Phase Semantics and the Undecidability of Boolean BI

(presented in LICS'10)

Dominique Larchey-Wendling & Didier Galmiche

TYPES team, LORIA – CNRS

Nancy, France

GEOCAL-LAC, LORIA, Nancy

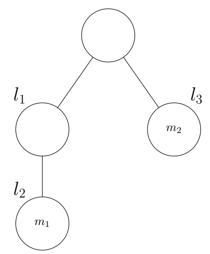
Separation Logic

- Introduced by Reynolds&O'Hearn 01 to model:
  - a **resource** logic
  - properties of the memory space (cells)
  - aggregation of cells into heaps: $\mathrm{Loc} \rightharpoonup_{\mathrm{f}} \mathrm{Val}$
  - heaps can be combined: $\emptyset$, $A \uplus B = C$
- Combines:
  - classical logic connectives: $\wedge$, $\vee$, $\rightarrow$ ...
  - multiplicative conjunction: $*$
- Defined via Kripke semantics extended by:

$$m \Vdash A * B \quad \text{iff} \quad \exists a, b \text{ s.t. } a, b \triangleright m \text{ and } a \Vdash A \text{ and } b \Vdash B$$

Separation models

- Decomposition $a, b \triangleright m$ interpreted in various structures:
  - stacks in pointer logic (Reynolds&O'Hearn&Yang 01), $a \uplus b \sqsubseteq m$
  - but also $a \uplus b = m$ (Calcagno&Yang&O'Hearn 01)
  - trees in spatial logics (Calcagno&Cardelli&Gordon 02) $a \mid b \equiv m$
  - resource trees in BI-Loc (Biri&Galmiche07)



- Additive $\rightarrow$ can be Boolean (pointwise) or intuitionistic

Bunched Implication logic (**BI**)

- Introduced by Pym 99, 02
  - **intuitionistic** logic connectives: $\wedge$, $\vee$, $\rightarrow$ ...
  - multiplicative connectives of MILL: $*$, $-\!\!*$, 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 $(\mathsf{M}, \circ, \leqslant)$
  - 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 intuitionistic in BI, mostly Boolean in Separation Logic

Boolean BI (BBI)

- Loosely defined by Pym as $\mathsf{BI} + \{\neg\neg A \to A\}$
  - cut elimination lost, no “nice” sequent calculus
  - Kripke sem. by relational 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 (commutative) partial monoids $(\mathsf{M}, \circ)$
  - has a sound and complete (labelled tableaux) proof-system

Proof theory for BBI

- Compared to (intuitionistic) BI: much less satisfying situation
  - BI has Bunched sequent calculus (O'Hearn&Pym 99)
  - with cut-elimination from its inception
  - BI is decidable (Galmiche et al. 05)
- Hilbert system s/c for relational BBI (LW.&Galmiche 06, Yang)
- Semantic tableaux s/c for (partial) monoidal BBI
  - (unexpected) embedding of BI into BBI (LW.&Galmiche 09)
- Display calculi s/c for relational BBI (Brotherston 09, 10)

Kripke semantics of **BBI** (i)

- Non-deterministic(/relational) monoid (ND) $(M, \circ, \epsilon)$
  - $\circ : M \times M \longrightarrow \mathbb{P}(M)$ and $\epsilon \in M$
  - for $X, Y \in \mathbb{P}(M)$, $\boxed{X \circ Y = \{z \mid \exists x \in X, \exists y \in Y, z \in x \circ y\}}$
  - $\epsilon \circ x = \{x\}$ (neutrality), $x \circ y = y \circ x$ (commutativity)
  - $x \circ (y \circ z) = (x \circ y) \circ z$ (associativity)
  - $(\mathbb{P}(M), \circ, \{\epsilon\})$ is a (usual) commutative monoid
  - residuation: $X \multimap Y = \{z \mid z \circ X \subseteq Y\}$

Kripke semantics of **BBI** (ii)

- Boolean (pointwise) Kripke semantics extended by:

$$
\begin{array}{lll}
m \Vdash A * B & \text{iff} & \exists a, b \text{ s.t. } m \in a \circ b \text{ and } a \Vdash A \text{ and } b \Vdash B \\
m \Vdash A \mathrel{-\!\!*} B & \text{iff} & \forall a, b \ \ (b \in a \circ m \text{ and } a \Vdash A) \Rightarrow b \Vdash B \\
m \Vdash \mathsf{I} & \text{iff} & m = \epsilon
\end{array}
$$

- Decision problems:
  - checking a particular model ($m \Vdash A$), Calcagno et al. 01 (SL)
  - validity in a particular interpretation ($\forall m, m \Vdash A$)
  - $\boxed{\text{univ. validity}}$ w.r.t. class of models ($\forall \mathcal{M} \forall \Vdash \forall m, m \Vdash A$)

