Verification of Immediate Observation Petri Nets

Chana Weil-Kennedy, *Technical University of Munich*

joint work with Mikhail Raskin, Javier Esparza

European Research Council
Established by the European Commission

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`

[Czerwinzki, Lasota, Lazic, Leroux, Mazowiecki, '19]

Petri nets & reachability

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

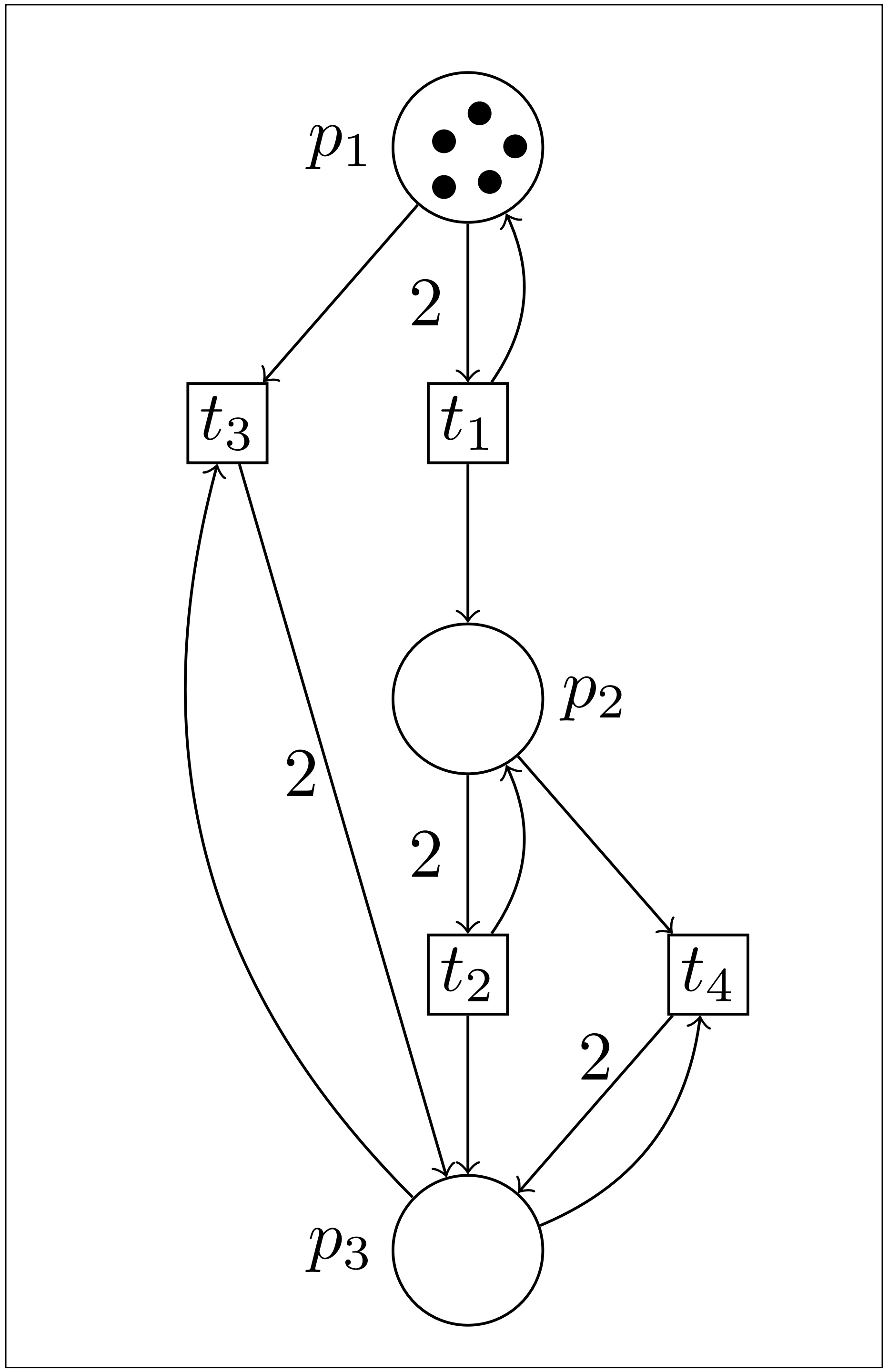
Reachability problem: Given a Petri net $\mathcal{N}$, and markings M_0 and M can marking M_0 reach marking M in $\mathcal{N}$?

