# Formal completeness for Boolean BI

Dominique Larchey-Wendling
TYPES team

LORIA – CNRS
Nancy, France

ANR-Dynres, Nancy, France

# Bunched Implication logic (**BI**)

- Introduced by Pym 99, 02
  - intuitionistic logic connectives: $\wedge$, $\vee$, $\rightarrow$ $\ldots$
  - multiplicative connectives of MILL: $*$, $-\!\!*$, $\mathsf{I}$
  - sound and complete bunched sequent calculus, with cut elimination
- Kripke semantics (Pym&O'Hearn 99, Galmiche&Mery&Pym 02)
  - partially ordered partial commutative monoids $(\mathcal{M}, \circ, \leqslant)$
  - intuitionistic Kripke semantics for additives
  - relevant Kripke semantics for multiplicatives
  - sound and complete Kripke semantics for BI

# BI Logic continued

- In BI, decomposition interpreted by $a \circ b \leqslant m$:
  - resource monoids (partial, ordered)
  - intuitionistic additives and relevant multiplicatives
- BI has proof systems:
  - cut-free bunched sequent calculus (Pym 99)
  - resource tableaux (Galmiche&Mery&Pym 05)
  - inverse method (Donnelly&Gibson et al. 04)
- Additives are intuitionistic in BI, mostly Boolean in Separation Logic

# Boolean **BI** (**BBI**)

- Loosely defined by Pym as $\mathsf{BI} + \{\neg\neg A \to A\}$
  - no known pure sequent based proof system
  - Kripke semantics by ND-monoids (Larchey&Galmiche 06)
  - Display Logic based cut-free proof-system (Brotherston 09)
- Other definition (logical core of Separation and Spatial logics)
  - additive implication $\to$ Kripke interpreted pointwise
  - based on partial (commutative) monoids $(\mathcal{M}, \circ, \mathsf{e})$
  - has a sound and complete (labelled tableaux) proof-system
- two different logics, both undecidable (Larchey&Galmiche 10)

## Words and constraints based models for **BBI**

- Resources as Words of $L^\star$ = lists of letters
- Constraints = (ordered) pairs of words: $m \multimap n$ with $m, n \in L^\star$
- Partial monoidal equivalence $\sim$ (PME)

$$\frac{}{\epsilon \multimap \epsilon}\langle\epsilon\rangle \qquad \frac{x \multimap y}{y \multimap x}\langle s\rangle \qquad \frac{ky \multimap ky \qquad x \multimap y}{kx \multimap ky}\langle c\rangle$$

$$\frac{xy \multimap xy}{xy \multimap yx}\langle com\rangle \qquad \frac{xy \multimap xy}{x \multimap x}\langle d\rangle \qquad \frac{x \multimap y \qquad y \multimap z}{x \multimap z}\langle t\rangle$$

- PME = set of constraints closed under these rules
- given $\mathcal{C}$, the closure is $\overline{\mathcal{C}} = \sim_{\mathcal{C}}$; compactness prop.

# Constraints based Kripke models for **BBI**

- Start with a $\mathsf{PME} \sim$
- The alphabet $\mathsf{A}_\sim = \{l \in L \mid l \sim l\}$
- The language $\mathsf{L}_\sim = \{m \in L^\star \mid m \sim m\}$
- A monotonic valuation $\mathsf{L}_\sim \longrightarrow \mathcal{P}(\mathsf{Var})$

$$m \sim n \Rightarrow m \Vdash V \Rightarrow n \Vdash V$$

- Usual (pointwise) Kripke interpretation for $\wedge$, $\vee$, $\rightarrow$, $\neg$, $\bot$ and $\top$

$$\begin{array}{lll} m \Vdash_\sim \mathsf{I} & \text{iff} & \epsilon \sim m \\ m \Vdash_\sim A * B & \text{iff} & \exists x, y\ xy\ R\ m \wedge x \Vdash_\sim A \wedge y \Vdash_\sim B \\ m \Vdash_\sim A \mathrel{-\!\!*} B & \text{iff} & \forall x, y\ (xm\ R\ y \wedge x \Vdash_\sim A) \Rightarrow y \Vdash_\sim B \end{array}$$

