$$\boxed{\begin{array}{cr} A \wedge B \to A * B & \text{when } A \text{ or } B \text{ is pure} \\ A * B \to A \wedge B & \text{when } A \text{ and } B \text{ are pure} \\ (A \wedge B) * C \leftrightarrow A \wedge (B * C) & \text{when } A \text{ is pure} \\ (A \mathrel{-\!\!*} B) \to (A \to B) & \text{when } A \text{ is pure} \\ (A \to B) \to (A \mathrel{-\!\!*} B) & \text{when } A \text{ and } B \text{ are pure} \end{array}}$$

Figure 3: Reynolds' axiom schemata for purity

$$\boxed{\begin{array}{c} \Box A \wedge B \to \Box A * B \\ \Box A * \Box B \to \Box A \wedge \Box B \\ (\Box A \wedge B) * C \leftrightarrow \Box A \wedge (B * C) \\ (\Box A \mathrel{-\!\!*} B) \to (\Box A \to B) \\ (\Box A \to \Box B) \to (\Box A \mathrel{-\!\!*} \Box B) \end{array}}$$

Figure 4: Reynolds' axioms expressed as theorems of modal BI

and heap, then it is certainly independent of the heap, i.e. pure—even though the relation List involves both I and $\mapsto$.

This last example motivates our analysis of purity as modal necessity. If an assertion A is pure according to the semantic definition $(*)$, and *if it is satisfied* by a state s, h, then it is satisfied by all states s, h', where h' is an arbitrary heap. That is, when A is pure, $s, h \vDash A$ iff $\forall h'.\ s, h' \vDash A$. Written in this way, the modal character of pure assertions is apparent. In particular, let us define the connective $\Box$ semantically, as quantifying over all heaps:

$$s, h \vDash \Box A \quad \text{iff} \quad \forall h'.\ s, h' \vDash A$$

Then $\Box$ internalizes the condition that an assertion is pure, that is, $s, h \vDash \Box A$ if and only if $s, h \vDash A$ and A is pure. An immediate consequence is that Reynolds' axiom schemata can be replaced by the one given in Figure 4, where every formula A originally marked as pure is replaced by the formula $\Box A$, without any restrictions on A.

In fact, the propositions in Figure 4 are all theorems of modal BI—natural deduction proofs are given in Appendix A. Of course, we would like to know that the natural deduction rules including $\Box$ are sound with respect to the separation logic semantics—but that is a simple induction on derivations.

4 $\Box$, !, or both?

Whereas standard BI combines IL with MILL, the modal BI we have described combines intuitionistic S4 with MILL. A natural question is then: what about combining IL with MELL, or S4 with MELL? That is, we can consider extending the system with the exponential ! of linear logic.

The exponential has been explored to some extent before in other work, particularly the issue of (the lack of) a decomposition $A \to B \cong\, !\, A \mathrel{-\!\!*} B$ (see, e.g., [5]). Here we are more interested in comparing the $\Box$ and ! modalities. Formally, they are very similar; we introduce a flat context Π of hypotheses provable from the empty multiplicative context $\emptyset_m$, and a set of three rules that look exactly like their counterparts for $\Box$ except that $\emptyset_a$ is replaced by $\emptyset_m$:

$$\frac{}{A, \Pi \mid \emptyset_m \vdash A}\ \textit{emp}$$

$$\frac{\Pi \mid \emptyset_m \vdash A}{\Pi \mid \emptyset_m \vdash\, !\, A}\ !I \qquad \frac{\Pi \mid \Delta \vdash\, !\, A \quad A, \Pi \mid \Delta'(\emptyset_m) \vdash C}{\Pi \mid \Delta'(\Delta) \vdash C}\ !E$$

Categorically, this formal resemblance reflects that $\Box$ is a comonad for the cartesian closed structure of the doubly closed category (DCC, cf. [9]), while ! is a comonad for the symmetric monidal closed structure. We can easily get a natural deduction including both comonads by simply using a three-zone judgment, $\Pi \mid \Gamma \mid \Delta \vdash A$.

