Towards a Cut-free Sequent Calculus for Boolean BI

Sungwoo Park and Jonghyun Park
Pohang University of Science and Technology
Republic of Korea
{gla,parjong}@postech.ac.kr*

The logic of bunched implications (BI) of O'Hearn and Pym [5] is a substructural logic which freely combines additive connectives $\supset$, $\wedge$, $\vee$ from propositional logic and multiplicative connectives $-\!\!\star$, $\star$ from linear logic. Because of its concise yet rich representation of states of resources, BI is regarded as a logic suitable for reasoning about resources. For example, by building a model for BI based on a monoid of heaps, we obtain separation logic [7] which extends Hoare logic to facilitate reasoning about imperative programs manipulating heap memory.

Depending on its interpretation of additive connectives, BI comes with two flavors: intuitionistic BI and boolean BI. Intuitionistic BI interprets additive connectives intuitionistically, while boolean BI interprets additive connectives classically and admits such principles as the law of excluded middle. Both logics interpret multiplicative connectives intuitionistically and do not introduce multiplicative falsity or negation.

Intuitionistic BI has a well-developed proof theory. It has a natural deduction system with the normalization property and also a cut-free sequent calculus. Because free combinations of additive connectives and multiplicative connectives are allowed, contexts in such proof-theoretic formulations are not unordered sets as usual, but bunches: trees whose internal nodes indicate whether subtrees are combined additively or multiplicatively. For example, the sequent calculus uses a sequent of the form $\Gamma \longrightarrow A$ where Γ denotes a bunch and A is a formula.

For boolean BI, however, no such well-behaved proof theory exists. Usually a naive extension of intuitionistic BI with the double negation principle is taken as the proof-theoretic definition of boolean BI, but no equivalent cut-free sequent calculus has been reported yet. Following the style of multi-conclusioned sequent calculi, Pym [6] considers sequents of the form $\Gamma \longrightarrow \Gamma$ (where both sides use bunches), but it is shown that the cut elimination property fails in the resultant sequent calculus. As such, previous work on boolean BI has mostly focused on its Kripke semantics and Hilbert-style system [3, 4] or a different style of proof theory based on display logic [1].

Our goal is to develop a proof-theoretic formulation for building an automated theorem prover for boolean BI (and ultimately for separation logic). Ideally a cut-free sequent calculus for boolean BI would be the best candidate, but such a sequent calculus is unlikely to exist, as already observed by Brotherston [2]. Following the conjecture that such a sequent calculus does not exist, we aim to develop a cut-free sequent calculus for another variant of BI that may be incompatible with boolean BI (in the sense that it proves some non-theorems in boolean BI and fails to prove some theorems in boolean BI), but still interprets all additive connectives classically and all multiplicative connectives intuitionistically. By identifying such a variant of boolean BI for which a cut-free sequent calculus exists, we may also be able to better understand why boolean BI is unlikely to have a well-behaved proof theory.

The main obstacle is to identify a form of sequent such that additive connectives are interpreted classically (thereby admitting the law of excluded middle) while multiplicative connectives are interpreted intuitionistically. We find that sequents of the form $\Gamma \longrightarrow A$ or $\Gamma \longrightarrow \Gamma$

*This work was supported by the Engineering Research Center of Excellence Program of Korea Ministry of Education, Science and Technology(MEST)/National Research Foundation of Korea(NRF) (Grant 2010-0001726).

are inadequate, and introduce a new form of sequent, called *world sequent*, which expresses logical inconsistency in a tree-like structure of *worlds*. In order to interpret additive connectives classically, each world maintains not only true statements but also false statements.

Formally we define world sequents as follows:

$$\begin{array}{llll}
\text{formula} & A, B, C, \cdots & ::= & P \mid \top \mid \mathsf{I} \mid \bot \mid A \supset A \mid A \wedge A \mid A -\!\!\star A \\
 & & & \mid A \star A \mid A \vee A \mid \neg A \\
\text{boolean bunches} & \Delta & ::= & A \mid \emptyset_{\mathsf{a}} \mid \emptyset_{\mathsf{m}} \mid \Delta ; \Delta \mid W, W \\
\text{falsehood context} & \Psi & ::= & \cdot \mid \Psi ; A \\
\text{world sequent} & W & = & \Delta \longrightarrow_{\mathsf{B}} \Psi
\end{array}$$