Classes of models for BBI

- Partial (deterministic) monoids (PD): $a \circ b \subseteq \{k\}$
- Total (deterministic) monoids (TD): $a \circ b = \{k\}$
- Obviously: TD $\subsetneq$ PD $\subsetneq$ ND
- Separation models are in HM (Brotherston&Kanovich 10):
  - Heaps monoids: $(L \rightharpoonup_{\mathrm{f}} V, \uplus, \varnothing)$, sub-class of PD
  - RAM-domain model: $(\mathcal{P}_{\mathrm{f}}(\mathbb{N}), \uplus, \emptyset) \simeq (\mathbb{N} \rightharpoonup_{\mathrm{f}} \{\star\}, \uplus, \varnothing)$
- Free monoids: $(\mathbb{M}_{\mathrm{f}}(X), +, 0)$, sub-class of TD
- Validity defines different logics: $\boxed{\mathsf{BBI}_{\mathrm{ND}} \subsetneq \mathsf{BBI}_{\mathrm{PD}} \subsetneq \mathsf{BBI}_{\mathrm{TD}}}$

Overview of the main steps

- The map denoted $!(\cdot) \rightsquigarrow \mathsf{I} \wedge (\cdot)$:
  - is a (sound) embedding from ILL to BBI (not faithful)
  - is faithful for Trivial Phase Semantics
  - is faithful for fragments which are complete for TPS
- Search a fragment both complete for TPS and undecidable:
  - ILL undecidable but IMALL is, hence ! is needed
  - $(!, \oplus)$-Horn fragment (Kanovich 95) not complete for TPS
  - $\mathsf{s\text{-}IMELL}_0^{\multimap}$ fragment (De Groote et al 04) is complete for TPS
  - $\mathsf{s\text{-}IMELL}_0^{\multimap}$ decidability is equiv. to MELL (still open problem)
  - eILL extends $\mathsf{s\text{-}IMELL}_0^{\multimap}$ and fulfills the requirements

Kripke vs. Phase semantics for **BBI**

- Change of notation: $m \Vdash A$ iff $m \in [\![A]\!]$
- The interpretation of multiplicative conjunction $*$

$$
\begin{array}{rcl}
m \Vdash A * B & \text{iff} & \exists a, b \text{ s.t. } a \circ b = m \text{ and } a \Vdash A \text{ and } b \Vdash B \\
[\![A * B]\!] & = & [\![A]\!] \circ [\![B]\!]
\end{array}
$$

- Phase semantics for BBI (equiv. to Kripke sem.):

$$
\begin{array}{rl}
[\![\bot]\!] = \emptyset & [\![A \vee B]\!] = [\![A]\!] \cup [\![B]\!] \\
[\![\top]\!] = M & [\![A \wedge B]\!] = [\![A]\!] \cap [\![B]\!] \\
[\![\mathsf{I}]\!] = \{\epsilon\} & [\![A * B]\!] = [\![A]\!] \circ [\![B]\!] \\
[\![\neg A]\!] = M \backslash [\![A]\!] & [\![A \mathrel{-\!\!*} B]\!] = [\![A]\!] \multimap [\![B]\!]
\end{array}
$$

Phase semantics for **ILL**

- Intuitionistic phase space $(M, \circ, \epsilon, (\cdot)^\diamond, K)$:
  - $(M, \circ, \epsilon)$ in ND (usually TD)
  - $(\cdot)^\diamond$ is a closure operator with $A^\diamond \circ B^\diamond \subseteq (A \circ B)^\diamond$ (stability)
  - K sub-monoid of M: $\epsilon \in K$ and $K \circ K \subseteq K$
  - $K \subseteq \{\epsilon\}^\diamond \cap \{x \in M \mid x \in (x \circ x)^\diamond\}$
- Phase interpretation of ILL operators:

$$
\begin{aligned}
[\![\bot]\!] &= \emptyset^\diamond & \qquad [\![A \oplus B]\!] &= ([\![A]\!] \cup [\![B]\!])^\diamond \\
[\![\top]\!] &= M & \qquad [\![A \mathbin{\&} B]\!] &= [\![A]\!] \cap [\![B]\!] \\
[\![1]\!] &= \{\epsilon\}^\diamond & \qquad [\![A \otimes B]\!] &= ([\![A]\!] \circ [\![B]\!])^\diamond \\
[\![!\, A]\!] &= (K \cap [\![A]\!])^\diamond & \qquad [\![A \multimap B]\!] &= [\![A]\!] \multimap [\![B]\!]
\end{aligned}
$$

