Verification of Immediate Observation Petri Nets

Chana Weil-Kennedy, Technical University of Munich

joint work with Mikhail Raskin, Javier Esparza

The project has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme under grant agreement No 787367
Petri nets & reachability

Petri nets are a classic formal model for the representation of concurrent systems.

Reachability problem: Given a Petri net $\mathcal{N}$, and markings $M_0$ and $M$, can marking $M_0$ reach marking $M$ in $\mathcal{N}$?
Petri nets & reachability

Petri nets are a classic formal model for the representation of concurrent systems.

**Reachability problem:** Given a Petri net $\mathcal{N}$, and markings $M_0$ and $M$ can marking $M_0$ reach marking $M$ in $\mathcal{N}$?

---

non-elementary complexity

[Czerwinski, Lasota, Lazic, Leroux, Mazowiecki, '19]
Petri nets & reachability

Petri nets are a classic formal model for the representation of concurrent systems.

**Reachability problem:** Given a Petri net $\mathcal{N}$, and markings $M_0$ and $M$, can marking $M_0$ reach marking $M$ in $\mathcal{N}$?

*Non-elementary complexity* 
[Czerwinzki, Lasota, Lazic, Leroux, Mazowiecki, ’19]

Study subclasses of Petri nets
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., ’06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al.,'06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
Example

[The computational power of population protocols, Angluin et al., '06]
In this talk

Part 1: Immediate observation nets
   Parameterized reachability is easy
   + an intuition of why

Part 2: Branching immediate observation nets
   Parameterized reachability is still easy
   and BIO nets are expressive
Part 1:
Immediate observation nets
Immediate Observation nets

[Esparza, Raskin, W.-K., '19]

Immediate Observation nets (IO)

\[ \text{Immediate Observation nets (IO)} \]

\[ p_1 \rightarrow t \rightarrow p_3 \]

\[ p_2 \]
Immediate Observation nets

[Esparza, Raskin, W.-K., ’19]

Immediate Observation nets (IO)

\[ p_1 \xrightarrow{t} p_3 \xleftarrow{\ \ \ \ \ \ \ \ \ } p_2 \]
Immediate Observation nets

introduced to study immediate observation population protocols (distributed computing model).

[Esparza, Raskin, W.-K., ’19]

[Angluin, Aspnes, Eisenstat, Ruppert, ’07]
Immediate Observation nets

[Esparza, Raskin, W.-K., ’19]

- introduced to study immediate observation population protocols (distributed computing model).
  [Angluin, Aspnes, Eisenstat, Ruppert, ’07]

- other motivating scenarios: sensor networks, enzymatic chemical reactions networks
Immediate Observation nets

[Esparza, Raskin, W.-K., ’19]

Immediate Observation nets (IO)

- introduced to study **immediate observation** population protocols (distributed computing model).
  [Angluin, Aspnes, Eisenstat, Ruppert, ’07]

- other motivating scenarios: sensor networks, enzymatic chemical reactions networks

In these application domains we are interested in *parameterized* problems.
A **cube** is a boolean combination of constraints

\[ a \leq \#q \leq b \]

\[ \in \mathbb{N} \quad \in \mathbb{N} \cup \{\infty\} \]

**cube-reachability**: given cubes \( C \) and \( C' \), does there exist \( M \in C \) and \( M' \in C' \) such that \( M \) reaches \( M' \)?
Cube-reachability

A cube is a boolean combination of constraints $a \leq \#q \leq b \in \mathbb{N} \in \mathbb{N} \cup \infty$.

cube-reachability: given cubes $\mathcal{C}$ and $\mathcal{C}'$, does there exist $M \in \mathcal{C}$ and $M' \in \mathcal{C}'$ such that $M$ reaches $M'$? non-elementary for conservative Petri nets
Cube-reachability

A **cube** is a boolean combination of constraints

\[ a \leq \#q \leq b \]

\(\in \mathbb{N}\) \(\in \mathbb{N} \cup \infty\)

**cube-reachability**: given cubes \(\mathcal{C}\) and \(\mathcal{C}'\), does there exist \(M \in \mathcal{C}\) and \(M' \in \mathcal{C}'\) such that \(M\) reaches \(M'\) ?

