Sub-classical Boolean bunched logics and the meaning of par

James Brotherston (1) and Jules Villard (2)

(1) University College London

(2) Imperial College London /Facebook

CSL, TU Berlin, Sept 2015

Bunched logics

- Bunched logics extend classical or intuitionistic logic with various multiplicative connectives.

Bunched logics

- Bunched logics extend classical or intuitionistic logic with various multiplicative connectives.
- Formulas can be understood as sets of "worlds" (often "resources") in an underlying model.

Bunched logics

- Bunched logics extend classical or intuitionistic logic with various multiplicative connectives.
- Formulas can be understood as sets of "worlds" (often "resources") in an underlying model.
- The multiplicatives generally denote composition operations on these worlds.

Bunched logics

- Bunched logics extend classical or intuitionistic logic with various multiplicative connectives.
- Formulas can be understood as sets of "worlds" (often "resources") in an underlying model.
- The multiplicatives generally denote composition operations on these worlds.
- Bunched logics are closely related to relevant logics and can also be seen as (special) modal logics.

BBI, *proof-theoretically*

Provability in the bunched logic BBI is given by extending classical logic by

$$A * B \vdash B * A \qquad A * (B * C) \vdash (A * B) * C$$

$$A \vdash A * \top^* \qquad A * \top^* \vdash A$$

$$\frac{A_1 \vdash B_1 \quad A_2 \vdash B_2}{A_1 * A_2 \vdash B_1 * B_2} \qquad \frac{A * B \vdash C}{A \vdash B \mathrel{-\!\!*} C} \qquad \frac{A \vdash B \mathrel{-\!\!*} C}{A * B \vdash C}$$

(i.e., multiplicative intuitionistic linear logic.)

BBI, *semantically (1)*

A BBI-model is given by $\langle W, \circ, E \rangle$, where

- W is a set (of "worlds"),

BBI, *semantically (1)*

A BBI-model is given by $\langle W, \circ, E \rangle$, where

- W is a set (of "worlds"),
- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and

BBI, *semantically (1)*

A BBI-model is given by $\langle W, \circ, E \rangle$, where

- W is a set (of "worlds"),
- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- the set of units $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$.

BBI, *semantically (1)*

A BBI-model is given by $\langle W, \circ, E \rangle$, where

- W is a set (of "worlds"),
- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- the set of units $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$.

Separation logic is based on heap models, e.g. $\langle H, \circ, \{e\} \rangle$, where

BBI, *semantically (1)*

A BBI-model is given by $\langle W, \circ, E \rangle$, where

- W is a set (of "worlds"),
- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- the set of units $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$.

Separation logic is based on heap models, e.g. $\langle H, \circ, \{e\} \rangle$, where

- H is the set of heaps, i.e. finite partial maps $\mathrm{Loc} \rightharpoonup_{\mathrm{fin}} \mathrm{Val}$,

BBI, *semantically (1)*

A BBI-model is given by $\langle W, \circ, E\rangle$, where

- W is a set (of "worlds"),
- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- the set of units $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$.

Separation logic is based on heap models, e.g. $\langle H, \circ, \{e\}\rangle$, where

- H is the set of heaps, i.e. finite partial maps $\mathrm{Loc} \rightharpoonup_{\mathrm{fin}} \mathrm{Val}$,
- $\circ$ is union of domain-disjoint heaps, and

BBI, *semantically (1)*

A BBI-model is given by $\langle W, \circ, E \rangle$, where

- W is a set (of "worlds"),
- $\circ : W \times W \to \mathcal{P}(W)$ is associative and commutative (we extend $\circ$ pointwise to sets), and
- the set of units $E \subseteq W$ satisfies $w \circ E = \{w\}$ for all $w \in W$.

Separation logic is based on heap models, e.g. $\langle H, \circ, \{e\} \rangle$, where

- H is the set of heaps, i.e. finite partial maps $\mathrm{Loc} \rightharpoonup_{\mathrm{fin}} \mathrm{Val}$,
- $\circ$ is union of domain-disjoint heaps, and
- e is the empty map.

