Commodification of Accelerations for the Karp and Miller Construction

Alain Finkel[1], Serge Haddad[1,2], Igor Khmelnitsky[1,2]

(1) LSV ENS Paris-Saclay & CNRS

(2) Inria

Modélisation des Systèmes Réactifs, Angers, 13/11/2019

Plan

1. The Karp and Miller algorithm
2. Abstraction and acceleration
3. A simple proof of the Karp and Miller algorithm

Plan

Reachability and Covering in Petri Net

- **Reachability**

$$Reach(\mathcal{N}, \boldsymbol{m}_0) = \{\boldsymbol{m} \mid \exists \sigma \in T^* \ \boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}\}$$

- **Covering**

$$Cover(\mathcal{N}, \boldsymbol{m}_0) = \downarrow Reach(\mathcal{N}, \boldsymbol{m}_0) = \{\boldsymbol{m} \mid \exists \sigma \in T^* \ \boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}' \geq \boldsymbol{m}\}$$

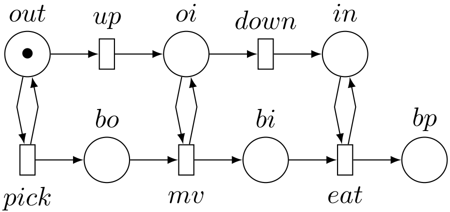
- **Finite representation of the covering**
  - $\mathbb{N}_\omega = \mathbb{N} \cup \{\omega\}$ and $\mathbb{Z}_\omega = \mathbb{Z} \cup \{\omega\}$
    with for all $n \in \mathbb{Z}$, $\omega > n$ and all $n \in \mathbb{Z}_\omega$, $\omega + n = \omega$
  - An ω-*marking* is an item of $\mathbb{N}_\omega^P$.
  - Let $\boldsymbol{m}$ be an ω-*marking*. Then:

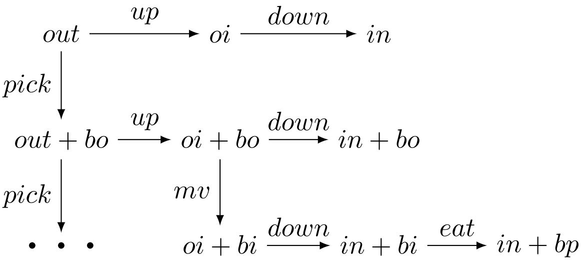
$$[\![\boldsymbol{m}]\!] = \{\boldsymbol{m}' \in \mathbb{N}^P \mid \boldsymbol{m}' \leq \boldsymbol{m}\}$$

There exists a finite (minimal) set of ω-markings $Clover(\mathcal{N}, \boldsymbol{m}_0)$ such that:

$$Cover(\mathcal{N}, \boldsymbol{m}_0) = \bigcup_{\boldsymbol{m} \in Clover(\mathcal{N}, \boldsymbol{m}_0)} [\![\boldsymbol{m}]\!]$$

Reachability Tree of a Petri Net





Building the Reachability Tree

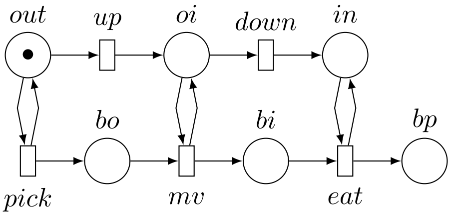
- **A semi-algorithm** to build (V, E, λ, δ)