Trivial phase semantics for ILL

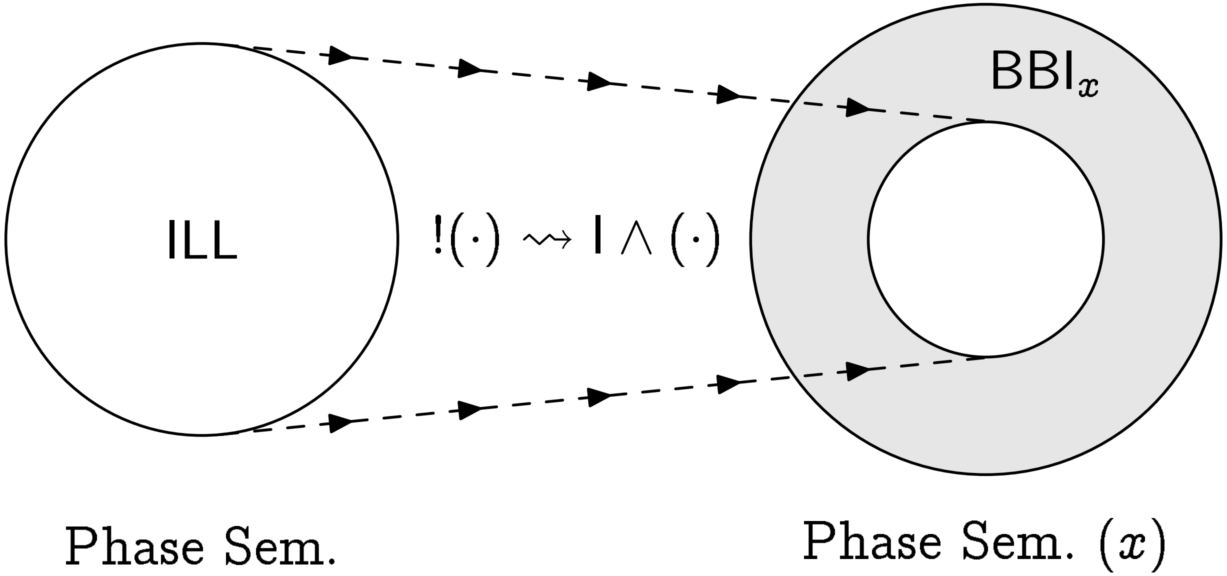
- Intuitionistic phase space $(M, \circ, \epsilon, (\cdot)^\diamond, K)$:
  - $(\cdot)^\diamond$ is the $\boxed{\text{identity closure}}$: $A^\diamond = A$
  - and as a consequence $K = \{\epsilon\}$
- Trivial phase interpretation of ILL operators:

$$
\begin{array}{rclcrcl}
[\![\bot]\!] & = & \emptyset & \qquad & [\![A \oplus B]\!] & = & [\![A]\!] \cup [\![B]\!] \\
[\![\top]\!] & = & M & & [\![A \mathbin{\&} B]\!] & = & [\![A]\!] \cap [\![B]\!] \\
[\![1]\!] & = & \{\epsilon\} & & [\![A \otimes B]\!] & = & [\![A]\!] \circ [\![B]\!] \\
[\![!\,A]\!] & = & \{\epsilon\} \cap [\![A]\!] & & [\![A \multimap B]\!] & = & [\![A]\!] \multimap [\![B]\!]
\end{array}
$$

