Kripke Models of Boolean BI and Invertible Resources

Dominique Larchey-Wendling

TYPES team

LORIA – CNRS

Nancy, France

Domains IX, Brighton, UK

Separation Logic

- Introduced by Reynolds&O'Hearn 01 to model:
  - properties of the memory space (cells)
  - aggregation of cells into wider structures
- Combines:
  - classical logic connectives: $\wedge$, $\vee$, $\rightarrow$ ...
  - multiplicative conjunction: $*$
- Defined via Kripke semantics extended by:

$$m \Vdash A * B \quad \text{iff} \quad \exists a, b \text{ s.t. } a \uplus b \subseteq m \wedge a \Vdash A \wedge b \Vdash B$$

Bunched Implication logic (BI)

- Introduced by Pym 99, 02
  - **intuitionistic** logic connectives: $\wedge$, $\vee$, $\rightarrow$ ...
  - multiplicative connectives: $*$, $-\!*$
  - sound and complete bunched sequent calculus
- Kripke semantics for BI, (Pym&O'Hearn 99, Galmiche et al. 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

Boolean **BI (BBI)**

- Loosely defined by Pym as $\mathsf{BI} + \{\neg\neg A \rightarrow A\}$
  - no known pure sequent based proof system
  - Kripke semantics is non-deterministic (Larchey&Galmiche)
  - faithfully embeds S4 and thus IL
- Other definition (logical core of Separation and Spatial logics)
  - additive implication $\rightarrow$ Kripke **interpreted classically**
  - based on (commutative) partial monoids $(\mathcal{M}, \circ)$
  - has a sound and complete (labelled tableaux) proof-system
  - still embeds S4 and IL
  - even (intuitionistic) BI (Larchey&Galmiche 08, submitted)

In this talk

- BI/BBI
  - constraints based Kripke models
  - resources vs labels, labelled calculi
- Proof-search based models
  - generation of constraints/properties of constraints models
  - BI (resource graphs)/BBI (deal with invertible resources ?)
- Consequences
  - expressivity
  - embedding
  - representation/implementation

Words and constraints based models for **BI/BBI**

- **Resources as Words** of $L^\star$ = multisets of letters
- Constraints = (ordered) pairs of words: $m \triangleleft\!\triangleright n$ with $m, n \in L^\star$
- Partial monoidal order (PMO): $\sqsubseteq$ closed under $\langle \epsilon, l, r, d, c, t \rangle$
- Partial monoidal equivalence (PME): $\sim$ closed under $\langle \epsilon, s, d, c, t \rangle$

PMOs	PMEs	PMOs & PMEs	
$\dfrac{x \triangleleft\!\triangleright y}{x \triangleleft\!\triangleright x}\,\langle l \rangle$	$\dfrac{x \triangleleft\!\triangleright y}{y \triangleleft\!\triangleright x}\,\langle s \rangle$	$\dfrac{}{\epsilon \triangleleft\!\triangleright \epsilon}\,\langle \epsilon \rangle$	$\dfrac{ky \triangleleft\!\triangleright ky \quad x \triangleleft\!\triangleright y}{kx \triangleleft\!\triangleright ky}\,\langle c \rangle$
$\dfrac{x \triangleleft\!\triangleright y}{y \triangleleft\!\triangleright y}\,\langle r \rangle$		$\dfrac{xy \triangleleft\!\triangleright xy}{x \triangleleft\!\triangleright x}\,\langle d \rangle$	$\dfrac{x \triangleleft\!\triangleright y \quad y \triangleleft\!\triangleright z}{x \triangleleft\!\triangleright z}\,\langle t \rangle$

- $\langle s \rangle + \langle t \rangle$ implies $\langle l \rangle$ and $\langle r \rangle$
- Hence a PME is also a PMO

Constraints based Kripke models for **BI/BBI**

- $R \equiv \sqsubseteq$ for BI / $R \equiv \sim$ for BBI
- Usual (pointwise) Kripke interpretation for $\wedge$, $\vee$, $\perp$ and $\top$