A world sequent $\Delta \longrightarrow_{\mathsf{B}} \Psi$ means that a boolean bunch Δ and a falsehood context Ψ in a world lead to logical inconsistency. A boolean bunch Δ consists of true statements about a world, and a falsehood context Ψ consists of false statements about a world. (We do not take the multi-conclusioned view when interpreting Ψ.) The additive zero $\emptyset_{\mathsf{a}}$ is a boolean bunch that is valid at every world, and the multiplicative zero $\emptyset_{\mathsf{m}}$ is a boolean bunch that is valid at an empty world. An additive boolean bunch $\Delta_1 ; \Delta_2$ describes a world where both Δ_1 and Δ_2 are valid. A multiplicative boolean bunch W_1, W_2 means that the current world can be divided into two adjacent worlds for which world sequents W_1 and W_2 hold, respectively. A world sequent $\Delta \longrightarrow_{\mathsf{B}} \Psi$ is provable if both $A \in \Delta$ and $A \in \Psi$ hold for some formula A, or if it contains another such world sequent. We use conventional precedence rules for logical connectives: $\neg > \wedge, \star > \vee > \supset, -\!\!\star$.

We formulate a variant of boolean BI with a sequent calculus based on world sequents, in which additive connectives are interpreted classically and multiplicative connectives are interpreted intuitionistically. We assume that additive boolean bunches satisfy commutative monoid equations for the additive zero $\emptyset_{\mathsf{a}}$ and the binary operation ;. That is, the following equivalence relations hold:

$$\begin{array}{rcl}
\Delta ; \emptyset_{\mathsf{a}} & \equiv & \emptyset_{\mathsf{a}} ; \Delta \quad \equiv \quad \Delta \\
\Delta ; \Delta' & \equiv & \Delta' ; \Delta \\
\Delta ; (\Delta' ; \Delta'') & \equiv & (\Delta ; \Delta') ; \Delta''
\end{array}$$

For multiplicative boolean bunches, however, we assume no equivalence relations that disturb the tree-like structure of worlds. In particular, we do not permit commutativity between world sequents, associativity involving multiplicative boolean bunches, and equivalence relations exploiting $\emptyset_{\mathsf{m}} \longrightarrow_{\mathsf{B}} \cdot$ as an identity world sequent:[1]

$$\begin{array}{rcl}
W, W' & \not\equiv & W', W \\
W, (W', W'' \longrightarrow_{\mathsf{B}} \cdot) & \not\equiv & (W, W' \longrightarrow_{\mathsf{B}} \cdot), W'' \\
(A \longrightarrow_{\mathsf{B}} \cdot), (\emptyset_{\mathsf{m}} \longrightarrow_{\mathsf{B}} \cdot) & \not\equiv & A \\
W, (\emptyset_{\mathsf{m}} \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} \cdot & \not\equiv & W
\end{array}$$

Since commutativity and associativity do not exist for multiplicative boolean bunches, every world has a unique adjacent world and there is an ordering between two adjacent worlds.

Figure 1 shows the sequent calculus based on world sequents. We use the following definitions of world contexts and bunch contexts:

$$\begin{array}{lcll}
\text{world contexts} & \omega & ::= & [\,] \mid \delta \longrightarrow_{\mathsf{B}} \Psi \\
\text{bunch contexts} & \delta & ::= & \omega, W \mid \delta ; \Delta
\end{array}$$

A world context ω is a world sequent with a hole in it; by filling the hole with a world sequent W, we produce a world sequent $\omega[W]$. A bunch context δ is a boolean bunch with a hole in it;

[1] There is no associativity for the binary operation , because the set of world sequents is not closed.

$$\dfrac{A \text{ atomic}}{\omega[A \longrightarrow_{\mathsf{B}} A]}\ \mathit{Init} \qquad \dfrac{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; \Delta' \longrightarrow_{\mathsf{B}} \Psi]}\ \mathsf{W} \qquad \dfrac{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi; A]}\ \mathsf{W}'$$

$$\dfrac{\omega[\Delta; \Delta'; \Delta' \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; \Delta' \longrightarrow_{\mathsf{B}} \Psi]}\ \mathsf{C} \qquad \dfrac{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi; A; A]}{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi; A]}\ \mathsf{C}'$$

$$\dfrac{}{\omega[\bot \longrightarrow_{\mathsf{B}} \cdot]}\ \bot L \qquad \dfrac{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi; \bot]}\ \bot R \qquad \dfrac{\omega[\Delta \longrightarrow_{\mathsf{B}} A; \Psi]}{\omega[\Delta; \neg A \longrightarrow_{\mathsf{B}} \Psi]}\ \neg L \qquad \dfrac{\omega[\Delta; A \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta \longrightarrow_{\mathsf{B}} \neg A; \Psi]}\ \neg R$$