ILL vs. **BBI** phase semantics

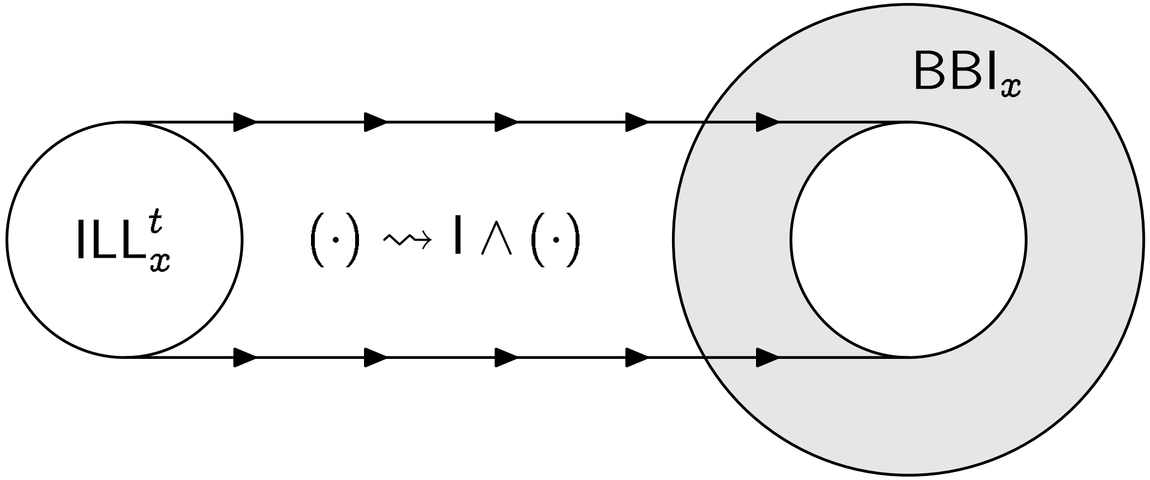
Trivial phase sem. for ILL	Phase sem. for BBI
$[\![\bot]\!] = \emptyset$	$[\![\bot]\!] = \emptyset$
$[\![\top]\!] = M$	$[\![\top]\!] = M$
$[\![1]\!] = \{\epsilon\}$	$[\![\mathsf{I}]\!] = \{\epsilon\}$
$[\![!\,A]\!] = \{\epsilon\} \cap [\![A]\!]$	$[\![\mathsf{I} \wedge A]\!] = \{\epsilon\} \cap [\![A]\!]$
$[\![A \oplus B]\!] = [\![A]\!] \cup [\![B]\!]$	$[\![A \vee B]\!] = [\![A]\!] \cup [\![B]\!]$
$[\![A \,\&\, B]\!] = [\![A]\!] \cap [\![B]\!]$	$[\![A \wedge B]\!] = [\![A]\!] \cap [\![B]\!]$
$[\![A \otimes B]\!] = [\![A]\!] \circ [\![B]\!]$	$[\![A * B]\!] = [\![A]\!] \circ [\![B]\!]$
$[\![A \multimap B]\!] = [\![A]\!] \multimap [\![B]\!]$	$[\![A \mathrel{-\!*} B]\!] = [\![A]\!] \multimap [\![B]\!]$

ILL as a fragment of BBI$_x$ ($x \in \{\mathrm{ND}, \mathrm{PD}, \mathrm{TD}\}$)



- Define a map denoted $!(\cdot) \rightsquigarrow \mathsf{I} \wedge (\cdot)$
  - replace $1/\mathsf{I}$, $\oplus/\vee$, $\&/\wedge$, $\otimes/*$, $\multimap/\mathrel{-\!\!*}$
  - replace $!\,A$ by $\mathsf{I} \wedge A$
- Result: $\boxed{\text{Sound embedding}}$ for phase semantics (but not faithful)

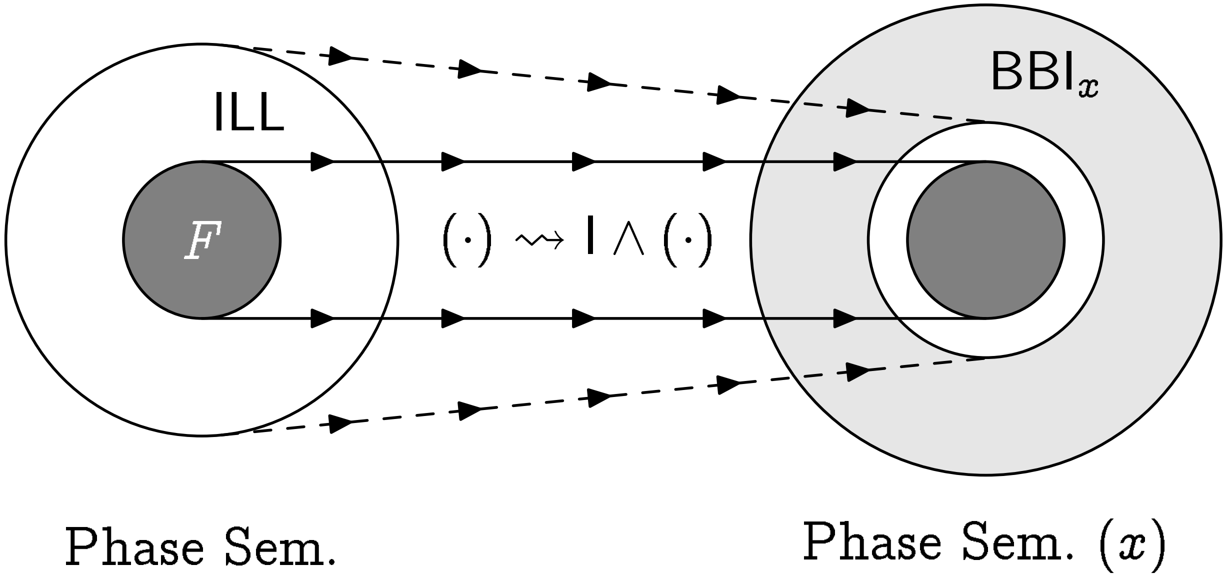
ILL_x^t as a fragment of BBI_x $(x \in \{\mathrm{ND}, \mathrm{PD}, \mathrm{TD}\})$