**PSPACE-complete for IO nets**

**non-elementary for conservative Petri nets**
**Cube-reachability**

A **cube** is a boolean combination of constraints

\[ a \leq \#q \leq b \in \mathbb{N} \]

**cube-reachability**: given cubes \( \mathcal{C} \) and \( \mathcal{C}' \), does there exist \( M \in \mathcal{C} \) and \( M' \in \mathcal{C}' \) such that \( M \) reaches \( M' \)?

- Correctness of IO population protocols is in PSPACE
- [Esparza, Raskin, W.-K., '19]

- [Esparza, Raskin, W.-K., '19]

- **PSPACE-complete** for IO nets

- non-elementary for conservative Petri nets
Main idea
Main idea

$p_1$

$p_2$

$p_3$

$M$

$p_1$

$p_2$

$p_3$

$t_1$

$t_2$

$t_3$

$t_4$
Main idea

$p_1$

$p_2$

$p_3$

$M$

$M'$
Pruning

$n = \text{number of places}$
Pruning

\[ n = \text{number of places} \]

\[ \leq M \leq M' \]
Pruning

\[ \leq M \]

preserves
- support of initial and final markings
- validity of firing sequence

\[ \leq M' \]

\( n = \text{number of places} \)
Boosting preserves

- support of initial and final markings
- validity of firing sequence
Boosting

preserves
• support of initial and final markings
• validity of firing sequence
Boosting

preserves
• support of initial and final markings
• validity of firing sequence

$\geq M$ $\geq M'$

C. Weil-Kennedy, TUM
Main idea

A **cube** is a boolean combination of constraints \( a \leq \#q \leq b \in \mathbb{N} \cup \infty \).

**cube-reachability**: given cubes \( C \) and \( C' \), does there exist \( M \in C \) and \( M' \in C' \) such that \( M \) reaches \( M' \)?
Main idea

A **cube** is a boolean combination of constraints

\[ a \leq \#q \leq b \]

\( \in \mathbb{N} \) \( \in \mathbb{N} \cup \infty \)

cube-reachability: given cubes \( \mathcal{C} \) and \( \mathcal{C}' \), does there exist \( M \in \mathcal{C} \) and \( M' \in \mathcal{C}' \) such that \( M \) reaches \( M' \)?

\( \leq n \cdot n^2 \)
+ lower bound \( \mathcal{C} \)
+ lower bound \( \mathcal{C}' \)
Main idea

A **cube** is a boolean combination of constraints $a \leq \#q \leq b$ where $a, b \in \mathbb{N}$ and $\#q \in \mathbb{N} \cup \{\infty\}$.

**cube-reachability**: given cubes $\mathcal{C}$ and $\mathcal{C}'$, does there exist $M \in \mathcal{C}$ and $M' \in \mathcal{C}'$ such that $M$ reaches $M'$?

- $\mathbb{NPSPACE} = \mathbb{PSPACE}$
- non-deterministically pick small markings $M_0$ and $M'_0$
- check if $M_0$ reaches $M'_0$

$\leq n \cdot n^2$
+ lower bound $\mathcal{C}$
+ lower bound $\mathcal{C}'$
Main idea

A **cube** is a boolean combination of constraints

\[
a \leq \#q \leq b
\]

\[
\in \mathbb{N} \quad \in \mathbb{N} \cup \infty
\]

cube-reachability: given cubes \( \mathcal{C} \) and \( \mathcal{C}' \), does there exist \( M \in \mathcal{C} \) and \( M' \in \mathcal{C}' \) such that \( M \) reaches \( M' \)?

- \( \text{NPSPACE} = \text{PSPACE} \)
- non-deterministically pick small markings \( M_0 \) and \( M'_0 \)
- check if \( M_0 \) reaches \( M'_0 \)

\( \leq n \cdot n^2 \)

+ lower bound \( \mathcal{C} \)
+ lower bound \( \mathcal{C}' \)

**PSPACE**
Parameterized problems

A **cube** is a boolean combination of constraints $a \leq \#q \leq b$ such that $a, b \in \mathbb{N}$ or $a, b \in \mathbb{N} \cup \{\infty\}$.

