Tableaux with constraints for separation logics

TYPES team

LORIA – CNRS

Nancy, France

ANR-Dynres, Nancy, France

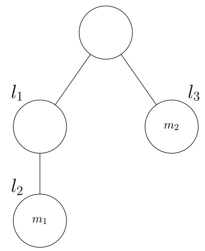
Separation Logic

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

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

Separation models

- Decomposition $a, b \triangleright m$ interpreted in various structures:
  - stacks in pointer logic (Reynolds&O'Hearn&Yang 01),
    $a \uplus b \subseteq m$
  - 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)



- Separation Algebra (SA): partial and cancellative comm. monoid
- 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 $(\mathcal{M}, \circ, \leqslant)$
  - 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 $(\mathcal{M}, \circ, \mathrm{e})$
  - has a sound and complete (labelled tableaux) proof-system
- two different logics, both undecidable (Larchey&Galmiche 10)

In this talk

- We focus on provability, not validity checking (specific model).
- Tools for propositional tautologies in partial monoidal BI and BBI
  - BI defined by partially ordered partial monoids
  - BBI defined by partial monoids
- Common methodology for BI/BBI
  - words and constraints based Kripke models
  - labels and contraints based tableaux calculi
- Properties of proof-search based models
  - resources graphs in BI
  - normal representations for BBI

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

- **Resources as Words** of $L^\star$ = multisets of letters

- Constraints = (ordered) pairs of words: $m \mathrel{-\!\!\bullet\!\!-} n$ with $m, n \in L^\star$
- Partial monoidal order $\sqsubseteq$ (PMO) or equivalence $\sim$ (PME)

PMOs	PMEs	PMOs & PMEs	
$\dfrac{x \mathrel{-\!\!\bullet\!\!-} y}{x \mathrel{-\!\!\bullet\!\!-} x}\ \langle l \rangle$ $\dfrac{x \mathrel{-\!\!\bullet\!\!-} y}{y \mathrel{-\!\!\bullet\!\!-} y}\ \langle r \rangle$	$\dfrac{x \mathrel{-\!\!\bullet\!\!-} y}{y \mathrel{-\!\!\bullet\!\!-} x}\ \langle s \rangle$	$\dfrac{}{\epsilon \mathrel{-\!\!\bullet\!\!-} \epsilon}\ \langle \epsilon \rangle$ $\dfrac{xy \mathrel{-\!\!\bullet\!\!-} xy}{x \mathrel{-\!\!\bullet\!\!-} x}\ \langle d \rangle$	$\dfrac{ky \mathrel{-\!\!\bullet\!\!-} ky \qquad x \mathrel{-\!\!\bullet\!\!-} y}{kx \mathrel{-\!\!\bullet\!\!-} ky}\ \langle c \rangle$ $\dfrac{x \mathrel{-\!\!\bullet\!\!-} y \qquad y \mathrel{-\!\!\bullet\!\!-} z}{x \mathrel{-\!\!\bullet\!\!-} z}\ \langle t \rangle$

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

- Constraints solving: given $\mathcal{C}$, compute the closure $\sqsubseteq_\mathcal{C}$ / $\sim_\mathcal{C}$?

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 $m \not\Vdash_\sim A$

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

Labelled tableaux for **BI** and **BBI**

- Statements ($\mathbb{T}A : m$, $\mathbb{F}B : n$) and assertions (ass : $m \multimap n$)
- Requirements (req : $m\ R\ n$) with $R = \sqsubseteq$ or $\sim$ (side condition)
- Tableaux expansion rules for I and $*$:

$$
\begin{array}{c|c|c}
\begin{array}{c}
\mathbb{T}\mathsf{I} : m \\
| \\
\text{ass} : \ \epsilon \multimap m
\end{array}
&
\begin{array}{c}
\mathbb{T}A * B : m \\
| \\
\text{ass} : \ ab \multimap m \\
\mathbb{T}A : a \\
\mathbb{T}B : b
\end{array}
&
\begin{array}{c}
\mathbb{F}A * B : m \\
| \\
\text{req} : \ xy\ R\ m \\
\begin{array}{cc}
\mathbb{F}A : x & \mathbb{F}B : y
\end{array}
\end{array}
\end{array}
$$

- Tableaux expansion rules for $-\!\!*$:

$$
\begin{array}{c}
\mathbb{T} A \mathrel{-\!\!*} B : m \\
| \\
\boxed{\text{req} : \; xm \; R \; y} \\
\diagup \quad \diagdown \\
\mathbb{F} A : x \qquad \mathbb{T} B : y
\end{array}
\qquad\qquad
\begin{array}{c}
\mathbb{F} A \mathrel{-\!\!*} B : m \\
| \\
\text{ass} : \; am \mathrel{-\!\!\bullet\!\!-} b \\
\mathbb{T} A : a \\
\mathbb{F} B : b
\end{array}
$$