Triv. Ph. Sem. (x) Phase Sem. (x)

- Result: $\boxed{!(\cdot) \rightsquigarrow \mathsf{I} \wedge (\cdot) \text{ is faithful}}$ for Trivial Phase Semantics

Towards the undecidability of BBI_x



- Among the known/unkown fragments of ILL, find F
  - s.t. $\boxed{F \text{ is complete}}$ for trivial phase semantics (in class x)
  - s.t. $\boxed{F \text{ is undecidable}}$

The elementary fragment eILL of ILL

- Extension of $\mathsf{s\text{-}IMELL}_0^{\multimap}$ (De Groote et al. 04)
- Elementary sequents: $!\,\Sigma, g_1, \ldots, g_k \vdash d$ $\quad$ (g_i, a, b, c, d variables)
  - In Σ: $a \multimap (b \multimap c)$, $(a \multimap b) \multimap c$ or $\boxed{(a \,\&\, b) \multimap c}$
  - where a, b and c variables
- G-eILL, goal directed rules for eILL:

$$\frac{}{!\,\Sigma, a \vdash a}\ \langle \mathrm{Ax} \rangle \qquad \frac{!\,\Sigma, \Gamma \vdash a \qquad !\,\Sigma, \Delta \vdash b}{!\,\Sigma, \Gamma, \Delta \vdash c}\ a \multimap (b \multimap c) \in \Sigma$$

$$\frac{!\,\Sigma, \Gamma, a \vdash b}{!\,\Sigma, \Gamma \vdash c}\ (a \multimap b) \multimap c \in \Sigma \qquad \frac{!\,\Sigma, \Gamma \vdash a \qquad !\,\Sigma, \Gamma \vdash b}{!\,\Sigma, \Gamma \vdash c}\ (a \,\&\, b) \multimap c \in \Sigma$$

Completeness results for elLL

- $\boxed{\text{G-elLL is sound for ND phase semantics}}$ on elLL
  - hence sound w.r.t. any class of models
- $\boxed{\text{free monoidal trivial phase sem. (FM) is complete for G-elLL}}$
  - hence G-elLL is complete for elLL
  - hence trivial phase sem. ($x \in \{\mathrm{ND}, \mathrm{PD}, \mathrm{TD}\}$) is also complete
- we can also prove elLL is complete for class HM (bisimulation)

Undecidability results for eILL/BBI

- encode two counter Minsky machines acceptance in eILL
  - compared to Kanovich 95: forking with & instead of $\oplus$
  - faithfullness proof by semantic argument like Lafont 96
  - Kanovich 95 was through normalization (i.e. cut-elimination)
  - Rem: Okada 02 proved cut-elim. through phase semantics
- obtain $\mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$ is undecidable, deduce $\boxed{\text{eILL is undecidable}}$
- Consequence: $\boxed{\mathsf{BBI}_x \text{ is undecidable}}$ $(x \in \{\mathrm{ND}, \mathrm{PD}, \mathrm{TD}, \mathrm{HM}, \mathrm{FM}\})$

Two counter Minsky Machines

- Two counters, a and b, values in $\mathbb{N}$
- $l+1$ positions, 0 is terminal position, l instructions
- State (i, x, y): i position, x value of a, y value of b
- Two kinds of instructions: "add 1" & "z.t./sub 1"

i: a := a + 1 ; goto j	$(i, x, y) \rightarrow (j, x+1, y)$
i: if a = 0 then goto j	$(i, 0, y) \rightarrow (j, 0, y)$
else a := a − 1 ; goto k	$(i, x+1, y) \rightarrow (k, x, y)$

- Acceptance: (x, y) accepted if $(1, x, y) \rightarrow^{\star} (0, 0, 0)$
- Minsky: there exists a MM with non-recursive acceptance

Encoding acceptance of two counter MM

- Build a sequent $!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i$ for state (i, x, y)
  - variables a and b for the two counters, plus $\underline{\mathsf{a}}$ and $\underline{\mathsf{b}}$ (z.t.)
  - variables $\mathsf{q}_0, \ldots \mathsf{q}_l$ represents the $l+1$ positions of the MM
  - instructions encoding in Σ, a and b never in goal position
  - acceptance as (universal) validity:

$$\boxed{(i, x, y) \to^\star (0, 0, 0) \quad \text{iff} \quad !\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i \text{ univ. valid}}$$

- Encode zero test on b: $!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \underline{\mathsf{a}}$ iff $y = 0$
- Prove soundness: $(i, x, y) \to^r (0, 0, 0) \Rightarrow !\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i$
- Prove completeness: $!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i \Rightarrow (i, x, y) \to^\star (0, 0, 0)$