**cube-reachability**: given cubes $\mathcal{C}$ and $\mathcal{C}'$, does there exist $M \in \mathcal{C}$ and $M' \in \mathcal{C}'$ such that $M$ reaches $M'$?

**Parameterized problems**: verifying predicates using boolean operators and reachability operators $\text{pre}^*$ and $\text{post}^*$ over cubes.

**PSPACE**
Parameterized problems

A **cube** is a boolean combination of constraints $a \leq \#q \leq b$ $\in \mathbb{N}$ $\in \mathbb{N} \cup \infty$

**cube-reachingability**: given cubes $\mathcal{C}$ and $\mathcal{C}'$, does there exist $M \in \mathcal{C}$ and $M' \in \mathcal{C}'$ such that $M$ reaches $M'$?

**PSPACE**

**parameterized problems**: verifying predicates using boolean operators and reachability operators $pre^*$ and $post^*$ over cubes

**PSPACE**

$pre^*(\mathcal{C})$ is the set of markings that can reach $\mathcal{C}$

$post^*(\mathcal{C})$ is the set of markings that $\mathcal{C}$ can reach
Parameterized problems

A **cube** is a boolean combination of constraints

\[ a \leq \#q \leq b \]

\[ \in \mathbb{N} \quad \in \mathbb{N} \cup \infty \]

cube-reachability: given cubes \( C \) and \( C' \), does there exist \( M \in C \) and \( M' \in C' \) such that \( M \) reaches \( M' \)?

**PSPACE**

**parameterized problems**: verifying predicates using boolean operators and reachability operators \( pre^* \) and \( post^* \) over cubes

**PSPACE**

\( pre^*(C) \) is the set of markings that can reach \( C \)

\( post^*(C) \) is the set of markings that \( C \) can reach

\[ e.g. \text{ reachability from cube } C \text{ to cube } C': \quad post^*(C) \cap C' \neq \emptyset \]
Parameterized problems

A **cube** is a boolean combination of constraints \( a \leq \# q \leq b \) \( \in \mathbb{N} \) \( \in \mathbb{N} \cup \infty \)

**cube-reachability**: given cubes \( C \) and \( C' \), does there exist \( M \in C \) and \( M' \in C' \) such that \( M \) reaches \( M' \)?

**parameterized problems**: verifying predicates using boolean operators and reachability operators \( pre^* \) and \( post^* \) over cubes

\( e.g. \) almost-sure reachability from cube \( C_{init} \) to cube \( C_{final} \)
Parameterized problems

A **cube** is a boolean combination of constraints

\[ a \leq \#q \leq b \]

\[ \in \mathbb{N} \quad \in \mathbb{N} \cup \mathbb{\infty} \]

cube-reachability: given cubes \( C \) and \( C' \), does there exist \( M \in C \) and \( M' \in C' \) such that \( M \) reaches \( M' \) ?

**PSPACE**

**Parameterized problems**: verifying predicates using boolean operators and reachability operators \( pre^* \) and \( post^* \) over cubes

**PSPACE**

e.g. almost-sure reachability from cube \( C_{init} \) to cube \( C_{final} \)

\[ post^*(C_{init}) \subseteq pre^*(C_{final}) \]
IO nets are flat

Flat

\[ \exists \text{ sequence } t_1^* t_2^* \ldots t_\ell^* \text{ such that } \forall M_0 \forall M, \ M_0 \rightarrow^* M \text{ iff } M_0 \xrightarrow{t_1^k t_2^k \ldots t_\ell^k} M \]

[Leroux, Sutre, ‘05]
IO nets are flat

Flat

∃ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0 \forall M$, $M_0 \rightarrow^* M$ iff $M_0 \xrightarrow{t_1^k t_2^k \ldots t_\ell^k} M$

[Leroux, Sutre, ’05]

check reachability properties with model checking tools that use acceleration techniques e.g. FAST [Bardin, Finkel, Leroux, Petrucci, ’03]
Part 2:
Branching immediate observation nets
Branching immediate observation nets

Immediate Observation nets (IO)

- Conservative
- Communication

C. Weil-Kennedy, TUM
Branching immediate observation nets

Immediate Observation nets (IO)

- Conservative
- Communication
Branching immediate observation nets

Immediate Observation nets (IO)