- Tableaux expansion rules for $\longrightarrow$ (only BI):

$$
\begin{array}{c}
\mathbb{T} A \longrightarrow B : m \\
| \\
\boxed{\text{req} : \; m \sqsubseteq x} \\
\diagup \quad \diagdown \\
\mathbb{F} A : x \qquad \mathbb{T} B : x
\end{array}
\qquad\qquad
\begin{array}{c}
\mathbb{F} A \longrightarrow B : m \\
| \\
\text{ass} : \; m \mathrel{-\!\!\bullet\!\!-} b \\
\mathbb{T} A : b \\
\mathbb{F} B : b
\end{array}
$$

Assertions and proof-search

$$\vdots$$

ass : $x_i \mathrel{-\!\!\bullet\!\!-} y_i$

$$\vdots$$

$\surd$ $\mathbb{T}A * B : m$

$$\vdots$$

$\boxed{\gamma}$

ass : $ab \mathrel{-\!\!\bullet\!\!-} m$

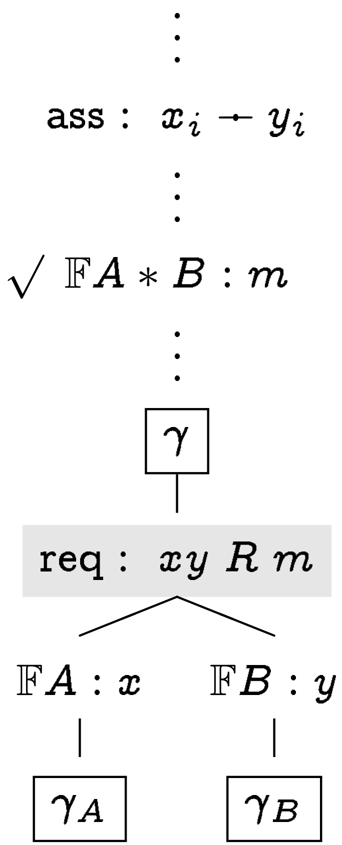
$\mathbb{T}A : a$

$\mathbb{T}B : b$

$\boxed{\gamma'}$

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

Requirements and proof-search



- $\mathcal{C} = \{\ldots, x_i \multimap y_i, \ldots\}$ from γ
- $A_\gamma = A_\mathcal{C} = \{c \in L \mid c \text{ occurs in } \mathcal{C}\}$
- $\sqsubseteq_\gamma = \sqsubseteq_\mathcal{C}$ and $\sim_\gamma = \sim_\mathcal{C}$
- branch expansion
  - x, y s.t. $xy \sqsubseteq_\gamma m$ (BI)
  - x, y s.t. $xy \sim_\gamma m$ (BBI)
  - $\sqsubseteq_{\gamma_A} = \sqsubseteq_{\gamma_B} = \sqsubseteq_\gamma$ (BI)
  - $\sim_{\gamma_A} = \sim_{\gamma_B} = \sim_\gamma$ (BBI)

Closure condition for proof-search

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

- $\mathcal{C} = \{\ldots, x_i \multimap y_i, \ldots\}$ from γ
- $A_\gamma = A_\mathcal{C} = \{c \in L \mid c \text{ occurs in } \mathcal{C}\}$
- $\sqsubseteq_\gamma = \sqsubseteq_\mathcal{C}$ and $\sim_\gamma = \sim_\mathcal{C}$
- branch closure
  - $m \sqsubseteq_\gamma n$ (BI)
  - $m \sim_\gamma n$ (BBI)

BBI proof of $(\mathsf{J} * \mathsf{J}) \to \mathsf{J}$ with $\mathsf{J} = \neg(\top \mathrel{-\!\!\circledast} \neg \mathsf{I})$

$$\mathsf{ass}_0 : \; c \mathrel{-\!\!\bullet\!\!-} d$$
$$\surd_1 \; \mathbb{F}(\mathsf{J} * \mathsf{J}) \to \mathsf{J} : c$$
$$\surd_2 \; \mathbb{T}\mathsf{J} * \mathsf{J} : c$$
$$\surd_{11} \; \mathbb{F}\mathsf{J} : c$$
$$\mathsf{ass}_2 : \; a_0 a_1 \mathrel{-\!\!\bullet\!\!-} c$$
$$\surd_3 \; \mathbb{T}\neg(\top \mathrel{-\!\!\circledast} \neg \mathsf{I}) : a_0$$
$$\surd_7 \; \mathbb{T}\mathsf{J} : a_1$$
$$\surd_4 \; \mathbb{F}\top \mathrel{-\!\!\circledast} \neg \mathsf{I} : a_0$$
$$\boxed{\gamma_0}$$