`non-elementary complexity`

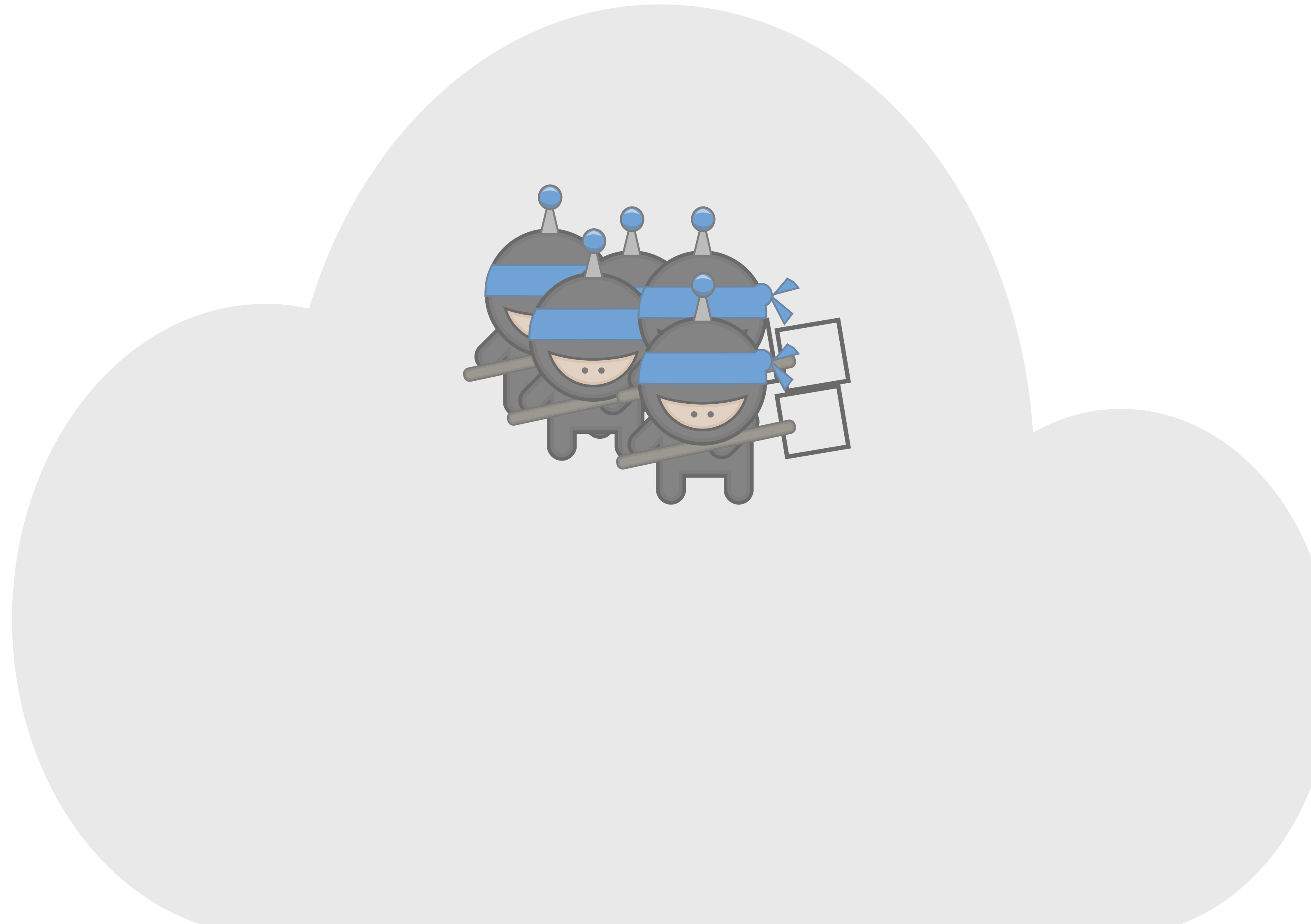
[Czerwinzki, Lasota, Lazic, Leroux, Mazowiecki, '19]