BI/BBI	$m \Vdash_R \mathsf{I}$ iff $\epsilon \, R \, m$
	$m \Vdash_R A * B$ iff $\exists x, y \; xy \, R \, m \wedge x \Vdash_R A \wedge y \Vdash_R B$
	$m \Vdash_R A \mathrel{-\!\!*} B$ iff $\forall x, y \; (xm \, R \, y \wedge x \Vdash_R A) \Rightarrow y \Vdash_R B$
BI	$m \Vdash_\sqsubseteq A \rightarrow B$ iff $\forall x \; (m \sqsubseteq x \wedge x \Vdash_\sqsubseteq A) \Rightarrow x \Vdash_\sqsubseteq B$
BBI	$m \Vdash_\sim A \rightarrow B$ iff $m \Vdash_\sim A \Rightarrow m \Vdash_\sim B$
	$m \Vdash_\sim \neg A$ iff $m \nVdash_\sim A$

Complete constraints based Kripke semantics

- Quotient monoids:
  - $L^\star/\sqsubseteq$ = partially ordered partial monoid
  - $L^\star/\sim$ = partial monoid
- These quotient maps $\sqsubseteq \mapsto L^\star/\sqsubseteq$ and $\sim \mapsto L^\star/\sim$ are full:
  - any partially ordered partial monoid is of the form $L^\star/\sqsubseteq$
  - any partial monoid is of the form $L^\star/\sim$
- Completeness theorem:
  - $\Vdash_\sqsubseteq$ sound and complete Kripke semantics for BI
  - $\Vdash_\sim$ sound and complete Kripke semantics for BBI

Proof methods for BI and BBI

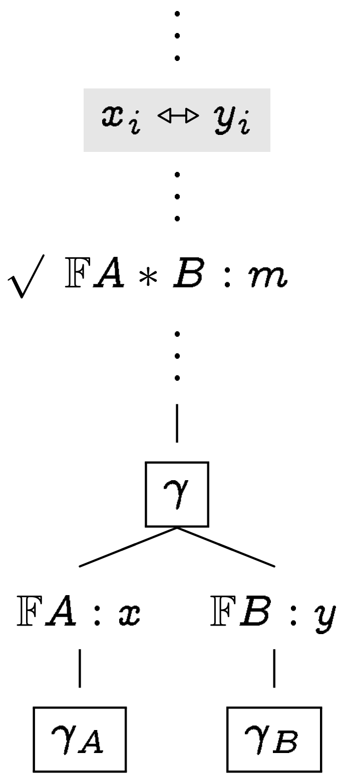
- Labels and constraints based methods
  - calculi with constraints: $\mathbb{T}A : m$, $\mathbb{F}B : n$, $m \leftrightarrow n$
  - sound and complete proof-search method for BI and BBI
  - counter-models extracted from proof-search (Hintikka)
- Properties of the models generated by proof-search
  - implement/optimize theorem provers
  - extract complete sub-classes of counter-models
  - model theoretic and logical links between BI and BBI
  - expressivity properties of BI and BBI

Constraints generated by proof-search (i)

$$
\begin{array}{c}
\vdots \\
x_i \leftrightarrow y_i \\
\vdots \\
\surd\ \mathbb{T}A * B : m \\
\vdots \\
\boxed{\gamma} \\
| \\
ab \leftrightarrow m \\
\mathbb{T}A : a \\
\mathbb{T}B : b \\
| \\
\boxed{\gamma'}
\end{array}
$$

- $\mathcal{C} = \{\ldots, x_i \leftrightarrow y_i, \ldots\}$ from γ
- $A_\gamma = A_\mathcal{C} = \{c \in L \mid c \text{ occurs in } \mathcal{C}\}$
- $\sqsubseteq_\gamma = \sqsubseteq_\mathcal{C}$ / $\sim_\gamma = \sim_\mathcal{C}$
- branch expansion
  - $a \neq b$ new $(a, b \notin A_\gamma)$
  - $\mathcal{C}' = \mathcal{C} \cup \{ab \leftrightarrow m\}$
  - ${\sqsubseteq_\gamma}' = \sqsubseteq_\gamma + \{ab \leftrightarrow m\}$
  - ${\sim_\gamma}' = \sim_\gamma + \{ab \leftrightarrow m\}$

