Petri net semantics for BI revisited

J.R. Courtault - D. Galmiche

ANR DynRes Meeting

LSV - ENS Cachan

June 2012

Introduction

Resource logics

- Some resource logics
  - Linear Logic **LL** (production / consumption) (Girard 1987)
  - Logic of Bunched Implications **BI** (separation / sharing) (Pym 2002)
- **BI** language $= \left\{ \begin{array}{l} \wedge, \vee, \rightarrow, \top, \bot \text{ (additives / } \textbf{IL}\text{)} \\ *, -\!\!*, \mathrm{I} \text{ (multiplicatives / } \textbf{MILL}\text{)} \end{array} \right.$
- **BI** calculi
  - Bunched sequent calculus (Pym 2002)
  - Labelled tableaux calculus (Galmiche-Méry-Pym 2005)
- **BI** semantics
  - Algebraic / topological / categorical semantics
  - Kripke semantics: resource monoid (RM)
    - with an incomplete treatment of $\bot$ (RM)
    - with a complete treatment of $\bot$ (partial RM / RM with inconsistency)

▶ Can we define a Petri net semantics for **BI**?

Introduction

Resource logics and Petri net semantics

- Petri net semantics for **ILL** (Engberg-Winskel 1990)
  - $A \& (B \oplus C) \dashv\vdash (A \& B) \oplus (A \& C)$ does not hold in **ILL**
  - Accessibility / provability ($M \to M'$ iff $\widehat{M} \multimap \widehat{M'}$)
  - Completeness only for some **ILL** fragments (Engberg-Winskel 1997)
- Petri net semantics for **BI** (O'Hearn-Yang 1999)
  - $A \wedge (B \vee C) \dashv\vdash (A \wedge B) \vee (A \wedge C)$ holds in **BI**
  - Accessibility / provability studied for **BBI** + **S4** modalities
  - Completeness only for some **BI** fragments

    ▷ Use of RM
- In this work
  - New Petri nets (called β-Petri nets)
  - New Petri net semantics for **BI** with completeness for **BI**

    ▷ Use of partial RM or RM with inconsistency.

Plan

Plan

BI Logic

Language

$$X ::= p \mid \top \mid \bot \mid \mathrm{I} \mid X \wedge X \mid X \vee X \mid X \rightarrow X \mid X * X \mid X \mathrel{-\!\!*} X$$

$$\neg\phi \equiv \phi \rightarrow \bot$$

Semantics (Galmiche-Méry-Pym 2005)

- Resource monoid with inconsistency: $\mathcal{M} = (R, \bullet, e, \pi, \sqsubseteq)$:
  - R set of resources
  - $e \in R$ and $\pi \in R$
  - $\bullet : R \times R \rightarrow R$ (associative, commutativity, e is unit)
  - $\sqsubseteq \subseteq R \times R$ a preorder (reflexive, transitive)
  - $\pi \in R$ with $\forall r \in R,\ r \sqsubseteq \pi$ and $\forall r \in R,\ r \bullet \pi = \pi$
  - Compatibility: $\forall r_1, r_2, r_3 \in R \cdot r_1 \sqsubseteq r_2 \Rightarrow r_1 \bullet r_3 \sqsubseteq r_2 \bullet r_3$

Semantics

- Interpretation: $[\![-]\!] : Prop \to \mathbb{P}(R)$
  - $\forall r, r' \in R \cdot r \sqsubseteq r'$ and $r \in [\![p]\!] \Rightarrow r' \in [\![p]\!]$
  - $\forall r \in R \cdot \pi \sqsubseteq r \Rightarrow r \in [\![p]\!]$
- Resource model: $\mathcal{K} = (\mathcal{M}, [\![-]\!], \vDash)$
  - $r \vDash p$ iff $r \in [\![p]\!]$
  - $r \vDash \mathrm{I}$ iff $e \sqsubseteq r$
  - $r \vDash \top$ always
  - $r \vDash \bot$ iff $\pi \sqsubseteq r$
  - $r \vDash \phi \wedge \psi$ iff $r \vDash \phi$ and $r \vDash \psi$
  - $r \vDash \phi \vee \psi$ iff $r \vDash \phi$ or $r \vDash \psi$
  - $r \vDash \phi \to \psi$ iff $\forall r' \in R \cdot r \sqsubseteq r' \Rightarrow r' \nvDash \phi$ or $r' \vDash \psi$
  - $r \vDash \phi * \psi$ iff $\exists r', r'' \in R \cdot r' \bullet r'' \sqsubseteq r$ and $r' \vDash \phi$ and $r'' \vDash \psi$
  - $r \vDash \phi \mathrel{-\!\!*} \psi$ iff $\forall r' \in R \cdot r' \vDash \phi \Rightarrow r \bullet r' \vDash \psi$