Study subclasses of Petri nets

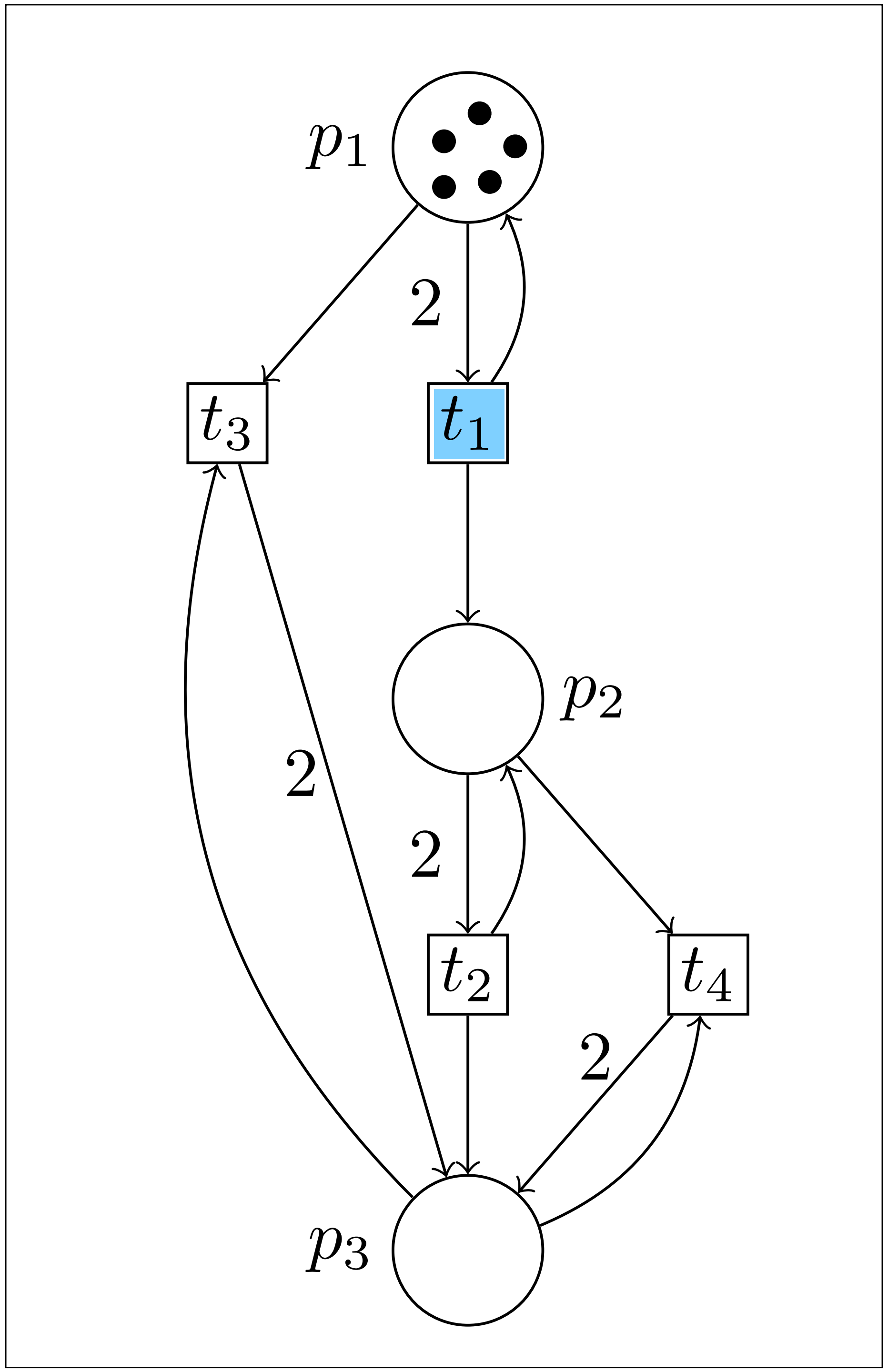
Example