Constraints generated by proof-search (ii)



- $\mathcal{C} = \{\ldots, x_i \Leftrightarrow y_i, \ldots\}$ from γ
- $A_\gamma = A_\mathcal{C} = \{c \in L \mid c \text{ occurs in } \mathcal{C}\}$
- $\sqsubseteq_\gamma = \sqsubseteq_\mathcal{C}$ / $\sim_\gamma = \sim_\mathcal{C}$
- branch expansion
  - x, y s.t. $xy \sqsubseteq_\gamma m$ / $xy \sim_\gamma m$
  - $\mathcal{C}_A = \mathcal{C}_B = \mathcal{C}$
  - $\sqsubseteq_{\gamma_A} = \sqsubseteq_{\gamma_B} = \sqsubseteq_\gamma$
  - $\sim_{\gamma_A} = \sim_{\gamma_B} = \sim_\gamma$

Constraints generated by proof-search (iii)

$$
\begin{array}{c}
\vdots \\
x_i \leftrightarrow y_i \\
\mathbb{T}X : m \\
\vdots \\
\mathbb{F}X : n \\
\vdots \\
\boxed{\gamma} \\
| \\
\times
\end{array}
$$

- $\mathcal{C} = \{\ldots, x_i \leftrightarrow y_i, \ldots\}$ from γ
- $A_\gamma = A_\mathcal{C} = \{c \in L \mid c \text{ occurs in } \mathcal{C}\}$
- $\sqsubseteq_\gamma = \sqsubseteq_\mathcal{C}$ / $\sim_\gamma = \sim_\mathcal{C}$
- branch closure
  - $m \sqsubseteq_\gamma n$ / $m \sim_\gamma n$

Extensions in BI (i)

- a and b are new letters ($a \not\sqsubseteq a$ and $b \not\sqsubseteq b$)
- m defined in $\sqsubseteq$ ($m \sqsubseteq m$)
- Four types of extensions

$$\sqsubseteq' = \sqsubseteq + \{ab \Leftrightarrow m\} \text{ (rule } \mathbb{T}{*}) \qquad \sqsubseteq' = \sqsubseteq + \{am \Leftrightarrow b\} \text{ (rule } \mathbb{F}{-\!*})$$

$$\sqsubseteq' = \sqsubseteq + \{m \Leftrightarrow b\} \quad \text{(rule } \mathbb{F}{\rightarrow}) \quad \sqsubseteq' = \sqsubseteq + \{\epsilon \Leftrightarrow m\} \quad \text{(rule } \mathbb{T}\mathsf{I})$$

- Basic PMO $=$ (finite or infinite) **sequence** of such extensions
- Extensions can be solved:

$$\begin{aligned} \sqsubseteq + \{ab \Leftrightarrow m\} = \sqsubseteq & \cup \{ax \Leftrightarrow ay \mid x \sqsubseteq y \text{ and } mx \sqsubseteq my\} \\ & \cup \{bx \Leftrightarrow by \mid x \sqsubseteq y \text{ and } mx \sqsubseteq my\} \\ & \cup \{abx \Leftrightarrow aby \mid x \sqsubseteq y \text{ and } mx \sqsubseteq my\} \\ & \cup \{abx \Leftrightarrow y \mid mx \sqsubseteq y\} \end{aligned}$$

Extensions in **BI** (ii)

- Properties of basic PMO $\sqsubseteq_{\mathcal{C}}$ (by induction on $\mathcal{C}$):
  - **ϵ-minimality**: if $m \sqsubseteq_{\mathcal{C}} \epsilon$ then $m = \epsilon$
  - **no square**: if $mm \sqsubseteq_{\mathcal{C}} mm$ then $m = \epsilon$
  - **regularity**: if $kx \sqsubseteq_{\mathcal{C}} ky$ then $x \sqsubseteq_{\mathcal{C}} y$