As mentioned in Section 2.2, $!$ is the modality of what are usually called "theorems" in the BI literature, i.e. propositions that can be proved from $\emptyset_m$. We will call these $!$-theorems, and distinguish them from $\Box$-theorems, which are propositions that can be proved from $\emptyset_a$. It is immediate by weakening that all $\Box$-theorems are $!$-theorems (and this is what motivates the definition in the literature—it expands the class of theorems). We might then expect that $\Box A \vdash {!}\,A$ is provable. The following pseudo-derivation illustrates why it is not:

$$\dfrac{\cdot \mid \cdot \mid \Box A \vdash \Box A \qquad \dfrac{\dfrac{\cdot \mid A \mid \emptyset_m \vdash A}{\cdot \mid A \mid \emptyset_m \vdash {!}\,A}\;!I}{\cdot \mid A \mid \emptyset_a \vdash {!}\,A}\;???}{\cdot \mid \cdot \mid \Box A \vdash {!}\,A}\;\Box E$$

After eliminating the $\Box$, we can assume nothing ($\emptyset_a$) about the context, and so in particular cannot assume it is $\emptyset_m$ and introduce $!$. Instead we can only prove a weaker entailment $\Box A \vdash {!}\,A * \top$. However, we can also relate *uses* of modal hypotheses by the following proposition:

Proposition 1 *If* $A, \Pi \mid \Gamma \mid \Delta \vdash C$ *then* $\Pi \mid A, \Gamma \mid \Delta \vdash C$.

Proof: By induction on the derivation of $A, \Pi \mid \Gamma \mid \Delta \vdash C$. The only interesting case is when the derivation is an application of *emp*, since that is the only rule where Π is inspected. In that case we have $C = A$, and we get the desired conclusion by applying the rule *pure*$'$. □

Another question we can ask is whether the encoding of axioms as Γ-assumptions from Section 2.3 can be replaced by a similar encoding using Π-assumptions. It seems this should be the case for axioms of the form $A \vdash B$ (as were those in 2.3), since the following bidirectional inferences are admissible (because the implication introduction rules are invertible):

$$\begin{array}{c} \emptyset_a \vdash A \to B \\ \hline\hline A \vdash B \\ \hline\hline \emptyset_m \vdash A \mathrel{-\!\!*} B \end{array}$$

Indeed, we can prove the following:

Proposition 2 $\Pi \mid A \to B, \Gamma \mid \Delta \vdash C$ *if and only if* $A \mathrel{-\!\!*} B, \Pi \mid \Gamma \mid \Delta \vdash C$

Proof: By induction on derivations. In the forward direction, the only interesting case is an application of *pure*. In that case we make the following transformation:

$$\dfrac{}{\Pi \mid A \to B, \Gamma \mid \emptyset_a \vdash A \to B}\;\mathit{pure} \qquad \Rightarrow \qquad \dfrac{\dfrac{\dfrac{}{A \mathrel{-\!\!*} B, \Pi \mid \Gamma \mid \emptyset_m \vdash A \mathrel{-\!\!*} B}\;\mathit{emp} \qquad \dfrac{}{A \mathrel{-\!\!*} B, \Pi \mid \Gamma \mid A \vdash A}\;\mathit{id}}{A \mathrel{-\!\!*} B, \Pi \mid \Gamma \mid A \vdash B}\;{-\!\!*}E}{A \mathrel{-\!\!*} B, \Pi \mid \Gamma \mid \emptyset_a \vdash A \to B}\;{\to}I$$

In the backwards direction, the interesting case is application of the rule *emp*:

$$\dfrac{}{A \mathrel{-\!\!*} B, \Pi \mid \Gamma \mid \emptyset_m \vdash A \mathrel{-\!\!*} B}\;\mathit{emp} \qquad \Rightarrow \qquad \dfrac{\dfrac{\dfrac{}{\Pi \mid A \to B, \Gamma \mid \emptyset_a \vdash A \to B}\;\mathit{pure} \qquad \dfrac{}{\Pi \mid A \to B, \Gamma \mid A \vdash A}\;\mathit{id}}{\Pi \mid A \to B, \Gamma \mid A \vdash B}\;{\to}E}{\Pi \mid A \to B, \Gamma \mid \emptyset_m \vdash A \mathrel{-\!\!*} B}\;{-\!\!*}I$$