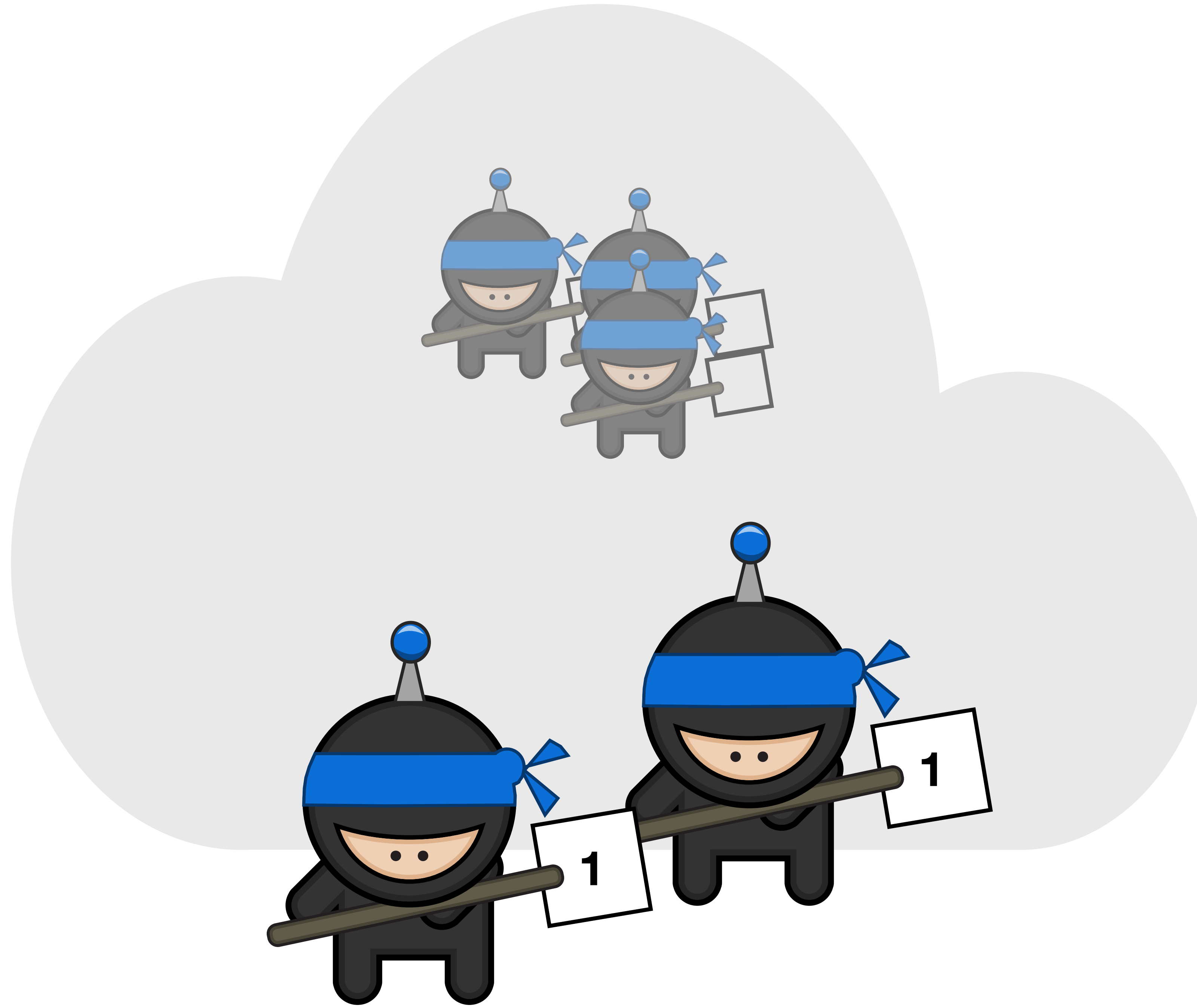
[The computational power of population protocols, Angluin et al.,'06]