# Labelled tableaux for **BBI**

- Statements $(\mathbb{T}A : m)$, assertions $(\text{ass} : \; m \multimap n)$ and $\text{req} : m \sim n$

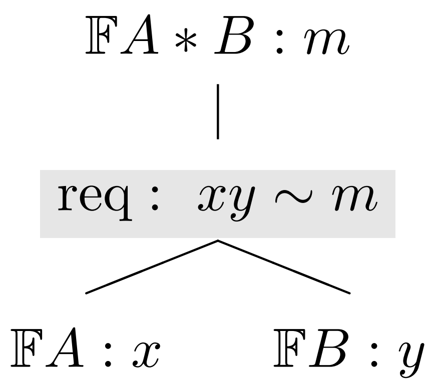
| | | |
|---|---|---|
| $\mathbb{T}\mathsf{I} : m$<br>$\mid$<br>$\text{ass} : \; \epsilon \multimap m$ | $\mathbb{T}A * B : m$<br>$\mid$<br>$\text{ass} : \; ab \multimap m$<br>$\mathbb{T}A : a$<br>$\mathbb{T}B : b$ | $\mathbb{F}A * B : m$<br>$\mid$<br>$\text{req} : \; xy \sim m$<br>branches: $\mathbb{F}A : x$ / $\mathbb{F}B : y$ |
| | $\mathbb{T}A \mathrel{-\!\!*} B : m$<br>$\mid$<br>$\text{req} : \; xm \sim y$<br>branches: $\mathbb{F}A : x$ / $\mathbb{T}B : y$ | $\mathbb{F}A \mathrel{-\!\!*} B : m$<br>$\mid$<br>$\text{ass} : \; am \multimap b$<br>$\mathbb{T}A : a$<br>$\mathbb{F}B : b$ |

## Formalization of tableaux rules

- Statements $\mathbb{T}A : m$ in $\mathcal{X}$ and assertions $m \dashrightarrow n$ in $\mathcal{C}$
- Tableau branch = $\mathsf{CSS}$ $(\mathcal{X}, \mathcal{C})$ $(\mathbb{S}F : m \in \mathcal{X} \Rightarrow m \sim_{\mathcal{C}} m)$
- Rules of the form $\dfrac{\text{cond}(\mathcal{X}, \mathcal{C})}{(\mathcal{X}_1, \mathcal{C}_1) \ \mid \ \cdots \ \mid \ (\mathcal{X}_k, \mathcal{C}_k)}$ , fireable
- An assertion rule (params: $A, B \in \mathsf{Form}, a, b \in L, m \in L^\star$)

| | |
|---|---|
| $\mathbb{T}A * B : m$<br>$\mid$<br>ass : $ab \dashrightarrow m$<br>$\mathbb{T}A : a$<br>$\mathbb{T}B : b$ | $\dfrac{\mathbb{T}A * B : m \in \mathcal{X} \text{ and } a \neq b \in L \backslash \mathsf{A}_{\mathcal{C}}}{(\{\mathbb{T}A : a, \mathbb{T}B : b\}, \{ab \dashrightarrow m\})} \ \langle \mathbb{T}* \rangle$ |

- A requirement rule (params: $A, B \in \mathsf{Form}, x, y, m \in L^\star$)




$$\frac{\mathbb{F}A * B : m \in \mathcal{X} \text{ and } xy \sim_{\mathcal{C}} m}{(\{\mathbb{F}A : x\}, \emptyset) \ \mid \ (\{\mathbb{F}B : y\}, \emptyset)} \ \langle \mathbb{F}* \rangle$$

- Closed tableau branch $(\mathcal{X}, \mathcal{C})$

$$\mathbb{T}A : m \in \mathcal{X} \text{ and } \mathbb{F}A : n \in \mathcal{X} \text{ and } m \sim_{\mathcal{C}} n \text{ for some } A, m, n$$