BBI, *semantically (2)*

Semantics of formula A w.r.t. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by forcing relation $w \models_\rho A$:

BBI, *semantically (2)*

Semantics of formula A w.r.t. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by forcing relation $w \models_\rho A$:

$$w \models_\rho P \quad \Leftrightarrow \quad w \in \rho(P)$$

BBI, *semantically (2)*

Semantics of formula A w.r.t. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by forcing relation $w \models_\rho A$:

$$\begin{array}{rcl} w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\ \vdots & & \\ w \models_\rho \top^* & \Leftrightarrow & w \in E \end{array}$$

BBI, *semantically (2)*

Semantics of formula A w.r.t. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by forcing relation $w \models_\rho A$:

$$\begin{array}{rcl} w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\ \vdots & & \\ w \models_\rho \top^* & \Leftrightarrow & w \in E \\ w \models_\rho A_1 * A_2 & \Leftrightarrow & w \in w_1 \circ w_2 \text{ and } w_1 \models_\rho A_1 \text{ and } w_2 \models_\rho A_2 \end{array}$$

BBI, *semantically (2)*

Semantics of formula A w.r.t. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by forcing relation $w \models_\rho A$:

$$
\begin{array}{rcl}
w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\
\vdots & & \\
w \models_\rho \top^* & \Leftrightarrow & w \in E \\
w \models_\rho A_1 * A_2 & \Leftrightarrow & w \in w_1 \circ w_2 \text{ and } w_1 \models_\rho A_1 \text{ and } w_2 \models_\rho A_2 \\
w \models_\rho A_1 \mathrel{-\!\!*} A_2 & \Leftrightarrow & \forall w', w'' \in W. \text{ if } w'' \in w \circ w' \text{ and } w' \models_\rho A_1 \\
 & & \text{then } w'' \models_\rho A_2
\end{array}
$$

BBI, *semantically (2)*

Semantics of formula A w.r.t. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by forcing relation $w \models_\rho A$:

$$\begin{array}{rcl}
w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\
\vdots & & \\
w \models_\rho \top^* & \Leftrightarrow & w \in E \\
w \models_\rho A_1 * A_2 & \Leftrightarrow & w \in w_1 \circ w_2 \text{ and } w_1 \models_\rho A_1 \text{ and } w_2 \models_\rho A_2 \\
w \models_\rho A_1 \mathrel{-\!\!*} A_2 & \Leftrightarrow & \forall w', w'' \in W.\ \text{if } w'' \in w \circ w' \text{ and } w' \models_\rho A_1 \\
 & & \text{then } w'' \models_\rho A_2
\end{array}$$

A is valid in M iff $w \models_\rho A$ for all ρ and $w \in W$.

BBI, *semantically (2)*

Semantics of formula A w.r.t. BBI-model $M = \langle W, \circ, E \rangle$, valuation ρ, and $w \in W$ given by forcing relation $w \models_\rho A$:

$$
\begin{array}{rcl}
w \models_\rho P & \Leftrightarrow & w \in \rho(P) \\
\vdots & & \\
w \models_\rho \top^* & \Leftrightarrow & w \in E \\
w \models_\rho A_1 * A_2 & \Leftrightarrow & w \in w_1 \circ w_2 \text{ and } w_1 \models_\rho A_1 \text{ and } w_2 \models_\rho A_2 \\
w \models_\rho A_1 \mathrel{-\!\!*} A_2 & \Leftrightarrow & \forall w', w'' \in W.\ \text{if } w'' \in w \circ w' \text{ and } w' \models_\rho A_1 \\
& & \text{then } w'' \models_\rho A_2
\end{array}
$$

A is valid in M iff $w \models_\rho A$ for all ρ and $w \in W$.

Theorem (Galmiche and Larchey-Wendling, 2006)

A formula is BBI-*provable iff it is valid in all* BBI-*models.*

Motivating question

- $*$ is understood as a resource-sensitive version of conjunction (with $-\!\!*$ its adjoint implication).