- Conservative
- Communication

Branching Parallel Processes (BPP)

- Token creation and destruction
- Communication-free

[Christensen et al., '93] [Yen, '97] [Lasota, '09] [Mayr, Weihmann, '15]
Branching immediate observation nets

Immediate Observation nets (IO)
- Conservative
- Communication

Branching Parallel Processes (BPP)
- Token creation and destruction
- Communication-free

[Christensen et al., '93] [Yen, '97] [Lasota, '09] [Mayr, Weihmann, '15]
Branching immediate observation nets

Immediate Observation nets (IO)

- Conservative
- Communication

Branching Parallel Processes (BPP)

- Token creation and destruction
- Communication-free

Branching Immediate Observation nets (BIO)

- Token creation and destruction
- Communication

[Christensen et al., '93][Yen, '97][Lasota, '09][Mayr, Weihmann, '15][Esparza, Raskin, W.-K., '20]
Branching immediate observation nets

Immediate Observation nets (IO)
- Conservative
- Communication

Branching Parallel Processes (BPP)
- Token creation and destruction
- Communication-free

Branching Immediate Observation nets (BIO)
- Token creation and destruction
- Communication

[Christensen et al., '93] [Yen, '97] [Lasota, '09] [Mayr, Weihmann, '15]
[Esparza, Raskin, W.-K., '20]

C. Weil-Kennedy, TUM
Cube-reachability

A **cube** is a boolean combination of constraints $a \leq \#q \leq b \in \mathbb{N}$.

**cube-reachability**: given cubes $C$ and $C'$, does there exist $M \in C$ and $M' \in C'$ such that $M$ reaches $M'$?
Cube-reachability

A cube is a boolean combination of constraints

\[ a \leq \#q \leq b \in \mathbb{N} \cup \{\infty\} \]

cube-reachability: given cubes \( C \) and \( C' \), does there exist \( M \in C \) and \( M' \in C' \) such that \( M \) reaches \( M' \)?

still PSPACE-complete!
A **cube** is a boolean combination of constraints $a \leq #q \leq b \in \mathbb{N}$. In the context of **cube-reachability**, given cubes $C$ and $C'$, does there exist $M \in C$ and $M' \in C'$ such that $M$ reaches $M'$? 

**cube-reachability** is still **PSPACE-complete**!

**Parameterized problems**: verifying predicates using boolean operators and reachability operators $\text{pre}^*$ and $\text{post}^*$ over cubes.
Non-semilinear reachability

BIO nets can have non-semilinear reachability set

[Hopcroft, Pansiot, '79] example of a 3-dimensional VASS

BIO net

\[\text{Hopcroft, Pansiot, '79}\]

\[c_2\]
\[t_1\]
\[p\]
\[c_3\]
\[t_2\]
\[t_3\]
\[t_4\]
\[q\]
\[c_1\]
Non-semilinear reachability

BIO nets can have **non-semilinear** reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS

![BIO net diagram]

C. Weil-Kennedy, TUM
Non-semilinear reachability

BIO nets can have non-semilinear reachability set

[Hopcroft, Pansiot, '79] example of a 3-dimensional VASS
Non-semilinear reachability

BIO nets can have **non-semilinear** reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS
Non-semilinear reachability

BIO nets can have non-semilinear reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS
Non-semilinear reachability

BIO nets can have non-semilinear reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS

BIO net

VASS to Petri net

classic translation
Non-semilinear reachability

BIO nets can have **non-semilinear** reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS

[BIO net]

[Classic translation: VASS to Petri net]
Non-semilinear reachability

BIO nets can have non-semilinear reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS

VASS to Petri net classic translation

C. Weil-Kennedy, TUM
Non-semilinear reachability

BIO nets can have non-semilinear reachability set

[Hopcroft, Pansiot, '79] example of a 3-dimensional VASS
Non-semilinear reachability

BIO nets can have non-semilinear reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS

C. Weil-Kennedy, TUM
Non-semilinear reachability

BIO nets can have non-semilinear reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS

\[c_2 + c_3 \leq 2^{c_1}\]
Non-semilinear reachability

BIO nets can have **non-semilinear** reachability set

[Hopcroft, Pansiot, ’79] example of a 3-dimensional VASS

Until now, unbounded Petri net classes with provably simpler reachability than the general case have semilinear reachability sets
BIO nets are locally flat