□

As a corollary, using the implications and logical constants, we can relate arbitrary modal assumptions as follows:

Proposition 3 $\Pi \mid A, \Gamma \mid \Delta \vdash C$ *if and only if* $\top \mathrel{-\!\!*} A, \Pi \mid \Gamma \mid \Delta \vdash C$.

Proposition 4 *$A, \Pi \mid \Gamma \mid \Delta \vdash C$ if and only if $\Pi \mid I \to A, \Gamma \mid \Delta \vdash C$.*

As for translating the modal connectives themselves, again we cannot conclude $\Box(A \to B) = !(A -\!\!* B)$, but instead only $\Box(A \to B) = !(A -\!\!* B) * \top$ (whence $\Box A = !(\top -\!\!* A) * \top$) and $!(A -\!\!* B) = \Box(A \to B) \wedge I$ (whence $!\, A = \Box(I \to A) \wedge I$).

We may now legitimately wonder whether there is any reason to have separate modalities $\Box$ and $!$, since they are interdefinable. However, we should first realize that the translation of $\Box$ to $!$ requires the presence of $\top$ and $-\!\!*$, and the translation of $!$ to $\Box$ requires I and $\to$, yet it is certainly possible to consider fragments of the logic with both $\Box$ and $!$ but without any of these other connectives or constants. Moreover, there is reason to keep $\Box$ primitive from a conceptual point of view, simply because it arises as the very natural notion of purity in separation logic, as we saw in Section 3. The same could certainly turn out to be the case for $!$ in a different domain.

References

[1] Bodil Biering, Lars Birkedal, and Noah Torp-Smith. BI hyperdoctrines and higher-order separation logic. To appear in ESOP 2005.

[2] Lars Birkedal, Noah Torp-Smith, and John Reynolds. Local reasoning about a copying garbage collector. In *POPL*, pages 220–231. 2004.

[3] J.-Y. Girard. Linear logic: Its syntax and semantics. In J.-Y. Girard, Y. Lafont, and L. Regnier, editors, *Advances in Linear Logic (Proc. of the Workshop on Linear Logic, Cornell University, June 1993)*, number 222. Cambridge University Press, 1995.

[4] S. Ishtiaq and P.W. O'Hearn. Bi as an assertion language for mutable data structures. In *POPL*, pages 14–26, 2001.

[5] Peter O'Hearn. On bunched typing. *Journal of Functional Programming*, 13(4):747–796, 2002.

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

[7] Frank Pfenning and Rowan Davies. A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science*, 11(4):511–540, 2001.

[8] David Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002.

[9] David Pym, Peter O'Hearn, and Hongseok Yang. Possible worlds and resources: The semantics of BI. *Theoretical Computer Science*, 315(1):257–305, 2004.

[10] John Reynolds. Separation logic: a logic for shared mutable data structures. In *LICS*, pages 55–74, 2002.

[11] Hongseok Yang. *Local Reasoning for Stateful Programs.* Ph. D dissertation, University of Illinois, Urbana-Champaign, Illinois, July 2001.

[12] Hongseok Yang. Relational separation logic, March 2004. Submitted to Theoretical Computer Science.

A Derivations for Reynolds' axiom schemata

In these derivations we omit applications of $\equiv$, and some initial steps of eliminating connectives.