Motivating question

- $*$ is understood as a resource-sensitive version of conjunction (with $-\!\!*$ its adjoint implication).
- Might there be a resource-sensitive version of disjunction?

Motivating question

- $*$ is understood as a resource-sensitive version of conjunction (with $-\!\!*$ its adjoint implication).
- Might there be a resource-sensitive version of disjunction?
- If so, then
  - how should we interpret it?

Motivating question

- $*$ is understood as a resource-sensitive version of conjunction (with $-\!\!*$ its adjoint implication).
- Might there be a resource-sensitive version of disjunction?
- If so, then
  - how should we interpret it?
  - what logical properties ought it to have? and

Motivating question

- $*$ is understood as a resource-sensitive version of conjunction (with $-\!\!*$ its adjoint implication).
- Might there be a resource-sensitive version of disjunction?
- If so, then
  - how should we interpret it?
  - what logical properties ought it to have? and
  - can we find natural models in which it makes sense?

First answer: Classical BI

- Classical BI (CBI) is classical logic plus *classical* multiplicative linear logic.

First answer: Classical BI

- Classical BI (CBI) is classical logic plus *classical* multiplicative linear logic.
- CBI-models are given by $\langle W, \circ, E, U \rangle$, where $\langle W, \circ, E \rangle$ is a BBI-model, and $U \subseteq W$ satisfies:

First answer: Classical BI

- Classical BI (CBI) is classical logic plus *classical* multiplicative linear logic.
- CBI-models are given by $\langle W, \circ, E, U\rangle$, where $\langle W, \circ, E\rangle$ is a BBI-model, and $U \subseteq W$ satisfies:

$$\forall w \in W.\ \exists\ \textit{unique}\ {-w} \in W.\ (w \circ -w) \cap U \neq \emptyset$$

First answer: Classical BI

- Classical BI (CBI) is classical logic plus *classical* multiplicative linear logic.
- CBI-models are given by $\langle W, \circ, E, U \rangle$, where $\langle W, \circ, E \rangle$ is a BBI-model, and $U \subseteq W$ satisfies:

$$\forall w \in W.\ \exists\ \textit{unique}\ -w \in W.\ (w \circ -w) \cap U \neq \emptyset$$

- That is, every world w has a unique "dual" $-w$. Models include Abelian groups, bit arrays, regular languages, etc.

First answer: Classical BI

- Classical BI (CBI) is classical logic plus *classical* multiplicative linear logic.
- CBI-models are given by $\langle W, \circ, E, U \rangle$, where $\langle W, \circ, E \rangle$ is a BBI-model, and $U \subseteq W$ satisfies:

$$\forall w \in W.\ \exists\ \mathit{unique}\ {-w} \in W.\ (w \circ -w) \cap U \neq \emptyset$$

- That is, every world w has a unique "dual" $-w$. Models include Abelian groups, bit arrays, regular languages, etc.
- Negation defined by $w \models {\sim}A \Leftrightarrow -w \not\models A$.

First answer: Classical BI

- Classical BI (CBI) is classical logic plus *classical* multiplicative linear logic.
- CBI-models are given by $\langle W, \circ, E, U \rangle$, where $\langle W, \circ, E \rangle$ is a BBI-model, and $U \subseteq W$ satisfies:

$$\forall w \in W.\ \exists\ \mathit{unique}\ {-w} \in W.\ (w \circ -w) \cap U \neq \emptyset$$

- That is, every world w has a unique "dual" $-w$. Models include Abelian groups, bit arrays, regular languages, etc.
- Negation defined by $w \models \sim A \Leftrightarrow -w \not\models A$.
- We have $\sim\sim A \equiv A$ and $A \mathbin{\overset{*}{\vee}} B =_{\mathrm{def}} \sim(\sim A * \sim B)$.