# Oracles

- Oracle = set of CSS which is $\preccurlyeq$-downward closed, of finite character, open and saturated
- $\mathcal{P}$ is $\preccurlyeq$-downward closed if $(\mathcal{X}, \mathcal{C}) \in \mathcal{P}$ holds whenever both $(\mathcal{X}, \mathcal{C}) \preccurlyeq (\mathcal{X}', \mathcal{C}')$ and $(\mathcal{X}', \mathcal{C}') \in \mathcal{P}$ hold
- $\mathcal{P}$ is of finite character if $(\mathcal{X}, \mathcal{C}) \in \mathcal{P}$ holds whenever $(\mathcal{X}_f, \mathcal{C}_f) \in \mathcal{P}$ holds for every $(\mathcal{X}_f, \mathcal{C}_f) \preccurlyeq_f (\mathcal{X}, \mathcal{C})$
- $\mathcal{P}$ is open if $(\mathcal{X}, \mathcal{C})$ is open for every $(\mathcal{X}, \mathcal{C}) \in \mathcal{P}$
- $\mathcal{P}$ is saturated if for any $(\mathcal{X}, \mathcal{C}) \in \mathcal{P}$ and any fireable instance on $(\mathcal{X}, \mathcal{C})$, at least one of its expansions $(\mathcal{X} \cup \mathcal{X}_i, \mathcal{C} \cup \mathcal{C}_i)$ belongs to $\mathcal{P}$
- not having a closed tableau = oracle $\mathcal{P}$ (excluded middle)

# Fair strategy + Oracles = Hintikka **CSS**

- fair strategy = infinite enumeration of statements $\mathbb{S}_i F_i : m_i$
- start $(\mathcal{X}_0, \mathcal{C}_0)$, notation $\mathcal{C}_i = \mathcal{C}_0 \cup \{x_1 \twoheadrightarrow y_1, \ldots, x_i \twoheadrightarrow y_i\}$
- $(\mathcal{X}_i \cup \{\mathbb{S}_i F_i : m_i\}, \mathcal{C}_i) \notin \mathcal{P} \Rightarrow \mathcal{X}_{i+1} = \mathcal{X}_i$ and $x_{i+1} \twoheadrightarrow y_{i+1} = \epsilon \twoheadrightarrow \epsilon$
- $(\mathcal{X}_i \cup \{\mathbb{S}_i F_i : m_i\}, \mathcal{C}_i) \in \mathcal{P} \Rightarrow \mathcal{X}_{i+1} = \mathcal{X}_i \cup \{\mathbb{S}_i F_i : m_i\} \cup \mathcal{X}_e$

| $\mathbb{S}_i$ | $F_i$ | $\mathcal{X}_e$ | $x_{i+1} \twoheadrightarrow y_{i+1}$ |
|---|---|---|---|
| $\mathbb{T}$ | $\mathsf{I}$ | $\emptyset$ | $\epsilon \twoheadrightarrow m_i$ |
| $\mathbb{T}$ | $A * B$ | $\{\mathbb{T}A : a, \mathbb{T}B : b\}$ | $ab \twoheadrightarrow m_i$ |
| $\mathbb{F}$ | $A \twoheadrightarrow\!\!* B$ | $\{\mathbb{T}A : a, \mathbb{F}B : b\}$ | $am_i \twoheadrightarrow b$ |
| otherwise | | $\emptyset$ | $\epsilon \twoheadrightarrow \epsilon$ |

with $\begin{cases} a = c_{n_0+2i} \\ b = c_{n_0+2i+1} \end{cases}$

## PS generated constraints, strong completeness

- Basic extension of a $\mathsf{PME} \sim$
  1. $ab \multimap m$ with $m \sim m$ and $a \neq b \in L \backslash \mathsf{A}_{\sim}$;
  2. $am \multimap b$ with $m \sim m$ and $a \neq b \in L \backslash \mathsf{A}_{\sim}$;
  3. $\epsilon \multimap m$ with $m \sim m$.
- Simple $\mathsf{PME}$ = infinite sequence of basic extensions
- The PS generated $\mathsf{PME}$ is simple (Hintikka)
- Simple $\mathsf{PME}$ = complete subclass of models