BI Logic

Validity / Monotonicity / Inconsistency

Definition (validity)

A formula ϕ is *RM-valid* (denoted $\vDash \phi$) if and only if $e \vDash \phi$ for any resource model.

Lemma (monotonicity)

If $r \vDash \phi$ and $r \sqsubseteq r'$ then $r' \vDash \phi$.

Lemma (inconsistency)

Let ϕ be a BI formula, $\pi \vDash \phi$.

Plan

Petri nets with inconsistency

Presentation

- Every system has a finite memory
  - Some data can be "too big" to be encoded in memory
  - Error message: "Out of memory"
- Petri nets model systems
  - But no "out of Petri net memory"
  - Petri nets model *theoretic* systems but not *real* systems
  - Some markings have to be considered as errors (error-markings)
- *Memory linearity*
  - If a marking is not an error then its submarkings are not errors
- *Loss of execution control*
  - If a error occurs then the system cannot be controled
  - An error-marking can access to all markings

Petri nets with inconsistency

Definition

- A Petri net with inconsistency (β-PN) $\mathcal{R} = (P, T, pre, post, \mathbb{M}^c(P), \beta)$
  - P is a set of *places*
  - T is a set of *transitions*
  - *Markings* are functions $P \to \mathbb{N}$
  - $\mathbb{M}^c(P)$ is a set of marking called *consistent markings*:

    CRP: $\forall M \in \mathbb{M}^c(P) \cdot (\forall p \in P \cdot N(p) \leq M(p)) \Rightarrow N \in \mathbb{M}^c(P)$ (memory linearity)
  - β is a special element called *inconsistent marking*
    - β is not a marking ($\beta(p)$ undefined)
    - β represents an error occurring in the system
  - *pre* and *post* are two functions $T \to \mathbb{M}^c(P)$.

Petri nets with inconsistency

Markings: addition/transition

- Marking addition:

$$M + N = \begin{cases} O & \text{such that } O \in \mathbb{M}^c(P) \text{ and } M(p) + N(p) = O(p) \\ \beta & \text{if } O \text{ does not exist} \end{cases}$$

  - Remark: $\beta + M = \beta$

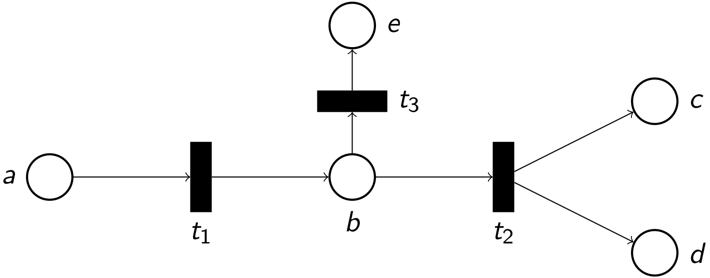
- Marking transition relation ($\Rightarrow$):

$$M \Rightarrow N \text{ iff } M = \beta \text{ or } (\exists t \in T \cdot \exists M' \in \mathbb{M}^c(P) \cdot M = pre(t) + M' \\ \text{and } N = post(t) + M')$$

  - Remark: $\beta \Rightarrow M$ (loss of execution control)