CBI *is (often) too strong*

- Many BBI-models cannot be made into CBI-models, because worlds in those models don't have natural duals.

CBI *is (often) too strong*

- Many BBI-models cannot be made into CBI-models, because worlds in those models don't have natural duals.
- There is no $U \subseteq \mathbb{N}$ such that $\langle \mathbb{N}, +, \{0\}, U \rangle$ is a CBI-model.

CBI *is (often) too strong*

- Many BBI-models cannot be made into CBI-models, because worlds in those models don't have natural duals.
- There is no $U \subseteq \mathbb{N}$ such that $\langle \mathbb{N}, +, \{0\}, U \rangle$ is a CBI-model.
- Similarly, for the heap model, there is no $U \subseteq H$ such that $\langle H, \circ, \{e\}, U \rangle$ is a CBI-model.

BiBBI: *Sub-classical* BBI

We add multiplicative disjunction $\mathbin{\overset{*}{\vee}}$, coimplication $\setminus^*$ and (maybe) falsum $\bot^*$ to BBI via the following rules:

BiBBI: *Sub-classical* BBI

We add multiplicative disjunction $\mathbin{\overset{*}{\vee}}$, coimplication $\setminus^*$ and (maybe) falsum $\bot^*$ to BBI via the following rules:

Monotonicity:

$$\frac{A_1 \vdash B_1 \quad A_2 \vdash B_2}{A_1 \mathbin{\overset{*}{\vee}} A_2 \vdash B_1 \mathbin{\overset{*}{\vee}} B_2}$$

Residuation:

$$\frac{A \vdash B \mathbin{\overset{*}{\vee}} C}{A \setminus^* B \vdash C}$$

Commutativity:

$$A \mathbin{\overset{*}{\vee}} B \vdash B \mathbin{\overset{*}{\vee}} A$$

(Other principles are considered optional!)

Semantics of BiBBI

A basic BiBBI-model is given by $\langle W, \circ, E, \triangledown, U \rangle$, where

- $\langle W, \circ, E \rangle$ is a BBI-model,

Semantics of BiBBI

A basic BiBBI-model is given by $\langle W, \circ, E, \triangledown, U \rangle$, where

- $\langle W, \circ, E \rangle$ is a BBI-model,
- $\triangledown \colon W \times W \to \mathcal{P}(W)$ (extended pointwise to sets), and

Semantics of BiBBI

A basic BiBBI-model is given by $\langle W, \circ, E, \triangledown, U \rangle$, where

- $\langle W, \circ, E \rangle$ is a BBI-model,
- $\triangledown \colon W \times W \to \mathcal{P}(W)$ (extended pointwise to sets), and
- $U \subseteq W$.

Semantics of BiBBI

A basic BiBBI-model is given by $\langle W, \circ, E, \triangledown, U \rangle$, where

- $\langle W, \circ, E \rangle$ is a BBI-model,
- $\triangledown \colon W \times W \to \mathcal{P}(W)$ (extended pointwise to sets), and
- $U \subseteq W$.

Forcing relation for new connectives:

$$
\begin{aligned}
w \models_\rho A \overset{*}{\vee} B \quad \Leftrightarrow \quad & \forall w_1, w_2 \in W.\ w \in w_1 \triangledown w_2 \text{ implies} \\
& w_1 \models_\rho A \text{ or } w_2 \models_\rho B
\end{aligned}
$$

Semantics of BiBBI

A basic BiBBI-model is given by $\langle W, \circ, E, \triangledown, U \rangle$, where

- $\langle W, \circ, E \rangle$ is a BBI-model,
- $\triangledown \colon W \times W \to \mathcal{P}(W)$ (extended pointwise to sets), and
- $U \subseteq W$.