$$\dfrac{\omega[\Delta; A; B \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; A \wedge B \longrightarrow_{\mathsf{B}} \Psi]}\ \wedge L \qquad \dfrac{\omega[\Delta \longrightarrow_{\mathsf{B}} A; \Psi] \quad \omega[\Delta \longrightarrow_{\mathsf{B}} B; \Psi']}{\omega[\Delta \longrightarrow_{\mathsf{B}} A \wedge B; \Psi; \Psi']}\ \wedge R$$

$$\dfrac{\omega[\Delta; \emptyset_{\mathsf{m}} \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; \mathsf{I} \longrightarrow_{\mathsf{B}} \Psi]}\ \mathsf{I}L \qquad \dfrac{}{\omega[\emptyset_{\mathsf{m}} \longrightarrow_{\mathsf{B}} \mathsf{I}]}\ \mathsf{I}R$$

$$\dfrac{\omega[(\Delta \longrightarrow_{\mathsf{B}} \Psi), (\Delta' \longrightarrow_{\mathsf{B}} \Psi'; A); \Delta'' \longrightarrow_{\mathsf{B}} \Psi''] \quad \omega[B; \Delta'' \longrightarrow_{\mathsf{B}} \Psi'']}{\omega[(\Delta; A \mathrel{-\!\!\star} B \longrightarrow_{\mathsf{B}} \Psi), (\Delta' \longrightarrow_{\mathsf{B}} \Psi'); \Delta'' \longrightarrow_{\mathsf{B}} \Psi'']}\ \mathrel{-\!\!\star} L$$

$$\dfrac{\omega[(\Delta \longrightarrow_{\mathsf{B}} \Psi), (\Delta'; A \longrightarrow_{\mathsf{B}} \Psi'); \Delta'' \longrightarrow_{\mathsf{B}} \Psi''; B]}{\omega[(\Delta \longrightarrow_{\mathsf{B}} \Psi; A \mathrel{-\!\!\star} B), (\Delta' \longrightarrow_{\mathsf{B}} \Psi'); \Delta'' \longrightarrow_{\mathsf{B}} \Psi'']}\ \mathrel{-\!\!\star} R$$

$$\dfrac{\omega[\Delta; (A \longrightarrow_{\mathsf{B}} \cdot), (B \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} \Psi]}{\omega[\Delta; A \star B \longrightarrow_{\mathsf{B}} \Psi]}\ \star L$$

$$\dfrac{\omega[\Delta''; (\Delta \longrightarrow_{\mathsf{B}} \Psi; A), (\Delta' \longrightarrow_{\mathsf{B}} \Psi') \longrightarrow_{\mathsf{B}} \Psi''] \quad \omega[\Delta''; (\Delta \longrightarrow_{\mathsf{B}} \Psi), (\Delta' \longrightarrow_{\mathsf{B}} \Psi'; B) \longrightarrow_{\mathsf{B}} \Psi'']}{\omega[\Delta''; (\Delta \longrightarrow_{\mathsf{B}} \Psi), (\Delta' \longrightarrow_{\mathsf{B}} \Psi') \longrightarrow_{\mathsf{B}} A \star B; \Psi'']}\ \star R$$

Figure 1: Sequent calculus

by filling the hole with a world sequent W, we produce a boolean bunch $\delta[W]$. We define $\top$ as $\neg\bot$, $A \supset B$ as $\neg(A \wedge \neg B)$, and $A \vee B$ as $\neg(\neg A \wedge \neg B)$.

To informally explain the rules for multiplicative connectives, we introduce new notations. We use w to denote worlds and write (w, w') for a world that is divided into a left subworld w and a right subworld w'. We write $w \bowtie w'$ to mean that the left world w and the right world w' are adjacent to each other. We write $w \models A$ to mean that A is true at world w and $w \not\models A$ that A is false at world w. We use $\Rightarrow$ for logical implication.

The rules $\mathrel{-\!\!\star} L$ and $\mathrel{-\!\!\star} R$ are based on the following interpretation of the multiplicative implication $\mathrel{-\!\!\star}$:

- $A \mathrel{-\!\!\star} B$ is true at world w if and only if $\forall w', w \bowtie w' \Rightarrow w' \models A \Rightarrow (w, w') \models B$.
- $A \mathrel{-\!\!\star} B$ is false at world w if and only if $\exists w', w \bowtie w'$ and $w' \models A$ and $(w, w') \not\models B$.

The rules $\mathrel{-\!\!\star} L$ and $\mathrel{-\!\!\star} R$ additionally exploit the property that every world has a unique adjacent world. Note that the truth of $A \mathrel{-\!\!\star} B$ assumes the truth of A at the right adjacent world only, which suggests that we may introduce another multiplicative implication that symmetrically makes an assumption about the left adjacent world. We do not consider such a multiplicative implication here because its development is completely analogous.