$\boxed{\Box A \wedge B \vdash \Box A * B}$

$$\dfrac{\cdot \mid \Box A \vdash \Box A \qquad \dfrac{\dfrac{A \mid \emptyset_a \vdash A}{A \mid \emptyset_m \vdash \Box A}\,\Box I' \qquad A \mid B \vdash B}{A \mid B \vdash \Box A * B}\,{*I}}{\cdot \mid \Box A; B \vdash \Box A * B}\,\Box E$$

$\boxed{\Box A * \Box B \vdash \Box A \wedge \Box B}$

$$\dfrac{\dfrac{\cdot \mid \Box A \vdash \Box A \qquad \dfrac{A \mid \emptyset_a \vdash A}{A \mid \emptyset_a, \Box B \vdash \Box A}\,\Box I'}{\cdot \mid \Box A, \Box B \vdash \Box A}\,\Box E \qquad \dfrac{\cdot \mid \Box B \vdash \Box B \qquad \dfrac{B \mid \emptyset_a \vdash B}{B \mid \Box A, \emptyset_a \vdash \Box B}\,\Box I'}{\cdot \mid \Box A, \Box B \vdash \Box B}\,\Box E}{\cdot \mid \Box A, \Box B \vdash \Box A \wedge \Box B}\,\wedge I'$$

$\boxed{(\Box A \wedge B) * C \vdash \Box A \wedge (B * C)}$

$$\dfrac{\cdot \mid \Box A \vdash \Box A \qquad \dfrac{\dfrac{A \mid \emptyset_a \vdash A}{A \mid B, C \vdash \Box A}\,\Box I'}{A \mid B, C \vdash \Box A \wedge (B * C)}\,\wedge I}{\cdot \mid (\Box A; B), C \vdash \Box A \wedge (B * C)}\,\Box E$$

$\boxed{\Box A \wedge (B * C) \vdash (\Box A \wedge B) * C}$

$$\dfrac{\cdot \mid \Box A \vdash \Box A \qquad \dfrac{A \mid B * C \vdash B * C \qquad \dfrac{\dfrac{\dfrac{A \mid \emptyset_a \vdash A}{A \mid \emptyset_a \vdash \Box A}\,\Box I \qquad A \mid B \vdash B}{A \mid B \vdash \Box A \wedge B}\,\wedge I \qquad A \mid C \vdash C}{A \mid B, C \vdash (\Box A \wedge B) * C}\,{*I}}{A \mid B * C \vdash (\Box A \wedge B) * C}\,{*E}}{\cdot \mid \Box A; (B * C) \vdash (\Box A \wedge B) * C}\,\Box E$$

$\boxed{\Box A \mathrel{-\!\!*} B \vdash \Box A \to B}$

$$\dfrac{\dfrac{\cdot \mid \Box A \vdash \Box A \qquad \dfrac{A \mid \Box A \mathrel{-\!\!*} B \vdash \Box A \mathrel{-\!\!*} B \qquad \dfrac{A \mid \emptyset_a \vdash A}{A \mid \emptyset_m \vdash \Box A}\,\Box I'}{A \mid \Box A \mathrel{-\!\!*} B \vdash B}\,{-\!\!*E}}{\cdot \mid \Box A \mathrel{-\!\!*} B; \Box A \vdash B}\,\Box E}{\cdot \mid \Box A \mathrel{-\!\!*} B \vdash \Box A \to B}\,{\to I}$$

$\boxed{\Box A \to \Box B \vdash \Box A \mathrel{-\!\!*} \Box B}$

$$\dfrac{\cdot \mid \Box A \vdash \Box A \qquad \dfrac{\dfrac{A \mid \Box A \to \Box B \vdash \Box A \to \Box B \qquad \dfrac{A \mid \emptyset_a \vdash A}{A \mid \emptyset_a \vdash \Box A}\;\Box I}{A \mid \Box A \to \Box B \vdash \Box B}\;{\to}E \qquad \dfrac{A, B \mid \emptyset_a \vdash B}{A, B \mid \emptyset_a, \emptyset_a \vdash \Box B}\;\Box I'}{A \mid \Box A \to \Box B, \emptyset_a \vdash \Box B}\;\Box E}{\dfrac{\cdot \mid \Box A \to \Box B, \Box A \vdash \Box B}{\cdot \mid \Box A \to \Box B \vdash \Box A \mathrel{-\!\!*} \Box B}\;{\mathrel{-\!\!*}}I}\;\Box E$$