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

\[
A \ast B \vdash B \ast A \quad A \ast (B \ast C) \vdash (A \ast B) \ast C
\]

\[
A \vdash A \ast \top^* \quad A \ast \top^* \vdash A
\]

\[
A_1 \vdash B_1 \quad A_2 \vdash B_2 \quad A \ast B \vdash C \quad A \vdash B \dashv * C
\]

\[
A_1 \ast A_2 \vdash B_1 \ast B_2 \quad A \vdash B \dashv * C \quad A \ast B \vdash C
\]

(i.e., multiplicative intuitionistic linear logic.)
A **BBI-model** is given by \( \langle W, \circ, E \rangle \), where

- \( W \) is a set (of “worlds”),
- \( E \subseteq W \) satisfies \( w \circ E = \{ w \} \) for all \( w \in W \).
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”),
- \( \circ : W \times W \rightarrow \mathcal{P}(W) \) 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 \( w \in W \).
A **BBI-model** is given by $\langle W, \circ, E \rangle$, where

- $W$ is a set (of “worlds”),
- $\circ : W \times W \rightarrow P(W)$ 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
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 \( \text{Loc} \twoheadrightarrow_{\text{fin}} \text{Val} \),
A **BBI-model** is given by $\langle W, \circ, E \rangle$, where

- $W$ is a set (of “worlds”),
- $\circ : W \times W \rightarrow \mathcal{P}(W)$ 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 $\text{Loc} \rightarrow_{\text{fin}} \text{Val}$,
- $\circ$ 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 \( \text{Loc} \to_{\text{fin}} \text{Val} \),
- \( \circ \) 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 $\rho$, and $w \in W$ given by forcing relation $w \models_\rho A$: 

$$
\begin{align*}
\text{if } w' \in w \circ w' & \text{ and } w' \models_\rho A_1 \\
\text{then } w'' \models_\rho A_2
\end{align*}
$$
Semantics of formula $A$ w.r.t. BBI-model $M = \langle W, \circ, E \rangle$, valuation $\rho$, and $w \in W$ given by forcing relation $w \models \rho A$:

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

$$
\begin{align*}
  w \models_\rho P & \iff w \in \rho(P) \\
  \vdots \\
  w \models_\rho \top^* & \iff w \in E
\end{align*}
$$
**BBI, semantically (2)**

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

$$w \models_\rho P \iff w \in \rho(P)$$

$$w \models_\rho \top^* \iff w \in E$$

$$w \models_\rho A_1 \ast A_2 \iff w \in w_1 \circ w_2 \text{ and } w_1 \models_\rho A_1 \text{ and } w_2 \models_\rho A_2$$
BBI, semantically (2)

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

$$w \models \rho P \iff w \in \rho(P)$$

$$w \models \rho \top^\ast \iff w \in E$$

$$w \models \rho A_1 \cdot \ast A_2 \iff w \in w_1 \circ w_2 \text{ and } w_1 \models \rho A_1 \text{ and } w_2 \models \rho A_2$$

$$w \models \rho A_1 \rightarrow \ast A_2 \iff \forall w', w'' \in W. \text{ if } w'' \in w \circ w' \text{ and } w' \models \rho A_1 \text{ then } w'' \models \rho A_2$$
**BBI, semantically (2)**

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

\[
\begin{align*}
  w \models \rho P & \iff w \in \rho(P) \\
  \vdots \\
  w \models \rho \top^* & \iff w \in E \\
  w \models \rho A_1 \ast A_2 & \iff w \in w_1 \circ w_2 \text{ and } w_1 \models \rho A_1 \text{ and } w_2 \models \rho A_2 \\
  w \models \rho A_1 \rightarrow A_2 & \iff \forall w', w'' \in W. \text{ if } w'' \in w \circ w' \text{ and } w' \models \rho A_1 \text{ then } w'' \models \rho A_2
\end{align*}
\]

$A$ is valid in $M$ iff $w \models \rho A$ for all $\rho$ and $w \in W$. 
**BBI, semantically (2)**