Forcing relation for new connectives:

$$
\begin{array}{rcl}
w \models_\rho A \overset{*}{\vee} B & \Leftrightarrow & \forall w_1, w_2 \in W.\ w \in w_1 \triangledown w_2 \text{ implies} \\
 & & w_1 \models_\rho A \text{ or } w_2 \models_\rho B \\
w \models_\rho A \setminus^{*} B & \Leftrightarrow & w'' \in w' \triangledown w \text{ and } w'' \models_\rho A \text{ and } w' \not\models_\rho B
\end{array}
$$

Semantics of BiBBI

A basic BiBBI-model is given by $\langle W, \circ, E, \triangledown, U \rangle$, where

- $\langle W, \circ, E \rangle$ is a BBI-model,
- $\triangledown \colon W \times W \to \mathcal{P}(W)$ (extended pointwise to sets), and
- $U \subseteq W$.

Forcing relation for new connectives:

$$\begin{array}{rcl}
w \models_\rho A \overset{*}{\vee} B & \Leftrightarrow & \forall w_1, w_2 \in W.\ w \in w_1 \triangledown w_2 \text{ implies} \\
 & & w_1 \models_\rho A \text{ or } w_2 \models_\rho B \\
w \models_\rho A \mathbin{\backslash^{*}} B & \Leftrightarrow & w'' \in w' \triangledown w \text{ and } w'' \models_\rho A \text{ and } w' \not\models_\rho B \\
w \models_\rho \bot^{*} & \Leftrightarrow & w \notin U
\end{array}$$

This is compatible with CBI interpretation of these connectives.

Bells and whistles

Principle	**Axiom**	**Model condition**
Associativity	$A \overset{*}{\parr} (B \overset{*}{\parr} C) \vdash (A \overset{*}{\parr} B) \overset{*}{\parr} C$	$w_1 \triangledown (w_2 \triangledown w_3) = (w_1 \triangledown w_2) \triangledown w_3$
Unit expansion	$A \vdash A \overset{*}{\parr} \bot^*$	$w \triangledown U \subseteq \{w\}$
Unit contraction	$A \overset{*}{\parr} \bot^* \vdash A$	$w \in w \triangledown U$
Contraction	$A \overset{*}{\parr} A \vdash A$	$w \in w \triangledown w$
Weak distribution	$A * (B \overset{*}{\parr} C) \vdash (A * B) \overset{*}{\parr} C$	$(x_1 \circ x_2) \cap (y_1 \triangledown y_2) \neq \emptyset$ implies $\exists w.\ y_1 \in x_1 \circ w$ and $x_2 \in w \triangledown y_2$
Classicality	$\sim\sim A \vdash A$	$\exists ! -w.\ (w \circ -w) \cap U \neq \emptyset$

Theorem

Each axiom defines the corresponding model condition.

Some technical results

For any collection $\mathcal{A}$ of axioms from our table, we have:

Some technical results

For any collection $\mathcal{A}$ of axioms from our table, we have:

Theorem
A BiBBI-*formula is provable in* $\mathrm{BiBBI} + \mathcal{A}$ *iff it is valid in the corresponding subclass of basic* BiBBI-*models.*

Some technical results

For any collection $\mathcal{A}$ of axioms from our table, we have:

Theorem
A BiBBI*-formula is provable in* $\mathrm{BiBBI} + \mathcal{A}$ *iff it is valid in the corresponding subclass of basic* BiBBI*-models.*

(Completeness is by embedding $\mathrm{BiBBI} + \mathcal{A}$ into a Sahlqvist fragment of modal logic.)

Some technical results

For any collection $\mathcal{A}$ of axioms from our table, we have:

Theorem
A BiBBI-*formula is provable in* $\mathrm{BiBBI} + \mathcal{A}$ *iff it is valid in the corresponding subclass of basic* BiBBI-*models.*

(Completeness is by embedding $\mathrm{BiBBI} + \mathcal{A}$ into a Sahlqvist fragment of modal logic.)