$\Rightarrow^*$ is the reflexive and transitive closure of $\Rightarrow$

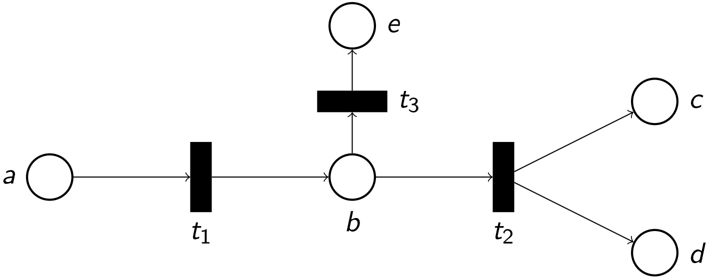
An example



- We suppose that $\mathbb{M}^c(P) = \{M \mid M(e) \leq 2\}$ (it verifies **CRP**)
- $[a, b] + [a, c, e] = [a, a, b, c, e]$
- $[a, e] + [e, e] = \beta$

Petri nets with inconsistency

An example

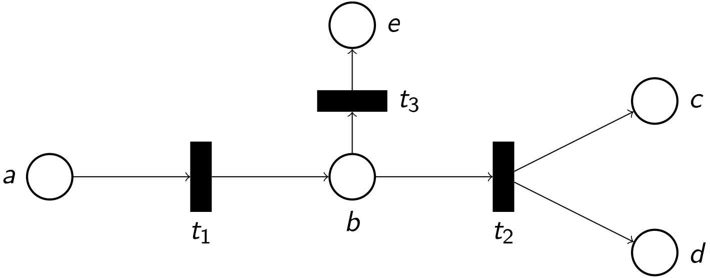


- $pre(t_2) = [b]$ and $post(t_2) = [c, d]$
- $[a, b] = pre(t_2) + [a]$ and $[a, c, d] = post(t_2) + [a]$:

$$[a, b] \Rightarrow [a, c, d]$$

Petri nets with inconsistency

An example



- $[a, b, e] \Rightarrow^* [a, a, a, a]$:

$$[a, b, e] \Rightarrow [b, b, e] \Rightarrow [b, e, e] \Rightarrow \beta \Rightarrow [a, a, a, a]$$

Petri nets with inconsistency

Some remarks

- β-PN are not equivalent to PN with a bound on tokens:
  $P = \{a, b, c\}$
  $\mathbb{M}^c(P) = \{[a], [c], []\}$
  - The bound is 0: $[a] \notin \mathbb{M}^c(P)$ which is absurd
  - The bound is $n > 0$: $\underbrace{[b, b, ..., b]}_{n \text{ times}} \in \mathbb{M}^c(P)$ which is absurd

- β-PN are not equivalent to PN with a bound on places:
  $P = \{a, b\}$
  $\mathbb{M}^c(P) = \{[\mathbf{a}, \mathbf{b}], [\mathbf{b}, \mathbf{b}], [a], [b], []\}$
  - $bound(b) = 2$ because $[b, b] \in \mathbb{M}^c(P)$ and $[b, b, b] \notin \mathbb{M}^c(P)$
  - $bound(a) = 1$ because $[a] \in \mathbb{M}^c(P)$ and $[a, a] \notin \mathbb{M}^c(P)$
  - But $[a, b, b] \notin \mathbb{M}^c(P)$

Plan

Petri net semantics for BI

β-**PN Semantics** with $\mathbb{M}(P) = \mathbb{M}^c(P) \cup \{\beta\}$

- Interpretation: $i : Prop \to \mathbb{P}(\mathbb{M}(P))$
  - If $N \in i(p)$ and $M \Rightarrow^* N$ then $M \in i(p)$
  - $\beta \in i(p)$