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

$$w \models_\rho P \iff w \in \rho(P)$$

$$w \models_\rho \top^* \iff w \in E$$

$$w \models_\rho A_1 \ast A_2 \iff w \in w_1 \circ w_2 \text{ and } w_1 \models_\rho A_1 \text{ and } w_2 \models_\rho A_2$$

$$w \models_\rho A_1 \rightarrow A_2 \iff \forall w', w'' \in W. \text{ if } w'' \in w \circ w' \text{ and } w' \models_\rho A_1 \text{ then } w'' \models_\rho A_2$$

$A$ is valid in $M$ iff $w \models_\rho A$ for all $\rho$ 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 \( \neg * \) its adjoint implication).
Motivating question

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

• Might there be a resource-sensitive version of disjunction?
Motivating question

• * is understood as a resource-sensitive version of conjunction (with \(\neg*\) 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 $\neg*$ 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 \( \neg^* \) 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:

  \[ \forall w \in W. \exists \text{unique} -w \in W. (w \circ -w) \cap U \neq \emptyset \]

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

- Negation defined by $w|\pi = \sim A \iff -w|\pi = A$.

- We have $\sim\sim A \equiv A$ and $A \ast \lor B = \text{def } \sim (\sim A \ast \sim B)$.
**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:

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

\[
\forall w \in W. \exists \text{ unique } -w \in W. (w \circ -w) \cap U \neq \emptyset
\]

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:

  \[
  \forall w \in W. \exists \text{ unique } -w \in W. (w \circ -w) \cap U \neq \emptyset
  \]

- That is, every world \( w \) has a unique “dual” \(-w\). Models include Abelian groups, bit arrays, regular languages, etc.

- Negation defined by \( w \models \sim A \iff -w \not\models A \).
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:

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

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

- Negation defined by $w \models \neg A \iff -w \not\models A$.

- We have $\neg\neg A \equiv A$ and $A \upharpoonright B =_{\text{def}} \neg(\neg A \upharpoonright \neg B)$. 
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 $\uparrow$, coimplication $\downarrow$ and (maybe) falsum $\bot$ to BBI via the following rules:
BiBBI: *Sub-classical BBI*

We add multiplicative disjunction $\Diamond$, coimplication $\ast$ and (maybe) falsum $\bot$ to BBI via the following rules:

**Monotonicity:**

\[
\frac{A_1 \vdash B_1 \quad A_2 \vdash B_2}{A_1 \Diamond A_2 \vdash B_1 \Diamond B_2}
\]

**Residuation:**

\[
\frac{A \vdash B \Diamond C}{A \ast B \vdash C}
\]

**Commutativity:**

\[
A \Diamond B \vdash B \Diamond A
\]

(Other principles are considered **optional**)
A basic BiBBI-model is given by $\langle W, \circ, E, \nabla, U \rangle$, where

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

A basic BiBBI-model is given by \( \langle W, \circ, E, \nabla, U \rangle \), where

- \( \langle W, \circ, E \rangle \) is a BBI-model,
- \( \nabla: W \times W \rightarrow \mathcal{P}(W) \) (extended pointwise to sets), and
A basic BiBBI-model is given by $\langle W, \circ, E, \nabla, U \rangle$, where

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

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

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

Forcing relation for new connectives:

$w \models_\rho A \ast B \iff \forall w_1, w_2 \in W. \ w \in w_1 \nabla w_2 \implies w_1 \models_\rho A \text{ or } w_2 \models_\rho B$
A basic BiBBI-model is given by \( \langle W, \circ, E, \nabla, U \rangle \), where

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

Forcing relation for new connectives:

\[
\begin{align*}
\rho \models A \nabla B & \iff \forall w_1, w_2 \in W. w \in w_1 \nabla w_2 \text{ implies } w_1 \models A \text{ or } w_2 \models B \\
\rho \models A \setminus B & \iff w'' \in w' \nabla w \text{ and } w'' \models A \text{ and } w' \not\models B
\end{align*}
\]

This is compatible with CBI interpretation of these connectives.
**Semantics of BiBBI**

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

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

Forcing relation for new connectives:

- $w \models_{\rho} A \upstar B \iff \forall w_1, w_2 \in W. w \in w_1 \nabla w_2$ implies $w_1 \models_{\rho} A$ or $w_2 \models_{\rho} B$