Flat

∃ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0 \forall M, \ M_0 \rightarrow M$ iff $M_0 \xrightarrow{t_1^k t_2^k \ldots t_\ell^k} M$

BIO nets are not flat…
BIO nets are locally flat

**Flat**

\[ \exists \text{ sequence } t_1^* t_2^* \ldots t_\ell^* \text{ such that } \forall M_0 \forall M, \ M_0 \rightarrow M \text{ iff } M \xrightarrow{t_1^* t_2^* \ldots t_\ell^*} M \]

BIO nets are not flat...

**Locally flat**

\[ \forall M, \ \exists \text{ sequence } t_1^* t_2^* \ldots t_\ell^* \text{ such that } \forall M_0, \ M_0 \rightarrow M \text{ iff } M \xrightarrow{t_1^* t_2^* \ldots t_\ell^*} M \]

**BIO nets are locally flat**
BIO nets are locally flat

Flat

\[ \exists \text{ sequence } t_1^* t_2^* \ldots t_\ell^* \text{ such that } \forall M_0 \forall M, \ M_0 \rightarrow^* M \iff M_0 \overset{t_1^k t_2^k \ldots t_\ell^k}{\rightarrow^*} M \]

BIO nets are not flat...

Locally flat

\[ \forall M, \ \exists \text{ sequence } t_1^* t_2^* \ldots t_\ell^* \text{ such that } \forall M_0, \ M_0 \rightarrow^* M \iff M_0 \overset{t_1^k t_2^k \ldots t_\ell^k}{\rightarrow^*} M \]

check reachability properties with model checking tools that use acceleration techniques e.g. FAST [Bardin, Finkel, Leroux, Petrucci, ’03]
Cube-reachability summary

non-elementary
[Czerwinsky, Lasota, Lazic, Leroux, Mazowiecki, ’19]
Cube-reachability summary

- General Petri nets
  - BPP
  - IO
  - Conservative

- BIO

- NP-complete [Esparza, ’97]

- non-elementary [Czerwinzki, Lasota, Lazic, Leroux, Mazowiecki, ’19]
Cube-reachability summary

non-elementary
[Czerwinzki, Lasota, Lazic, Leroux, Mazowiecki, ’19]

PSPACE-complete
[Esparza, Raskin, W.-K., ’19]

NP-complete
[Esparza, ’97]

General Petri nets

Conservative

BIO

BPP

IO

C. Weil-Kennedy, TUM
Cube-reachability summary

- General Petri nets
  - PSPACE-complete
    - [Esparza, Raskin, W.-K., ’19]
  - PSPACE-complete
    - [Esparza, Raskin, W.-K., ’20]
- BIO
- Conservative
- BPP
- IO
- NP-complete
  - [Esparza, ’97]
- non-elementary
  - [Czerwinzki, Lasota, Lazic, Leroux, Mazowiecki, ’19]
Conclusion

• IO nets introduced to model population protocols: allowed to solve correctness

• cube-parameterized problems are in PSPACE

• BIO nets generalize BPP and IO nets, still have PSPACE cube-reachability

• BIO nets are first class of Petri nets with non-semilinear reachability set and elementary reachability problem

• IO nets are flat & BIO nets are locally flat, allowing efficient model checking
Conclusion

- IO nets introduced to model population protocols: allowed to solve correctness

- cube-parameterized problems are in PSPACE

- BIO nets generalize BPP and IO nets, still have PSPACE cube-reachability

- BIO nets are first class of Petri nets with non-semilinear reachability set and elementary reachability problem

- IO nets are flat & BIO nets are locally flat, allowing efficient model checking

- in future: apply proof method to parameterized reachability in other distributed systems
Conclusion

• IO nets introduced to model population protocols: allowed to solve correctness

• cube-parameterized problems are in PSPACE

• BIO nets generalize BPP and IO nets, still have PSPACE cube-reachability

• BIO nets are first class of Petri nets with non-semilinear reachability set and elementary reachability problem

• IO nets are flat & BIO nets are locally flat, allowing efficient model checking

• in future: apply proof method to parameterized reachability in other distributed systems

Thank you!