- β-PN model: $\mathcal{K} = (\mathcal{M}, i, \Vdash)$, with $\mathcal{M} = (\mathbb{M}(P), +, [\,], \beta, \Leftarrow^*)$ built on a β-PN $\mathcal{R} = (P, T, pre, post, \mathbb{M}^c(P), \beta)$
  - $M \Vdash p$ iff $M \in i(p)$
  - $M \Vdash \top$ always
  - $M \Vdash \bot$ iff $\beta \Leftarrow^* M$
  - $M \Vdash \mathrm{I}$ iff $[\,] \Leftarrow^* M$
  - $M \Vdash \phi \wedge \psi$ iff $M \Vdash \phi$ and $M \Vdash \psi$
  - $M \Vdash \phi \vee \psi$ iff $M \Vdash \phi$ or $M \Vdash \psi$
  - $M \Vdash \phi \to \psi$ iff $\forall M' \in \mathbb{M}(P)$ such that $M \Leftarrow^* M'$, $M' \nVdash \phi$ or $M' \Vdash \psi$
  - $M \Vdash \phi * \psi$ iff $\exists M', M'' \in \mathbb{M}(P)$ such that $M' + M'' \Leftarrow^* M$ and $M' \Vdash \phi$ and $M'' \Vdash \psi$
  - $M \Vdash \phi \mathrel{-\!\!*} \psi$ iff $\forall M' \in \mathbb{M}(P)$ such that $M' \Vdash \phi$, $M + M' \Vdash \psi$

Validity / Comparison

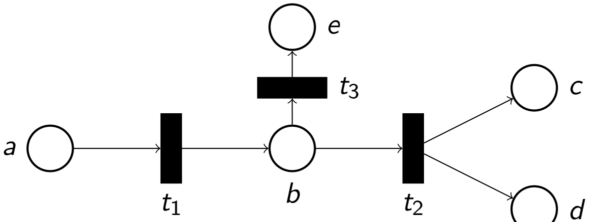
Definition: validity

A formula ϕ is *β-PN valid* (denoted $\Vdash \phi$) if and only if $[] \Vdash \phi$ for any β-PN model.

PN semantics (O'Hearn et al.)	β-PN semantics
"Standard" Petri nets	β-Petri nets: $\beta + M = \beta$ and $\beta \Rightarrow M$
Resource monoids	Resource monoids with inconsistency
Incomplete treatment of $\bot$	Complete treatment of $\bot$
$M \Vdash \bot$ never	$M \Vdash \bot$ iff $\beta \Leftarrow^* M$

Petri net semantics for BI

An example

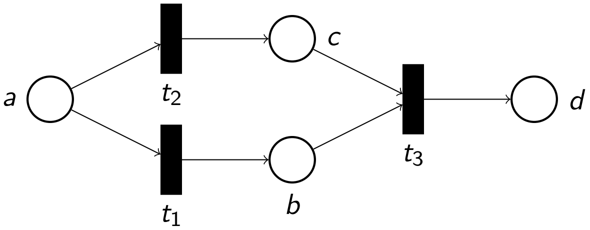


$$\mathbb{M}^c(P) = \{M \mid M(e) \leq 2\} \text{ and } i(p) = \{M \mid M \Rightarrow^* [p]\}$$

- $[b] \Vdash b$, $[a] \Vdash b$ and $\beta \Vdash b$
- $[a] \Vdash a$
- $[a] \Vdash a \wedge b$, because $[a] \Vdash a$ and $[a] \Vdash b$
- $[a] \nVdash a * b$, but $[a, a] \Vdash a * b$:
  $[a, a] \Rightarrow^* [a] + [b]$ and $[a] \Vdash a$ and $[a] \Vdash b$

Petri net semantics for BI

Another example



$$i(p) = \{M \mid M \Rightarrow^* [p]\}$$

- $[b] \Vdash c \mathrel{-\!\!*} d$:
  c can be obtain if enough tokens are added to make d holds

- $[b] \nVdash c \to d$:
  $[a] \Rightarrow^* [b]$ and $[a] \Vdash c$ and $[a] \nVdash d$

Plan

An adequate semantics

Soundness

Lemma

Let $\mathcal{R} = (P, T, pre, post, \mathbb{M}^c(P), \beta)$ be a β-PN. Let $\mathcal{M} = (\mathbb{M}(P), +, [\,], \beta, \Leftarrow^*)$. $\mathcal{M}$ is a resource monoid with inconsistency

- CRP $\Rightarrow$ $+$ is associative

Lemma

Let $\mathcal{R} = (P, T, pre, post, \mathbb{M}^c(P), \beta)$ be a β-PN. Let $\mathcal{M} = (\mathbb{M}(P), +, [\,], \beta, \Leftarrow^*)$ and $\mathcal{K} = (\mathcal{M}, i, \Vdash)$ be a β-PN model. $\mathcal{K}$ is a resource model.