$\Rightarrow$ **finiteness**: $\{m \in L^\star \mid m \sqsubseteq_{\mathcal{C}} m\}$ is finite ($\mathcal{C}$ finite sequence)

- Solving constraints in $\mathcal{C}$: (finite) resource graph (Mery 04)
- Complete sub-class for BI:
  - these properties hold for infinite sequences of basic extensions
  - regular monoids where ϵ is minimal and without square
- Application: no BI-formula F such that $m \Vdash_{\sqsubseteq} F$ iff $mm \sqsubseteq mm$

Extensions in **BBI** (i)

- a and b are new letters, m defined in $\sim$
- Three types of extensions

$$\sim' = \sim + \{ab \leftrightarrow m\} \qquad \text{(rule } \mathbb{T}*)$$

$$\sim' = \sim + \{am \leftrightarrow b\} \qquad \text{(rule } \mathbb{F}{-\!\!*})$$

$$\sim' = \sim + \{\epsilon \leftrightarrow m\} \qquad \text{(rule } \mathbb{T}\mathsf{I})$$

- Basic PME = (finite or infinite) sequence of such extensions
- Extensions $ab \leftrightarrow m$ (and $am \leftrightarrow b$) solved when $\boxed{mm \not\sim mm}$:

$$\begin{aligned} \sim + \{ab \leftrightarrow m\} = \sim &\cup \{ax \leftrightarrow ay, bx \leftrightarrow by \mid x \sim y \text{ and } mx \sim my\} \\ &\cup \{abx \leftrightarrow aby \mid mx \sim my\} \\ &\cup \{abx \leftrightarrow y, y \leftrightarrow abx \mid mx \sim y\} \end{aligned}$$

Extensions in BBI (ii)

- Problems with the $\sim + \{\epsilon \Leftrightarrow m\}$ extension:
  - does not preserve regularity
  - introduce squares (if $\epsilon \sim m$ then $mm \sim mm$)
  - ϵ-minimality irrelevant

$\Rightarrow$ Invertible letters produce $\boxed{\text{infinite models}}$ (not as in BI)

- No simple solution for $\sim + \{ab \Leftrightarrow m\}$ when $mm \sim mm$
- Invertible letters: $I_\sim = \{i \in L \mid ix \sim \epsilon \text{ for some } x \in L^\star\}$

$\Rightarrow$ How to discriminate invertible letters/resources and others ?

Algorithm to compute invertible letters

Require: A list $\mathcal{C}$ of constraints $[\ldots, m \Leftrightarrow n, \ldots]$
Ensure: $N(\mathcal{C}) = (I, \sigma, \mathcal{D}, \mathcal{E})$ terminates

$I \leftarrow \emptyset$, $\sigma \leftarrow \lambda x.x$, $\mathcal{D} \leftarrow [\,]$, $\mathcal{E} \leftarrow \mathcal{C}$
while choose $m \Leftrightarrow n \in \mathcal{E}$ s.t. $(m \in I^\star$ or $n \in I^\star)$ **do**
  $I \leftarrow I \cup A_m \cup A_n$, $\sigma \leftarrow \varphi(\sigma, I, m \Leftrightarrow n)$
  $\mathcal{D} \leftarrow \mathcal{D} @ [m \Leftrightarrow n]$, $\mathcal{E} \leftarrow \mathcal{E} \setminus (m \Leftrightarrow n)$
end while
return $(I, \sigma, \mathcal{D}, \mathcal{E})$

- Underlying sets: $\boxed{\mathcal{C} = \mathcal{D} \cup \mathcal{E}}$
- Discriminate invertible/non-invertible letters: $I_{\sim_\mathcal{C}} = I = A_\mathcal{D}$
- $\sigma : L \longrightarrow L^\star$ an inverse substitution: $i\sigma(i) \sim \epsilon$ for $i \in I^\star$
- If $m \Leftrightarrow n \in \mathcal{D}$ then $m, n \in I^\star$
- If $m \Leftrightarrow n \in \mathcal{E}$ then $m, n \notin I^\star$ (hence $\epsilon \Leftrightarrow m \notin \mathcal{E}$)