Encoding zero test on b (soundness)

- With $(\mathsf{a} \multimap \mathsf{a}) \multimap \underline{\mathsf{a}}$ and $\mathsf{a} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}})$ in Σ

$$
\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\langle \mathrm{Ax} \rangle \qquad \dfrac{\dfrac{}{!\,\Sigma, \mathsf{a}, \mathsf{b}^y \vdash \mathsf{a}}\langle \mathrm{Ax} \rangle}{!\,\Sigma, \mathsf{b}^y \vdash \underline{\mathsf{a}}}(\mathsf{a} \multimap \mathsf{a}) \multimap \underline{\mathsf{a}} \in \Sigma}{\vdots \quad \text{applied } x-1 \text{ times}}\mathsf{a} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}}) \in \Sigma
$$

$$
\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\langle \mathrm{Ax} \rangle \qquad \dfrac{}{!\,\Sigma, \mathsf{a}^{x-1}, \mathsf{b}^y \vdash \underline{\mathsf{a}}}}{!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \underline{\mathsf{a}}}\mathsf{a} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}}) \in \Sigma
$$

- is the only possible proof, and only when $y = 0$

Ground case of the recursion $r = 0$ (soundness)

- Corresponds to 0 transitions: $(i, x, y) \rightarrow^0 (0, 0, 0)$
- In this case, $i = x = y = 0$
- With $(\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0$ in Σ

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\ \langle \mathrm{Ax} \rangle}{!\,\Sigma \vdash \mathsf{q}_0}\ (\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0 \in \Sigma$$

- We have our (unique) G-eILL proof

Encoding add 1 to a (soundness)

- With $(\mathsf{a} \multimap \mathsf{q}_j) \multimap \mathsf{q}_i$ in Σ
- "add 1" instruction: $\boxed{i : \mathsf{a} := \mathsf{a} + 1 \ ; \ \mathsf{goto}\ j}$
- Operational semantics: $(i, x, y) \rightarrow (j, x+1, y) \rightarrow^r (0, 0, 0)$
- Recursively built (unique) G-eILL proof to establish validity:

$$\dfrac{\dfrac{\cdots}{!\,\Sigma, \mathsf{a}^x, \mathsf{a}, \mathsf{b}^y \vdash \mathsf{q}_j}}{!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i} \ (\mathsf{a} \multimap \mathsf{q}_j) \multimap \mathsf{q}_i \in \Sigma$$

Encoding sub 1/zero test on a (soundness) (i)

- "sub 1/zero t.": $\boxed{i : \mathsf{if\ a} = 0 \text{ then goto } j \text{ else } \mathsf{a} := \mathsf{a} - 1 \text{ ; goto } k}$
- Case $x = 0$, with $(\underline{\mathsf{b}} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i$ in Σ
- Operational semantics: $(i, 0, y) \rightarrow (j, 0, y) \rightarrow^r (0, 0, 0)$
- Corresponding (unique) G-eILL proof:

$$\dfrac{\dfrac{\text{z.t. on } \mathsf{a}}{!\,\Sigma, \mathsf{b}^y \vdash \underline{\mathsf{b}}} \qquad \dfrac{\ldots}{!\,\Sigma, \mathsf{b}^y \vdash \mathsf{q}_j}}{!\,\Sigma, \mathsf{b}^y \vdash \mathsf{q}_i} \; (\underline{\mathsf{b}} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i \in \Sigma$$

Encoding sub 1/zero test on a (soundness) (ii)

- "sub 1/zero t.": $\boxed{i : \text{if } \mathsf{a} = 0 \text{ then goto } j \text{ else } \mathsf{a} := \mathsf{a} - 1 \text{ ; goto } k}$
- Case $x + 1 > 0$, with $\mathsf{a} \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)$ in Σ
- Operational semantics: $(i, x+1, y) \rightarrow (k, x, y) \rightarrow^r (0, 0, 0)$
- Corresponding (unique) G-eILL proof:

$$\dfrac{\dfrac{}{!\,\Sigma, \mathsf{a} \vdash \mathsf{a}}\langle\mathrm{Ax}\rangle \qquad \dfrac{\cdots}{!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_k}}{!\,\Sigma, \mathsf{a}, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i}\ \mathsf{a} \multimap (\mathsf{q}_k \multimap \mathsf{q}_i) \in \Sigma$$