Theorem (soundness)

Let a formula ϕ. If ϕ is RM-valid then ϕ is β-PN valid.

An adequate semantics

Completeness

How to transform RM-countermodels into β-PN countermodel

A labelled calculus

- Labelled tableaux calculus
  - L_r set of *labels* built from:
    - Constants $C_r = \{c_1, c_2, ...\} \cup \{1\}$
    - A function $\circ$ on L_r (associative and commutative)
    - 1 is unit of $\circ$
    - Example: $c_1 \circ c_3 \circ c_1 = c_1 \circ c_1 \circ c_3 \circ 1$
  - *Label constraints*: $x \leq y$ where x and y are labels
- A branch $\mathcal{B}$ contains
  - *Labelled formulae* $S\phi : x$ where $S \in \{T, F\}$ and x is a label
  - *Assertions* = label constraints
  - *x inconsistent label*: $\exists y, z \in L_r \cdot T\bot : y \in \mathcal{B}$ and $y \circ z \leq x \in \overline{Ass}(\mathcal{B})$ (reflexive, transitive and compatible closure)

An adequate semantics

BI countermodels properties

- Countermodels $(R, \bullet, e, \pi, \sqsubseteq)$ extracted from a branch $\mathcal{B}$:
  - R is the set of all consistent labels of $\mathcal{B}$
  - $e = 1$
  - π is a new element
  - $r_1 \bullet r_2 = \begin{cases} r_1 \circ r_2 & \text{if } r_1 \circ r_2 \text{ is consistent} \\ \pi & \text{else} \end{cases}$

▶ Resources are consistent labels:
if $r \in R$ then r is of the form $c_{a_1} \circ \ldots \circ c_{a_n}$

▶ $x \circ 1 = x$.
If a label $l = c_{a_1} \circ \ldots \circ c_{a_n}$ then $l = 1$ or $c_{a_i} \in C_r \setminus \{1\}$ for all $1 \leq i \leq n$

An adequate semantics

Some definitions

Definition (atomic resource decomposition)

Let $r \in R \setminus \{\pi\}$. the *atomic resource decomposition* of r, noted $ARD(r)$, is the empty multiset $\{\}$ if r is the label 1 and the multiset $\{c_{a_1}, ..., c_{a_n}\}$ if r is the label $c_{a_1} \circ ... \circ c_{a_n}$.

- $c_{a_i} \neq 1$ for all $1 \leq i \leq n$

Definition (atomic resource)

An *atomic resource* r is a resource s.T. $r \neq e$ and $ARD(r) = \{r\}$.

An adequate semantics

An example

- Let $r \in R$
- r corresponds to a consistent label ($c_2 \circ c_2 \circ c_3 \circ c_4$ for example)
- c_2, c_3 and c_4 are consistent labels
  (property: sublabels of consistent label are consistent)
- $c_2, c_3, c_4 \in R$
- $ARD(r) = \{c_2, c_2, c_3, c_4\}$
- $ARD(c_2) = \{c_2\}$ (c_2 is an atomic resource)

- Atomic resources will be places
- Atomic resource decompositions will be markings

An adequate semantics

Countermodel transformation

- A function Θ:
  Let $\mathcal{K} = (\mathcal{M}, [\![-]\!], \vDash)$, with $\mathcal{M} = (R, \bullet, e, \pi, \sqsubseteq)$ being a resource countermodel of a formula ϕ. $\Theta(\mathcal{K}) = (\mathcal{M}', i, \Vdash)$ where $\mathcal{M}' = (\mathbb{M}(P), +, [\,], \beta, \Leftarrow^*)$ is built on a β-PN $\mathcal{R} = (P, T, pre, post, \mathbb{M}^c(P), \beta)$, such that:
  - $P = \{r \in R \setminus \{\pi\} \mid r$ is an atomic resource$\}$
  - $\mathbb{M}^c(P) = \{[r_1, ..., r_n] \mid r \in R \setminus \{\pi\}$ and $ARD(r) = \{r_1, ..., r_n\}\}$
  - $T = \{t_{r_j \to r_i} \mid r_i \sqsubseteq r_j$ and $r_i \neq \pi$ and $r_j \neq \pi\}$
  - $pre(t_{r_j \to r_i}) = [r_{j_1}, ..., r_{j_n}]$ where $ARD(r_j) = \{r_{j_1}, ..., r_{j_n}\}$
  - $post(t_{r_j \to r_i}) = [r_{i_1}, ..., r_{i_n}]$ where $ARD(r_i) = \{r_{i_1}, ..., r_{i_n}\}$
  - β is a new element such that $\beta \notin \mathbb{M}^c(P)$
  - $\forall p \in Prop$, $\forall M \in \mathbb{M}(P)$, $M \in i(p)$ iff $(M = \beta)$ or $(M = [c_1, ..., c_m]$ and $c_1 \bullet ... \bullet c_m \in [\![p]\!])$