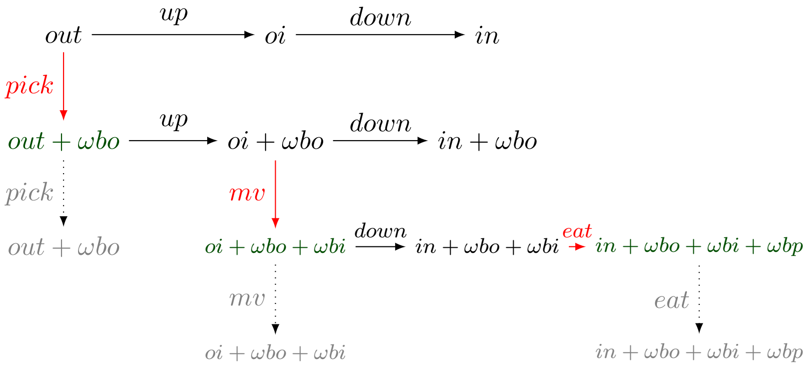
$u \leftarrow CreateV()$; $\lambda(u) \leftarrow \boldsymbol{m}_0$; $Front \leftarrow \emptyset$; $Insert(Front, u)$
$V \leftarrow \{u\}$; $E \leftarrow \emptyset$
While $Front \neq \emptyset$ **do**
  $u \leftarrow FairlyExtract(Front)$
  For all $\lambda(u) \xrightarrow{t} \boldsymbol{m}$ **do**
    $v \leftarrow CreateV()$; $\lambda(v) \leftarrow \boldsymbol{m}$; $Insert(Front, v)$
    $V \leftarrow V \cup \{v\}$; $E \leftarrow E \cup \{(u, v)\}$; $\delta(u, v) = t$

- **Consistency** $\lambda(r) = \boldsymbol{m}_0$ and for all edge $u \xrightarrow{t} v$, one has $\lambda(u) \xrightarrow{t} \lambda(v)$.
- **Completeness** For all $\boldsymbol{m} \in Reach(\mathcal{N}, \boldsymbol{m}_0)$, there exists $u \in V$ such that:
  - either $u \notin Front$ and $\lambda(u) = \boldsymbol{m}$;
  - or $u \in Front$ and there exists $\sigma \in T^*$ such that: $\lambda(u) \xrightarrow{\sigma} \boldsymbol{m}$.

Then one applies fairness.

Covering Tree of a Petri Net





Building the Covering Tree

$u \leftarrow CreateV()$; $\lambda(u) \leftarrow \boldsymbol{m}_0$; $Front \leftarrow \emptyset$; $Insert(Front, u)$
$V \leftarrow \{u\}$; $E \leftarrow \emptyset$
While $Front \neq \emptyset$ **do**
$u \leftarrow Extract(Front)$

(1) u is covered by an ancestor
If $\exists v$ ancestor of u with $\lambda(v) \geq \lambda(u)$ **then** $V \leftarrow V \setminus \{u\}$; $E \leftarrow E \setminus V \times \{u\}$

(2) $\lambda(u)$ is "accelerated"
Else if $\exists v$ ancestor of u with $\lambda(v) < \lambda(u)$
and $\exists p\ \lambda(v)(p) < \lambda(u)(p) < \omega$ **then**
For all p such that $\lambda(v)(p) < \lambda(u)(p) < \omega$ **do** $\lambda(u)(p) \leftarrow \omega$
$Insert(Front, u)$

(3) one explores starting from u
Else
For all $\lambda(u) \xrightarrow{t} \boldsymbol{m}$ **do**
$v \leftarrow CreateV()$; $\lambda(v) \leftarrow \boldsymbol{m}$; $Insert(Front, v)$
$V \leftarrow V \cup \{v\}$; $E \leftarrow E \cup \{u \xrightarrow{t} v\}$

Consistency? For some edges $u \xrightarrow{t} v$, one does not have $\lambda(v) \xrightarrow{t} \lambda(w)$.

Plan

ω-transitions

- **Syntax**

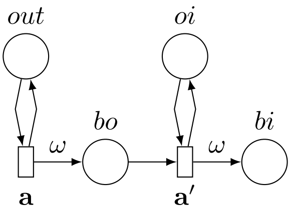
An ω-*transition* $\mathbf{a}$ is defined by:

- its backward incidence $\mathbf{Pre}(\mathbf{a}) \in \mathbb{N}_\omega^P$;
- its incidence $\mathbf{C}(\mathbf{a}) \in \mathbb{Z}_\omega^P$ with $\mathbf{Pre}(\mathbf{a}) + \mathbf{C}(\mathbf{a}) \geq 0$ and for all p, $\mathbf{Pre}(p, \mathbf{a}) = \omega \Rightarrow \mathbf{C}(p, \mathbf{a}) = \omega$.

- **Semantic**

Let $\boldsymbol{m} \in \mathbb{N}_\omega^P$. Then $\mathbf{a}$ is fireable if $\mathbf{Pre}(\mathbf{a}) \leq \boldsymbol{m}$ and its firing leads to $\boldsymbol{m} + \mathbf{C}(\mathbf{a})$.