Summary of the encoding and soundness

- Start with $\Sigma = \left\{ \begin{array}{l} \mathsf{a} \multimap (\underline{\mathsf{a}} \multimap \underline{\mathsf{a}}), \mathsf{b} \multimap (\underline{\mathsf{b}} \multimap \underline{\mathsf{b}}), \\ (\mathsf{a} \multimap \mathsf{a}) \multimap \underline{\mathsf{a}}, (\mathsf{a} \multimap \mathsf{a}) \multimap \underline{\mathsf{b}}, (\mathsf{a} \multimap \mathsf{a}) \multimap \mathsf{q}_0 \end{array} \right\}$
- For instruction i : a := a + 1 ; goto j
  - add $\{(\mathsf{a} \multimap \mathsf{q}_j) \multimap \mathsf{q}_i\}$ to Σ
- For instruction i : if a = 0 then goto j else a := a − 1 ; goto k
  - add $\{(\underline{\mathsf{b}} \mathbin{\&} \mathsf{q}_j) \multimap \mathsf{q}_i, \mathsf{a} \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)\}$ to Σ
- Soundness theorem:

$$\boxed{\text{if } (i, x, y) \to^\star (0, 0, 0) \text{ then } !\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i \text{ has a G-eILL proof}}$$

- as a consequence, $!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i$ is univ. valid

Completeness of the encoding (summary)

- Let us suppose $!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i$ is univ. valid, $\Sigma = \sigma_1, \ldots, \sigma_r$
- By trivial phase interpretation in $\mathbb{N} \times \mathbb{N}$ (class FM)

$$[\![\mathsf{a}]\!] = \{(1,0)\} \quad [\![\mathsf{b}]\!] = \{(0,1)\} \quad [\![\underline{\mathsf{a}}]\!] = \mathbb{N} \times \{0\} \quad [\![\underline{\mathsf{b}}]\!] = \{0\} \times \mathbb{N}$$

$$[\![\mathsf{q}_i]\!] = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid (i,x,y) \to^\star (0,0,0)\}$$

- We will show $\boxed{(0,0) \in [\![\sigma_i]\!]}$ for any i (completeness Lemma)
- By universal validity of $!\,\Sigma, \mathsf{a}^x, \mathsf{b}^y \vdash \mathsf{q}_i$, we derive:

$$[\![!\,\sigma_1]\!] \circ \cdots \circ [\![!\,\sigma_r]\!] \circ [\![\mathsf{a}]\!] \circ \cdots \circ [\![\mathsf{a}]\!] \circ [\![\mathsf{b}]\!] \circ \cdots \circ [\![\mathsf{b}]\!] \subseteq [\![\mathsf{q}_i]\!]$$

- Hence $\{(0,0)\} \circ \cdots \circ \{(0,0)\} \circ \{(x,0)\} \circ \{(0,y)\} \subseteq [\![\mathsf{q}_i]\!]$
- Thus $(x,y) \in [\![\mathsf{q}_i]\!]$, and as a consequence $(i,x,y) \to^\star (0,0,0)$

Inside the proof of the Completeness Lemma (i)

- Case of instruction i : $\mathsf{a} := \mathsf{a} + 1$; goto j
- Σ contains $(\mathsf{a} \multimap \mathsf{q}_j) \multimap \mathsf{q}_i$
- Completeness Lemma condition: $(0,0) \in [\![(\mathsf{a} \multimap \mathsf{q}_j) \multimap \mathsf{q}_i]\!]$
- Interpreted by $\quad [\![\mathsf{a}]\!] \multimap [\![\mathsf{q}_j]\!] \subseteq [\![\mathsf{q}_i]\!]$
- Translates into $\quad \forall x, y \quad (x,y) + (1,0) \in [\![\mathsf{q}_j]\!] \Rightarrow (x,y) \in [\![\mathsf{q}_i]\!]$
- Thus $\quad \forall x, y \quad (j, x+1, y) \to^{\star} (0,0,0) \Rightarrow (i, x, y) \to^{\star} (0,0,0)$
- This is exactly the operational semantics of “add 1 to a”

Inside the proof of the Completeness Lemma (ii)

- Case $x = 0$ of instruction i : if $\mathsf{a} = 0$ then goto j else ...
- Σ contains $(\underline{\mathsf{b}} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i$
- Completeness Lemma condition: $(0,0) \in [\![(\underline{\mathsf{b}} \,\&\, \mathsf{q}_j) \multimap \mathsf{q}_i]\!]$
- Interpreted by $\quad [\![\underline{\mathsf{b}}]\!] \cap [\![\mathsf{q}_j]\!] \subseteq [\![\mathsf{q}_i]\!]$
- or $\quad \forall x, y \quad \big(x = 0 \text{ and } (j, x, y) \to^\star (0,0,0)\big) \Rightarrow (i, x, y) \to^\star (0,0,0)$
- Thus $\quad \forall y \quad (j, 0, y) \to^\star (0,0,0) \Rightarrow (i, 0, y) \to^\star (0,0,0)$
- This is exactly the operational semantics of the “then” branch

Inside the proof of the Completeness Lemma (iii)