Relations between invertible words in $\mathcal{D}$

Let $N(\mathcal{C}) = (I, \sigma, \mathcal{D}, \mathcal{E})$ and $\mathcal{D} = [m_1 \Leftrightarrow n_1, \ldots, m_p \Leftrightarrow n_p]$

- For any $i \in I^\star = A_{\mathcal{D}}^\star$, i defined in $\sim_{\mathcal{C}}$ $(i \sim_{\mathcal{C}} i)$
- For any $i, j \in I^\star$, we have $i \sim_{\mathcal{C}} j$ iff $i \sim_{\mathcal{D}} j$
- Canonical embedding $I^\star \subseteq \mathbb{Z}^I$
- Subgroup generated by $\{\ldots, n_k - m_k, \ldots\}$: $G = \sum_{k=1}^{p} (n_k - m_k)\mathbb{Z}$
- For any $i, j \in I^\star$, we have $i \sim_{\mathcal{D}} j$ iff $j - i \in G$

$$\boxed{A_{\mathcal{D}}^\star / \sim_{\mathcal{D}} \;\simeq\; \mathbb{Z}^I / \textstyle\sum_k (n_k - m_k)\mathbb{Z}}$$

Reductions of constraints remaining in $\mathcal{E}$

Let $N(\mathcal{C}) = (I, \sigma, \mathcal{D}, \mathcal{E})$ and $\mathcal{E} = \mathcal{E}_0 \mathbin{@} [ab \leftrightarrow m] \mathbin{@} \mathcal{E}_1$

- Could be $am \leftrightarrow b$ but $\epsilon \leftrightarrow m \notin \mathcal{E}$ (because $\epsilon \in I^\star$)
- Order in $\mathcal{E}$ = same as in $\mathcal{C}$ ($\mathcal{E}$ obtained by deletion)
- If a (resp. b) not new in $\mathcal{D} \mathbin{@} \mathcal{E}_0$ then $a \in A_{\mathcal{D}} = I$ (resp. $b \in I$)
- Either a or b new (because otherwise $ab \in I^\star$ thus $ab \leftrightarrow m \in \mathcal{D}$)
- If $a \in I$ then transform $ab \leftrightarrow m$ into $b \leftrightarrow \sigma(a)m$ (where b new)

$\boxed{\text{Obtain } \mathcal{E}' \text{ composed of: } ab \leftrightarrow m,\ b \leftrightarrow m,\ am \leftrightarrow b \text{ with } a, b \text{ new}}$

- $\mathcal{D} \mathbin{@} \mathcal{E}'$ equivalent to $\mathcal{D} \mathbin{@} \mathcal{E}$ ($\sim_{\mathcal{D}@\mathcal{E}'} = \sim_{\mathcal{D}@\mathcal{E}}$)

Properties of extensions in $\mathcal{D} @ \mathcal{E}'$

- $\sim_{\mathcal{D}}$ is regular: $kx \sim_{\mathcal{D}} ky \Rightarrow x \sim_{\mathcal{D}} y$ ($\sim_{\mathcal{D}}$ is a group)
- Prove by induction on the length of $\mathcal{E}'$:
  - $mm \sim_{\mathcal{D}@\mathcal{E}'} mm$ iff $m \in I^\star = A^\star_{\mathcal{D}}$
  - $\sim_{\mathcal{D}@\mathcal{E}'}$ is regular
- Hence basic (finite) extensions:
  - have "no square": $mm \sim mm$ iff $m \in I^\star_\sim$
  - are regular: $kx \sim_{\mathcal{D}} ky \Rightarrow x \sim_{\mathcal{D}} y$