- **Concatenation** *(using an example)*
  - $\mathbf{Pre}(\mathbf{a}) = out$ and $\mathbf{C}(\mathbf{a}) = \omega bo$
  - $\mathbf{Pre}(\mathbf{a}') = oi + bo$ and $\mathbf{C}(\mathbf{a}') = \omega bi - bo$
  - $\mathbf{Pre}(\mathbf{a} \cdot \mathbf{a}') = out + oi$ and $\mathbf{C}(\mathbf{a} \cdot \mathbf{a}') = \omega bo + \omega bi$

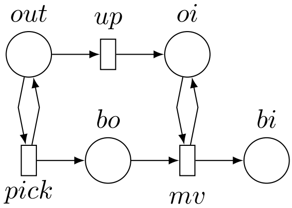


$$\boldsymbol{m} \xrightarrow{\mathbf{a}\mathbf{a}'} \boldsymbol{m}' \text{ if and only if } \boldsymbol{m} \xrightarrow{\mathbf{a}\cdot\mathbf{a}'} \boldsymbol{m}'.$$

Covering Abstraction

- An ω-transition $\mathbf{a}$ is an *abstraction* if for all n, there exists $\sigma_n \in T^*$ with:
  - $\mathbf{Pre}(\sigma_n) \leq \mathbf{Pre}(\mathbf{a})$;
  - For all p, $\mathbf{C}(p, \mathbf{a}) \neq \omega \Rightarrow \mathbf{C}(p, \sigma_n) \geq \mathbf{C}(p, \mathbf{a})$;
  - For all p, $\mathbf{Pre}(p, \mathbf{a}) \neq \omega \wedge \mathbf{C}(p, \mathbf{a}) = \omega \Rightarrow \mathbf{C}(p, \sigma_n) \geq n$.

- **Illustration**
  - $\mathbf{Pre}(\mathbf{a}) = out$ and $\mathbf{C}(\mathbf{a}) = oi - out + \omega bo + \omega bi$
  - $\sigma_n = pick^{2n}\ up\ mv^n$



Properties of Abstractions

The covering set is closed by abstraction firing.

Let $\mathbf{a}$ be an abstraction and $\boldsymbol{m} \in \mathbb{N}_\omega^P$. If:

- $[\![\boldsymbol{m}]\!] \subseteq Cover(\mathcal{N}, \boldsymbol{m}_0)$
- and $\boldsymbol{m} \xrightarrow{\mathbf{a}} \boldsymbol{m}'$

Then $[\![\boldsymbol{m}']\!] \subseteq Cover(\mathcal{N}, \boldsymbol{m}_0)$.

The set of abstractions is closed by concatenation.

Acceleration

$\mathbf{a}$ is an *acceleration* if $\mathbf{a}$ is an abstraction with $\mathbf{C}(\mathbf{a}) \in \{0, \omega\}^P$.

- **How to transform an abstraction into an acceleration?**

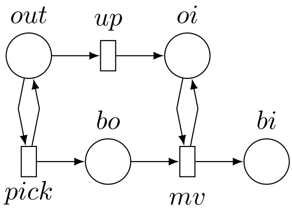
Let $\mathbf{a}$ be an abstraction and $\widehat{\mathbf{a}}$ defined by:

- If $\mathbf{C}(p, \mathbf{a}) < 0$ then $\mathbf{Pre}(p, \widehat{\mathbf{a}}) = \mathbf{C}(p, \widehat{\mathbf{a}}) = \omega$
- If $\mathbf{C}(p, \mathbf{a}) = 0$ then $\mathbf{Pre}(p, \widehat{\mathbf{a}}) = \mathbf{Pre}(p, \mathbf{a})$ and $\mathbf{C}(p, \widehat{\mathbf{a}}) = 0$
- If $\mathbf{C}(p, \mathbf{a}) > 0$ then $\mathbf{Pre}(p, \widehat{\mathbf{a}}) = \mathbf{Pre}(p, \mathbf{a})$ and $\mathbf{C}(p, \widehat{\mathbf{a}}) = \omega$

Then $\widehat{\mathbf{a}}$ is an acceleration.

- **Illustration**

- mv is a transition hence an abstraction.
- $\mathbf{Pre}(\widehat{mv}) = oi + \omega bo$ and $\mathbf{C}(\widehat{mv}) = \omega bo + \omega bi$.