The rules $\star L$ and $\star R$ are based on the following interpretation of the multiplicative conjunction $\star$:

- $A \star B$ is true at world w if and only if $\exists w_1, \exists w_2, w = (w_1, w_2)$ and $w_1 \models A$ and $w_2 \models B$.

- $A \star B$ is false at world w if and only if $\forall w_1, \forall w_2, w = (w_1, w_2) \Rightarrow (w_1 \not\models A$ or $w_2 \not\models B)$.

The rule $\star L$ is the only rule that creates new world sequents (when read in a bottom-up way).

To prove a formula A, we build a proof of a sequent of the following form:

$$\cdots(((\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}} A), (\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} \cdot), (\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} \cdot)\cdots$$

This sequent reflects the property that every world, including the world where we assume the falsehood of A, has a unique adjacent world. It also reflects the property that the multiplicative implication $-\!\!\star$ introduces true statements at right adjacent worlds only. As an example, we prove $A -\!\!\star B \vee A -\!\!\star \neg B$ as follows:

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{(\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}}), (\emptyset_{\mathsf{a}}; A; A \longrightarrow_{\mathsf{B}} \cdot); B \longrightarrow_{\mathsf{B}} B}\;\mathit{Init}}{(\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}}), (\emptyset_{\mathsf{a}}; A; A \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} B; \neg B}\;\neg R}{(\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}} A -\!\!\star \neg B), (\emptyset_{\mathsf{a}}; A \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} B}\;-\!\!\star L}{(\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}} A -\!\!\star B; A -\!\!\star \neg B), (\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} \cdot}\;-\!\!\star L}{(\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}} A -\!\!\star B \vee A -\!\!\star \neg B), (\emptyset_{\mathsf{a}} \longrightarrow_{\mathsf{B}} \cdot) \longrightarrow_{\mathsf{B}} \cdot}\;\vee R \text{ (derived rule)}$$

Incidentally $A -\!\!\star B \vee A -\!\!\star \neg B$ is not provable in boolean BI because the adjacent world assumed in $A -\!\!\star B$ is not necessarily identical to the adjacent world assumed in $A -\!\!\star \neg B$.

We state the cut elimination property as follows:

Theorem (Cut elimination). If $\omega[\Delta \longrightarrow_{\mathsf{B}} C; \Psi]$ and $\omega[\Delta; C \longrightarrow_{\mathsf{B}} \Psi]$, then $\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi]$.

In our sequent calculus, the cut elimination property holds only because, unlike in boolean BI, we permit no equivalence relations that disturb the tree-like structure of worlds. To be specific, the proofs of $\omega[\Delta \longrightarrow_{\mathsf{B}} C; \Psi]$ and $\omega[\Delta; C \longrightarrow_{\mathsf{B}} \Psi]$ can combine in a very complex way, and if we permit any equivalence relation that disturbs the tree-like structure of worlds, it becomes impossible to derive a proof of $\omega[\Delta \longrightarrow_{\mathsf{B}} \Psi]$. The lack of such equivalence relations is concisely expressed by unprovability of the following formulas:

$$\begin{array}{l} A \star B \supset B \star A \\ A \star (B \star C) \supset (A \star B) \star C \\ (A \star B) \star C \supset A \star (B \star C) \\ A \star \mathsf{I} \supset A \\ A \supset A \star \mathsf{I} \end{array}$$

This observation strongly suggests that there is no cut-free sequent calculus for boolean BI, which takes all these structural equivalence relations for granted.

References

[1] James Brotherston. A cut-free proof theory for boolean BI (via display logic). Technical Report DTR09-13, Imperial College London, 2009.

[2] James Brotherston. A unified display proof theory for bunched logic. In *Proceedings of MFPS-26*, 2010. To appear.

[3] Didier Galmiche and Dominique Larchey-Wendling. Expressivity properties of boolean BI through relational models. In *Proceedings of FSTTCS*, pages 357–368, 2006.

[4] Dominique Larchey-Wendling and Didier Galmiche. Exploring the relation between intuitionistic BI and boolean BI: an unexpected embedding. *Mathematical Structures in Computer Science*, 19(3):435–500, 2009.

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

[6] David Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications.* Kluwer Academic Publishers, 2002.

[7] John C. Reynolds. Separation logic: A logic for shared mutable data structures. In *Proceedings of the 19th IEEE Symposium on Logic in Computer Science*, pages 55–74, 2002.