$$\boxed{\gamma_0}$$
$$\mathsf{ass}_4 : \; b_0 a_0 \mathrel{-\!\!\bullet\!\!-} c_0$$
$$\mathbb{T}\top : b_0$$
$$\surd_5 \; \mathbb{F}\neg \mathsf{I} : c_0$$
$$\surd_6 \; \mathbb{T}\mathsf{I} : c_0$$
$$\mathsf{ass}_6 : \; \epsilon \mathrel{-\!\!\bullet\!\!-} c_0$$
$$\mathsf{ass}_8 : \; b_1 a_1 \mathrel{-\!\!\bullet\!\!-} c_1$$
$$\mathsf{ass}_{10} : \; \epsilon \mathrel{-\!\!\bullet\!\!-} c_1$$
$$\boxed{\gamma_1}$$

$$\boxed{\gamma_1}$$
$$\surd_{12} \; \mathbb{T}\top \mathrel{-\!\!\circledast} \neg \mathsf{I} : c$$
$$\mathsf{req}_{12} : \; (b_0 b_1)c \sim_{\mathcal{K}} \epsilon$$
$$\mathbb{F}\top : b_0 b_1 \qquad\qquad \mathbb{T}\neg \mathsf{I} : \epsilon$$
$$\times \qquad\qquad \mathbb{F}\mathsf{I} : \epsilon$$
$$\times$$

- with $\mathcal{K} = \{c \mathrel{-\!\!\bullet\!\!-} d, a_0 a_1 \mathrel{-\!\!\bullet\!\!-} c, b_0 a_0 \mathrel{-\!\!\bullet\!\!-} c_0, \epsilon \mathrel{-\!\!\bullet\!\!-} c_0, b_1 a_1 \mathrel{-\!\!\bullet\!\!-} c_1, \epsilon \mathrel{-\!\!\bullet\!\!-} c_1\}$

Checking the requirement

- $\mathcal{K} = \{c \leftarrow d, a_0 a_1 \leftarrow c, b_0 a_0 \leftarrow c_0, \epsilon \leftarrow c_0, b_1 a_1 \leftarrow c_1, \epsilon \leftarrow c_1\}$
- We check the requirement $b_0 b_1 c \sim_{\mathcal{K}} \epsilon$ by solving $\mathcal{K}$
- $\{c, d, a_0, a_1, b_0, b_1, c_0, c_1\}^\star / \sim_{\mathcal{K}}$ isomorphic to $\mathbb{Z} \times \mathbb{Z}$ with:

$$c_0 = c_1 = \epsilon = (0,0) \qquad a_0 = -b_0 = (1,0)$$
$$c = d = (1,1) \qquad a_1 = -b_1 = (0,1)$$

- $b_0 b_1 c \sim_{\mathcal{K}} \epsilon$ because $(-1,0) + (0,-1) + (1,1) = (0,0)$
- Remark: the solution of the (finite) set $\mathcal{K}$ is infinite

Tableaux completeness and counter-models

- Labels and constraints based methods:
  - calculi with constraints: $\mathbb{T}A : m$, $\mathbb{F}B : n$, $m \rightarrowtail n$
  - sound/complete proof-search method for tautologies of BI/BBI
  - $\boxed{\text{counter-models from open \& saturated proof-search branch}}$
- Why study the counter-models generated by proof-search:
  - $\boxed{\text{implement/optimize}}$ proof assistants
  - extract $\boxed{\text{complete sub-classes of counter-models}}$ (eg. SA)

PMO extensions in BI-tableaux (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

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

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

- Basic PMO = **finite sequence** of such extensions
- Extensions can be solved:

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

PMO extensions in BI-tableaux (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 $m = \epsilon$
  - cancellativity: 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
  - cancellative monoids where ϵ is minimal and without square

PME extensions in BBI-tableaux (i)

- a and b are new letters, m defined in $\sim$ (i.e. $m \sim m$)
- Three types of extensions

$$
\begin{array}{ll}
\sim' \;=\; \sim + \{ab \mathbin{-\!\bullet\!-} m\} & \quad (\text{rule } \mathbb{T}*) \\[1ex]
\sim' \;=\; \sim + \{am \mathbin{-\!\bullet\!-} b\} & \quad (\text{rule } \mathbb{F}{-\!*}) \\[1ex]
\sim' \;=\; \sim + \{\epsilon \mathbin{-\!\bullet\!-} m\} & \quad (\text{rule } \mathbb{T}\mathsf{I})
\end{array}
$$

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

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

PME extensions in BBI-tableaux (ii)

- Problems with the $\sim + \{\epsilon \multimap m\}$ extension:
  - does not preserve cancellativity
  - introduce squares: if $\epsilon \sim m$ then $mm \sim mm$ (not nec. $m = \epsilon$)

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

$$I_{\sim} = \{i \in L \mid \epsilon \sim im \text{ holds for some } m \in L^{\star}\}$$

- No simple solution for $\sim + \{ab \multimap m\}$ when $mm \sim mm$
- Not the same as the word problem in Thue systems (partiality)

How to compute the invertible letters ?