- $w \models_{\rho} A \setminus^{*} B \iff w'' \in w' \nabla w$ and $w'' \models_{\rho} A$ and $w' \not\models_{\rho} B$

- $w \models_{\rho} \bot^{*} \iff w \not\in U$

This is compatible with CBI interpretation of these connectives.
## Bells and whistles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Axiom</th>
<th>Model condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associativity</td>
<td>$A \vdash (B \vdash C) \vdash (A \vdash B) \vdash C$</td>
<td>$w_1 \lor (w_2 \lor w_3) = (w_1 \lor w_2) \lor w_3$</td>
</tr>
<tr>
<td>Unit expansion</td>
<td>$A \vdash A \vdash \perp^*$</td>
<td>$w \lor U \subseteq {w}$</td>
</tr>
<tr>
<td>Unit contraction</td>
<td>$A \vdash \perp^* \vdash A$</td>
<td>$w \in w \lor U$</td>
</tr>
<tr>
<td>Contraction</td>
<td>$A \vdash A \vdash A$</td>
<td>$w \in w \lor w$</td>
</tr>
<tr>
<td>Weak distribution</td>
<td>$A \ast (B \vdash C) \vdash (A \ast B) \vdash C$</td>
<td>$(x_1 \circ x_2) \cap (y_1 \lor y_2) \neq \emptyset$ implies ( \exists w. y_1 \in x_1 \circ w \text{ and } x_2 \in w \lor y_2 )</td>
</tr>
<tr>
<td>Classicality</td>
<td>$\sim \sim A \vdash A$</td>
<td>$\exists ! -w. (w \circ -w) \cap U \neq \emptyset$</td>
</tr>
</tbody>
</table>

**Theorem**

Each axiom defines the corresponding model condition.
Some technical results

For any collection \( A \) 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 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 BiBBI + $\mathcal{A}$ iff it is valid in the corresponding subclass of basic BiBBI-models.

(Completeness is by embedding 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 BiBBI + $\mathcal{A}$ iff it is valid in the corresponding subclass of basic BiBBI-models.

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

**Theorem**

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

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

\[ A \ast (B \uplus C) \vdash (A \ast B) \uplus C \]

which is a consequence of De Morgan equivalences (so holds in CBI), but not vice versa.
• The most interesting versions of BiBBI are those satisfying weak distribution:

\[ A \ast (B \mathbin{\boxtimes} C) \vdash (A \ast B) \mathbin{\boxtimes} C \]

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

• At the model level, this corresponds to:

\[(x_1 \circ x_2) \cap (y_1 \triangledown y_2) \neq \emptyset \text{ implies } \exists w. \ y_1 \in x_1 \circ w \text{ and } x_2 \in w \triangledown y_2\]
The most interesting versions of BiBBI are those satisfying weak distribution:

\[ A \ast (B \uplus C) \vdash (A \ast B) \uplus C \]

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

At the model level, this corresponds to:

\[(x_1 \circ x_2) \cap (y_1 \nabla y_2) \neq \emptyset \text{ implies } \exists w. y_1 \in x_1 \circ w \text{ and } x_2 \in w \nabla y_2\]

If \( \perp^\ast \) is a unit for \( \uplus^\ast \), we obtain the disjunctive syllogism:

\[ A \ast (\neg A \uplus B) \vdash B. \]
Heap intersection

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

**Definition**

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

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

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

**Definition**

Define $h \nabla h'$ to be the intersection of (partial functions) $h$ and $h'$ if $h(\ell) = h'(\ell)$ for all $\ell \in \text{dom}(h) \cap \text{dom}(h')$, and undefined otherwise.
In the heap model, we can obtain a weak-distributive $\nabla$ via at least two kinds of heap intersection:

**Definition**

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

**Definition**

Define $h \nabla h'$ 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 $\nabla$ via at least two kinds of heap intersection:

**Definition**

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

**Definition**

Define $h \nabla h'$ 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.

Thanks for listening!
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 $\forall^*$, $\exists^*$ 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 $\vee$, $\forall$ etc., in program analysis?

Thanks for listening!