Completeness

Lemma

Let $\mathcal{K} = (\mathcal{M}, [\![-]\!], \models)$, with $\mathcal{M} = (R, \bullet, e, \pi, \sqsubseteq)$, a resource countermodel of a formula ϕ. Let $\Theta(\mathcal{K}) = (\mathcal{M}', i, \Vdash)$ where $\mathcal{M}' = (\mathbb{M}(P), +, [\,], \beta, \Leftarrow^*)$ is built on β-PN $\mathcal{R} = (P, T, pre, post, \mathbb{M}^c(P), \beta)$.

The following properties are satisfied for any formula A:

1. $\beta \Vdash A$
2. If $r \not\models A$ and $r \neq \pi$ and $ARD(r) = \{c_{r_1}, ..., c_{r_n}\}$ then $[c_{r_1}, ..., c_{r_n}] \nVdash A$
3. If $r \models A$ and $r \neq \pi$ and $ARD(r) = \{c_{r_1}, ..., c_{r_n}\}$ then $[c_{r_1}, ..., c_{r_n}] \Vdash A$

Theorem (completeness)

Let a formula ϕ. If ϕ is β-PN valid then ϕ is RM-valid.

An adequate semantics

An example of countermodel transformation

- We consider the formula $((A * B) \wedge A) \mathrel{-\!\!*} (A \to B)$

- This formula is not valid
  ▶ Countermodel extracted with BI tableaux method:

  $\mathcal{K} = (\mathcal{M}, [\![-]\!], \vDash)$ where $\mathcal{M} = (R, \bullet, e, \pi, \sqsubseteq)$

- $R = \{e, c_1, c_2, c_3, c_4, c_3 \circ c_4, \pi\}$:
  - Atomic resources: c_1, c_2, c_3 and c_4
    ▶ Four places obtained by Θ: $P = \{c_1, c_2, c_3, c_4\}$
  - $\mathbb{M}^c(P) = \{[\,], [c_1], [c_2], [c_3], [c_4], [c_3, c_4]\}$
    Let us note that $ARD(c_3 \circ c_4) = \{c_3, c_4\}$

An adequate semantics

An example of countermodel transformation

- $[\![-]\!]$ is defined by: $[\![A]\!] = \{\pi, c_1, c_2, c_3\}$ and $[\![B]\!] = \{\pi, c_4\}$:
  - $i(A) = \{\beta, [c_1], [c_2], [c_3]\}$
  - $i(B) = \{\beta, [c_4]\}$

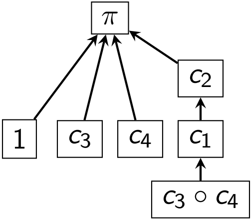
- $\bullet$ is defined by:

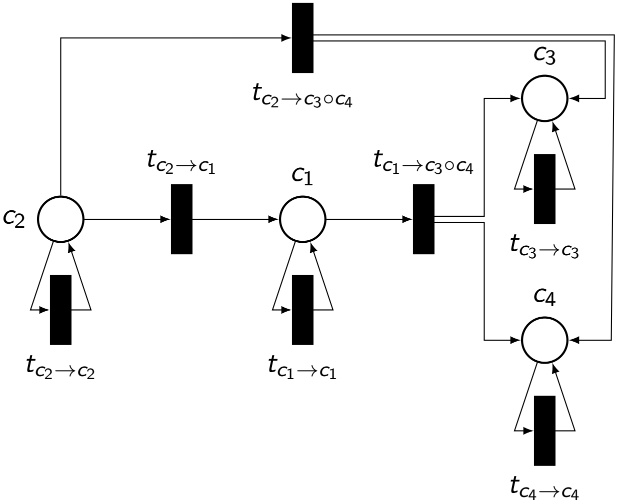
$\bullet$	e	c_1	c_2	c_3	c_4	$c_3 \circ c_4$	π
e	e	c_1	c_2	c_3	c_4	$c_3 \circ c_4$	π
c_1	c_1	π	π	π	π	π	π
c_2	c_2	π	π	π	π	π	π
c_3	c_3	π	π	π	$c_3 \circ c_4$	π	π
c_4	c_4	π	π	$c_3 \circ c_4$	π	π	π
$c_3 \circ c_4$	$c_3 \circ c_4$	π	π	π	π	π	π
π	π	π	π	π	π	π	π

An adequate semantics

An example of countermodel transformation

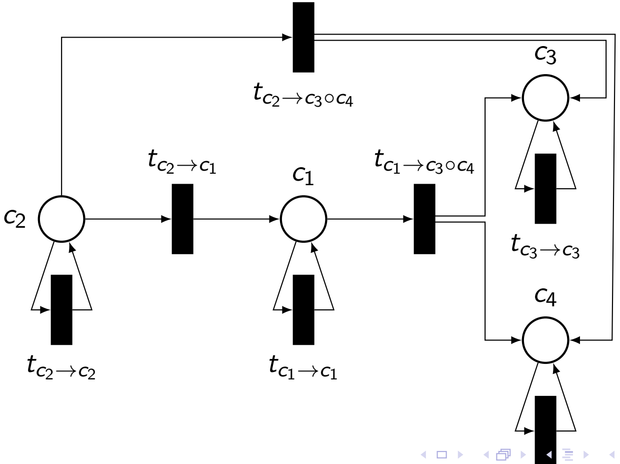
- $\sqsubseteq$ where reflexivity and transitivity is not represented





An example of countermodel transformation

- $\phi = ((A * B) \wedge A) -\!\!* (A \rightarrow B)$:
  $[c_1] \Vdash (A * B) \wedge A$ and $[c_1] + [] \nVdash A \rightarrow B$
- $i(A) = \{\beta, [c_1], [c_2], [c_3]\}$ and $i(B) = \{\beta, [c_4]\}$



Plan

Accessibility / provability: $M_1 \Rightarrow^* M_2$ **iff** $[] \Vdash \widehat{M_1} \multimap \widehat{M_2}$

- Interpretation restriction: $i_{\lhd}(p) = \{M \mid M \Rightarrow^* [p]\}$
- Transformation of markings into formulae:

$$\widehat{M} = \begin{cases} \bot & \text{si } M = \beta \\ \mathrm{I} & \text{si } M = [] \\ r_1 * \ldots * r_m & \text{si } M = [r_1, \ldots, r_m] \end{cases}$$

- Definition of closure: $\downarrow(M) = \{N \in \mathbb{M}(P) \mid N \Rightarrow^* M\}$

Theorem

Let $\mathcal{R} = (P, T, pre, post, \mathbb{M}^c(P), \beta)$ be a β-PN and $\mathcal{M} = (\mathbb{M}(P), +, [], \beta, \Leftarrow^*)$ and $\mathcal{K} = (\mathcal{M}, i_{\lhd}, \Vdash)$. For all markings M_1 and M_2 we have $M_1 \Rightarrow^* M_2$ iff $[] \Vdash \widehat{M_1} \multimap \widehat{M_2}$.

Plan

Conclusions - Perspectives

- New Petri nets with inconsistency (β-PN)
  - β corresponds to error markings
  - Memory linearity
  - Loss of execution control
- A transformation of RM countermodels into β-PN countermodels
- Soundness and completeness of β-Petri net semantics for BI
- Correspondence between accessibility and provability
- Future works:
  Petri net semantics for modal extensions of BI and their properties.