- Case $x+1>0$ of i : $\mathsf{if\ a = 0\ then} \ldots \mathsf{else\ a := a-1\ ;\ goto}\ k$
- Σ contains $\mathsf{a} \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)$
- Completeness Lemma condition: $(0,0) \in [\![\mathsf{a} \multimap (\mathsf{q}_k \multimap \mathsf{q}_i)]\!]$
- Interpreted by $\quad [\![\mathsf{a}]\!] \circ [\![\mathsf{q}_k]\!] \subseteq [\![\mathsf{q}_i]\!]$
- Becomes $\quad \forall x, y \quad (k, x+1, y) \rightarrow^\star (0,0,0) \Rightarrow (i, x, y) \rightarrow^\star (0,0,0)$
- This is exactly the operational semantics of the "else" branch

Consequences of the encoding of MM

- An encoding suitable for classes ND, PD, TD and FM
  - $\mathbb{N} \times \mathbb{N} \in \mathrm{FM} \subseteq \mathrm{TD} \subseteq \mathrm{PD} \subseteq \mathrm{ND}$
  - obtain for undecidability of $\mathsf{eILL}^t_{\mathbb{N}\times\mathbb{N}}$ and also for eILL
- Also of $\mathsf{BBI}_{\mathrm{ND}}$, $\mathsf{BBI}_{\mathrm{PD}}$, $\mathsf{BBI}_{\mathrm{TD}}$, $\mathsf{BBI}_{\mathrm{FM}}$ and $\mathsf{BBI}_{\mathbb{N}\times\mathbb{N}}$
- Undecidability for $\mathsf{BBI}_{\mathrm{HM}}$ through bisimulation

Conclusion, related works, perspectives

- Encoding suitable for class FM and thus, all classes
  - undecidability of eILL, BBI_x, $\forall x \in \{\mathrm{ND}, \mathrm{PD}, \mathrm{TD}, \mathrm{HM}, \mathrm{FM}\}$
- Encoding adapted for class of groups (LW., MFPS 10)
  - another proof of undecidability of Classical BI (CBI)
- Similar results by Brotherston&Kanovich (LICS 10)
  - focus on Separation Logic (RAM-domain model)
  - obtained completely independently, also applies to CBI
- What about decidability of BBI restricted to $\mathbb{N}$?
  - 1-counter MM are decidable (Bouajjani et al. 99)
- Complete the classification of BBI_x

Bisimulation vs. Kripke/phase semantics of **BBI**

- $(M, \circ, \epsilon)$ and $(N, \star, \pi)$ two ND monoids
- Bisimulation relation $\sim \subseteq M \times N$ checks:

$$m \sim m' \Rightarrow \begin{cases} m = \epsilon \ \text{ iff } \ m' = \pi \\ \forall a \circ b \ni m\, \exists a' \star b' \ni m' \ \ a \sim a' \text{ and } b \sim b' \\ \forall a' \star b' \ni m'\, \exists a \circ b \ni m \ \ a \sim a' \text{ and } b \sim b' \\ \forall b \in a \circ m\, \exists b' \in a' \star m' \ \ a \sim a' \text{ and } b \sim b' \\ \forall b' \in a' \star m'\, \exists b \in a \circ m \ \ a \sim a' \text{ and } b \sim b' \end{cases}$$

- if $m \sim m'$ then for any F of BBI, $\boxed{m \in [\![F]\!] \text{ iff } m' \in [\![F]\!]'}$

Bisimulating $\mathbb{N} \times \mathbb{N}$ in $\mathcal{P}_{\mathrm{f}}(\mathbb{N})$

- $(\mathcal{P}_{\mathrm{f}}(\mathbb{N}), \uplus, \emptyset)$ and $(\mathbb{N} \times \mathbb{N}, +, (0,0))$ are two ND monoids
- Let $\mathbb{N} = \mathbb{E} \uplus \mathbb{O}$ (e.g. even/odd numbers)
- For $X \in \mathcal{P}_{\mathrm{f}}(\mathbb{N})$, let $\varphi(X) = (\mathrm{card}(X \cap \mathbb{E}), \mathrm{card}(X \cap \mathbb{O}))$
- $\varphi : \mathcal{P}_{\mathrm{f}}(\mathbb{N}) \longrightarrow \mathbb{N} \times \mathbb{N}$ is a projection (surjective)
- $\varphi \subseteq \mathcal{P}_{\mathrm{f}}(\mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ is a bisimulation
- Use φ to transform the $\mathbb{N} \times \mathbb{N}$ model into a $\mathcal{P}_{\mathrm{f}}(\mathbb{N})$ model
  - simply define $[\![\mathrm{x}]\!]' = \varphi^{-1}\big([\![\mathrm{x}]\!]\big)$