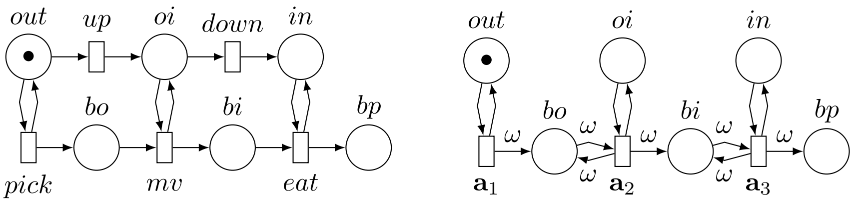
Plan

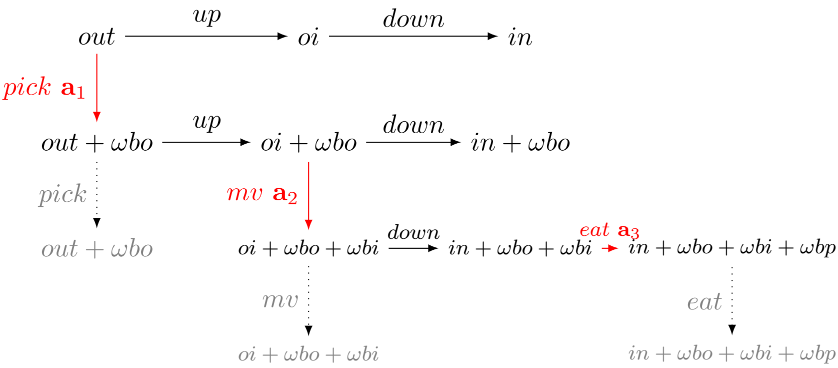
A New Labelling of Edges

Acc (a ghost variable) is a set of ω-transitions.

. . . Acc $\leftarrow \emptyset$
While $Front \neq \emptyset$ **do**
$u \leftarrow Extract(Front)$
(1) u is covered by an ancestor
. . .
(2) $\lambda(u)$ is "accelerated"
Else if $\exists v$ ancestor of u with $\lambda(v) < \lambda(u)$
and $\exists p\ \lambda(v)(p) < \lambda(u)(p) < \omega$ **then**
. . .
Let σ labelling the path from v to u and w the parent of u
Acc $\leftarrow$ Acc $\cup \{\widehat{\sigma}\}$; $\delta(w, u) \leftarrow \delta(w, u)\widehat{\sigma}$
(3) one explores starting from u
. . .

Enriched Covering Tree





Correction of the Algorithm

Termination *(by contradiction)*

- An infinite finitely branching tree implying an infinite branch;
- Strictly increasing subsequence of ω-markings on this branch ... but all ω-marking has at least a new ω.

Consistency

- For all edge (u,v), $\lambda(u) \xrightarrow{\delta(u,v)} \lambda(v)$;
- Acc is a set of accelerations.

Completeness

$\boldsymbol{m} \xrightarrow{\sigma} \boldsymbol{m}'$ is an *exploring sequence* if:

- there exists $u \in Front$ such that $\lambda(u) = \boldsymbol{m}$;
- for all $\boldsymbol{m}''$ visited by σ and all $v \in V \setminus Front$, $\boldsymbol{m}'' \not\leq \lambda(v)$.

For all $\boldsymbol{m} \in Cover(\mathcal{N}, \boldsymbol{m}_0)$,

- either there exists $u \in V \setminus Front$ such that $\lambda(u) \geq \boldsymbol{m}$;
- or there exists an exploring sequence $\boldsymbol{m}_1 \xrightarrow{\sigma} \boldsymbol{m}_2 \geq \boldsymbol{m}$.

Conclusion and Perspectives

Contributions

- Introduction of abstractions, accelerations and exploring sequences;
- Application to the proof of Karp and Miller algorithm;
- Definition of a well order on accelerations and bound on the size of minimal accelerations;
- Acceleration of Karp and Miller algorithm ... based on accelerations.

Perspectives

- Application of accelerations for improving the constructions aiming at minimizing the peak number of ω-markings *(see the demonstration of tool* `MinCov`*)*
- What about accelerations in the more general framework of well structured transitions systems?