- Given a (finite) sequence $\mathcal{C} = \{\ldots, m \rightarrowtail n, \ldots\}$
- Compute $I_{\mathcal{C}}$ the set of invertible letters of $\sim_{\mathcal{C}}$

$$I_{\mathcal{C}} = \{i \in L \mid \epsilon \sim_{\mathcal{C}} im \text{ holds for some } m \in L^{\star}\}$$

- Solution by fixpoint:
  - start with $I_{\mathcal{C}} = \emptyset$ and saturate with
  - if $\alpha \rightarrowtail \beta \in \mathcal{C}$ and $\alpha \in I_{\mathcal{C}}^{\star}$ then $\beta \in I_{\mathcal{C}}^{\star}$
  - if $\alpha \rightarrowtail \beta \in \mathcal{C}$ and $\beta \in I_{\mathcal{C}}^{\star}$ then $\alpha \in I_{\mathcal{C}}^{\star}$
- If $\mathcal{C}$ does not contain $m \rightarrowtail \epsilon$ or $\epsilon \rightarrowtail n$ then $I_{\mathcal{C}} = \emptyset$

Algorithm to compute invertible letters

Require: A list $\mathcal{C}$ of constraints $[\ldots, m \twoheadleftarrow n, \ldots]$
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 $m \twoheadleftarrow n \in \mathcal{E}$ s.t. $(m \in I^\star$ or $n \in I^\star)$ **do**
    $I \leftarrow I \cup A_m \cup A_n$, $\sigma \leftarrow \varphi(\sigma, I, m \twoheadleftarrow n)$
    $\mathcal{D} \leftarrow \mathcal{D}$ @ $[m \twoheadleftarrow n]$, $\mathcal{E} \leftarrow \mathcal{E} \backslash (m \twoheadleftarrow n)$
  end while
  return $(I, \sigma, \mathcal{D}, \mathcal{E})$

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

Representation for group PMEs

- Let us consider the **finite** $\mathcal{C} = \{m_k \dashv n_k \mid k \in [1, n]\}$
- In a group PME, all (defined) letters invertible: $A_{\mathcal{C}} = I_{\mathcal{C}} = I$
- Embed $I^\star$ in $\mathbb{Z}^I$ (vectors with non-negative coordinates)
- Define the sub-module $\mathbb{Z}_{\mathcal{C}} = \sum_{k=1}^{n} \mathbb{Z}(n_k - m_k)$
- We obtain the isomorphism: $\boxed{A_{\mathcal{C}}^\star/\!\sim_{\mathcal{C}} \;\simeq\; \mathbb{Z}^I/\mathbb{Z}_{\mathcal{C}}}$
- Compute the **Smith normal form** of a matrix of integers

Primary extensions of PMEs

- Given a PME $\sim$, $m \sim m$, $\alpha \neq \epsilon$, $A_\sim \cap A_\alpha = \emptyset$ and $ll \not\sim \alpha$
- The two following a primary extension:
  - $\sim + \{\alpha \to m\}$ if $m \notin I^\star_\sim$
  - $\sim + \{\alpha m \to b\}$ if $b \notin A_\sim \cup A_\alpha$
- Primary extensions preserves the two following properties:
  - invertible squares, i.e. $ll \sim ll \Rightarrow l \in I_\sim$
  - cancellativity, i.e. $kx \sim ky \Rightarrow x \sim y$
- Both properties hold for a group PME
- Primary PME: list of primary extensions of a group PME

Properties of basic **PMEs**

- Any basic PME can be obtained as a primary PME
- Basics PMEs have invertible squares and cancellativity
- Hence, counter-models obtained by proof-search are cancellative
- The tableau method is sound & complete for Separation Algebras

Normal representation for primary **PMEs**

- Let $\sim$ be a PME
- $(I, N, \mathcal{C}, h)$ is a **normal representation for** $\sim$ if:
  - I and N are finite subsets of L
  - $I_\sim = I$, $A_\sim = I \cup N$ and $I \cap N = \emptyset$
  - $\mathcal{C}$ is a finite set of constraints such that $A_\mathcal{C} \subseteq I$
  - $h : N^\star \times N^\star \longrightarrow_\mathrm{f} \mathbb{Z}^I$ is a partially and finitely defined map
  - for every $i, j \in I^\star$ and $x, y \in N^\star$:

$$\boxed{ix \sim jy \quad \text{iff} \quad j - i \in h_{x,y} + \mathbb{Z}_\mathcal{C}}$$