Direct application to expressivity of BBI

- By compactness, infinite sequence of basic PME extensions:
  - have "no square": $mm \sim mm$ iff $m \in \mathsf{I}^{\star}_{\sim}$
  - are regular: $kx \sim_{\mathcal{D}} ky \Rightarrow x \sim_{\mathcal{D}} y$
- $m \in \mathsf{I}^{\star}_{\sim}$ expressible by $m \Vdash_{\sim} \neg(\top \mathrel{-\!\!*} \neg\mathsf{I})$ in BBI
- Suppose $m \Vdash_{\sim} F$ iff $mm \sim mm$
  - then $F \rightarrow \neg(\top \mathrel{-\!\!*} \neg\mathsf{I})$ would valid in basic BBI models
  - by completeness: $F \rightarrow \neg(\top \mathrel{-\!\!*} \neg\mathsf{I})$ BBI-provable
  - obviously, $1 \nVdash_{\sim} F \rightarrow \neg(\top \mathrel{-\!\!*} \neg\mathsf{I})$ in $\mathbb{N}$

$$\boxed{\text{being squarable not expressible in BBI either}}$$

Related result: embedding **BI** into **BBI**

Let $\sqsubseteq$ be a basic PMO (infinite sequence of basic extensions)

- There exists K and $\sim$ such that:
  - $K \cap A_{\sqsubseteq} = \emptyset$
  - $\sim$ is a basic PME
  - for any $x, y \in A^{\star}_{\sqsubseteq}$, $\boxed{x \sqsubseteq y \text{ iff } \delta x \sim y \text{ for some } \delta \in K^{\star}}$
- Any basic model of BI represented by a basic model of BBI
- Idea: $\sqsubseteq + \{ab \Leftrightarrow m\} \;/\; \sim + \{\delta q \Leftrightarrow m, ab \Leftrightarrow q\}$ (δ, q new and $\delta \in K$)
- This embedding of (counter-)models can be extended into a **faithful embedding of BI into BBI** (Larchey&Galmiche 08, submitted)

Implementing PMEs

Representation matrix/graph for PMEs:

- Let $\sim$ be any PME over L, $I = I_\sim$ (invertible letters)
- For any $\alpha, \beta \in I^\star$, $x, y \in (L \backslash I)^\star$:

$$\boxed{\alpha x \sim \beta y \quad \text{iff} \quad \beta - \alpha \in H_{x,y}}$$

- $H_{x,y}$ is a (unique) congruence class of $\mathbb{Z}^I$
- $H_{x,y}$ either $\emptyset$ of $H_{x,y} = \delta_{x,y} + G_{x,y}$ with $G_{x,y}$ subgroup of $\mathbb{Z}^I$
- If $\sim$ is regular (as is the case for basic PMEs):
  - either $H_{x,y} = \emptyset$
  - or $G_{x,y} = G_{\epsilon,\epsilon}$ and in this case $H_{x,y} = \delta_{x,y} + G_{\epsilon,\epsilon}$

Implementing basic PMEs

Let $N'(\mathcal{C}) = (I, \sigma, \mathcal{D}, \mathcal{E}')$ with $\mathcal{D} = [m_1 \leftrightarrow n_1, \ldots, m_p \leftrightarrow n_p]$

- Goal = structure for deciding $\sim_{\mathcal{C}}$
- In this case $G_{\epsilon,\epsilon} = \sum_k (n_k - m_k)\mathbb{Z}$
- As $\sim_{\mathcal{C}}$ basic then $H_{x,y} = \emptyset$ whenever x or y contains a square:

  $\Rightarrow$ the matrix $H_{x,y}$ is finite
- When $H_{x,y}$ is not empty: $\boxed{\alpha x \sim_{\mathcal{C}} \beta y \quad \text{iff} \quad \beta - \alpha \in \delta_{x,y} + G_{\epsilon,\epsilon}}$
- Basic extensions $ab \leftrightarrow m$, $b \leftrightarrow m$, $am \leftrightarrow b$ of $\mathcal{E}'$:
  - translate into simple transformations of the matrix $(\delta_{x,y})$

Conclusion and perspectives

- Achievements:
  - complete tableaux with constraints method for BBI
  - properties of proof-search generated BBI constraints
  - expressivity properties for BI and BBI, embedding
  - algorithmic solution to BBI constraints solving
  - introduction of the notion of invertible resource
- Perspectives:
  - implement constraint solving and proof-search for BBI
  - decidability for BBI (approximate infinite extensions ?)
  - provide intuitive understanding of invertible resources
  - e.g. Petri Nets with token loans ?