Theorem
There is a display calculus proof system for $\mathrm{BiBBI} + \mathcal{A}$ *that is both complete and cut-eliminating.*

Weak distribution principle

- The most interesting versions of BiBBI are those satisfying weak distribution:

$$A * (B \mathbin{\overset{*}{\vee}} C) \vdash (A * B) \mathbin{\overset{*}{\vee}} C$$

  which is a consequence of De Morgan equivalences (so holds in CBI), but not vice versa

Weak distribution principle

- The most interesting versions of BiBBI are those satisfying weak distribution:

$$A * (B \mathbin{\overset{*}{\vee}} C) \vdash (A * B) \mathbin{\overset{*}{\vee}} C$$

  which is a consequence of De Morgan equivalences (so holds in CBI), but not vice versa

- At the model level, this corresponds to:

  $(x_1 \circ x_2) \cap (y_1 \triangledown y_2) \neq \emptyset$ implies $\exists w.\ y_1 \in x_1 \circ w$ and $x_2 \in w \triangledown y_2$

Weak distribution principle

- The most interesting versions of BiBBI are those satisfying weak distribution:

$$A * (B \mathbin{\overset{*}{\triangledown}} C) \vdash (A * B) \mathbin{\overset{*}{\triangledown}} C$$

  which is a consequence of De Morgan equivalences (so holds in CBI), but not vice versa

- At the model level, this corresponds to:

  $(x_1 \circ x_2) \cap (y_1 \triangledown y_2) \neq \emptyset$ implies $\exists w.\ y_1 \in x_1 \circ w$ and $x_2 \in w \triangledown y_2$

- If $\bot^*$ is a unit for $\overset{*}{\triangledown}$, we obtain the disjunctive syllogism: $A * ({\sim}A \mathbin{\overset{*}{\triangledown}} B) \vdash B$.

Heap intersection

In the heap model, we can obtain a weak-distributive $\triangledown$ via at least two kinds of heap intersection:

Heap intersection

In the heap model, we can obtain a weak-distributive $\triangledown$ via at least two kinds of heap intersection:

Definition

Define $h \triangledown h'$ to be the intersection of (partial functions) h and h' if $h(\ell) = h'(\ell)$ for all $\ell \in \mathrm{dom}(h) \cap \mathrm{dom}(h')$, and undefined otherwise.

Heap intersection

In the heap model, we can obtain a weak-distributive $\triangledown$ via at least two kinds of heap intersection:

Definition

Define $h \triangledown h'$ to be the intersection of (partial functions) h and h' if $h(\ell) = h'(\ell)$ for all $\ell \in \mathrm{dom}(h) \cap \mathrm{dom}(h')$, and undefined otherwise.

Definition

Define $h \triangledown h'$ to be the intersection of h and h' only where $h(\ell) = h'(\ell)$.

Heap intersection

In the heap model, we can obtain a weak-distributive $\triangledown$ via at least two kinds of heap intersection:

Definition

Define $h \triangledown h'$ to be the intersection of (partial functions) h and h' if $h(\ell) = h'(\ell)$ for all $\ell \in \mathrm{dom}(h) \cap \mathrm{dom}(h')$, and undefined otherwise.

Definition

Define $h \triangledown h'$ to be the intersection of h and h' only where $h(\ell) = h'(\ell)$.

The second is associative, but not the first. Neither intersection has a unit!

Future work

- The paper has quite a bit more about constructing models of different fragments of BiBBI.

Future work

- The paper has quite a bit more about constructing models of different fragments of BiBBI.
- Better (non)conservativity results for various fragments

Future work

- The paper has quite a bit more about constructing models of different fragments of BiBBI.
- Better (non)conservativity results for various fragments
- Explore further the space of models

Future work

- The paper has quite a bit more about constructing models of different fragments of BiBBI.
- Better (non)conservativity results for various fragments
- Explore further the space of models
- Applications of $\overset{*}{\vee}$, $\setminus^{*}$ etc., in program analysis?

Future work

- The paper has quite a bit more about constructing models of different fragments of BiBBI.
- Better (non)conservativity results for various fragments
- Explore further the space of models
- Applications of $\overset{*}{\vee}$, $\setminus^{*}$ etc., in program analysis?

Thanks for listening!