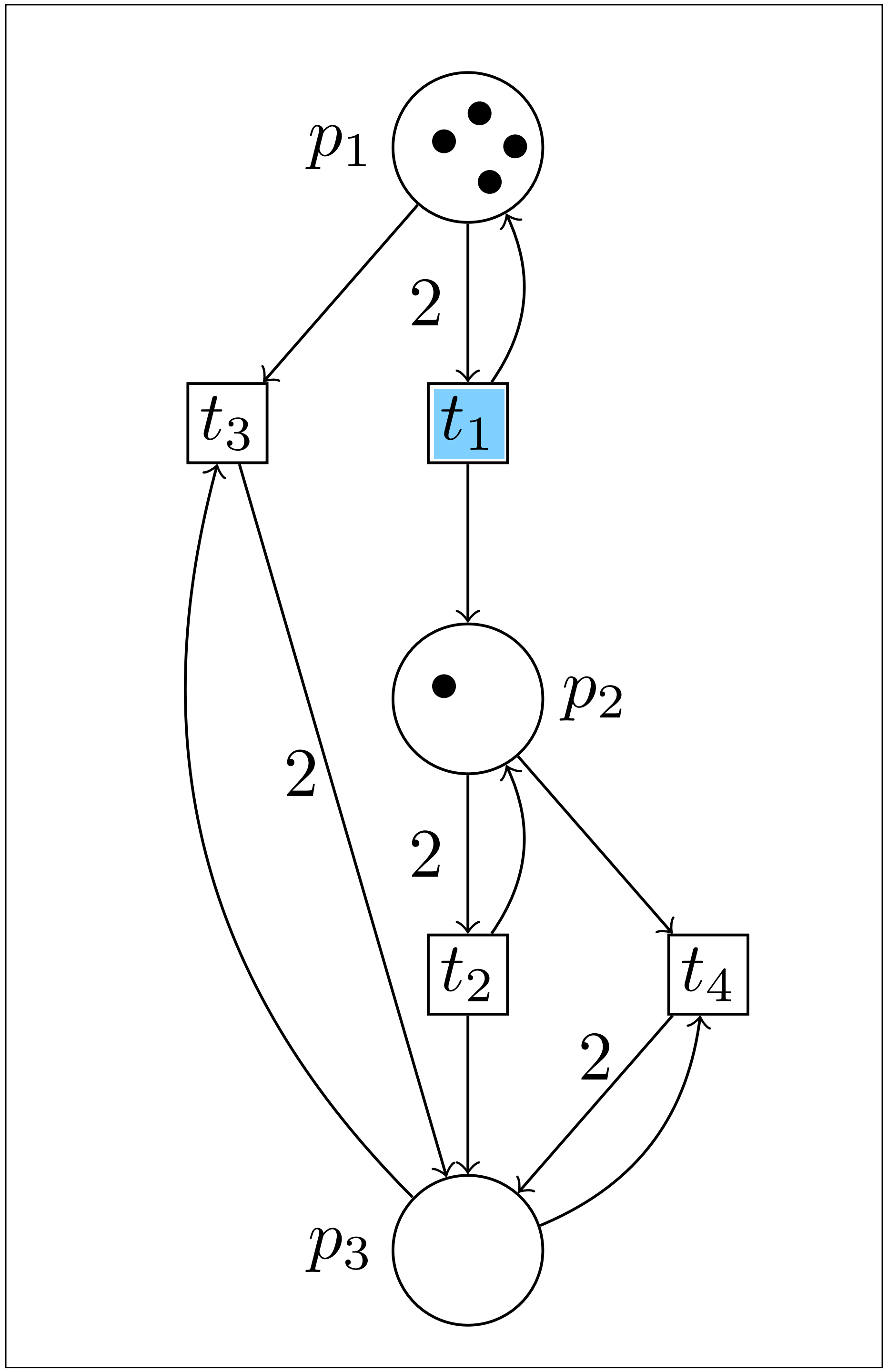
Example



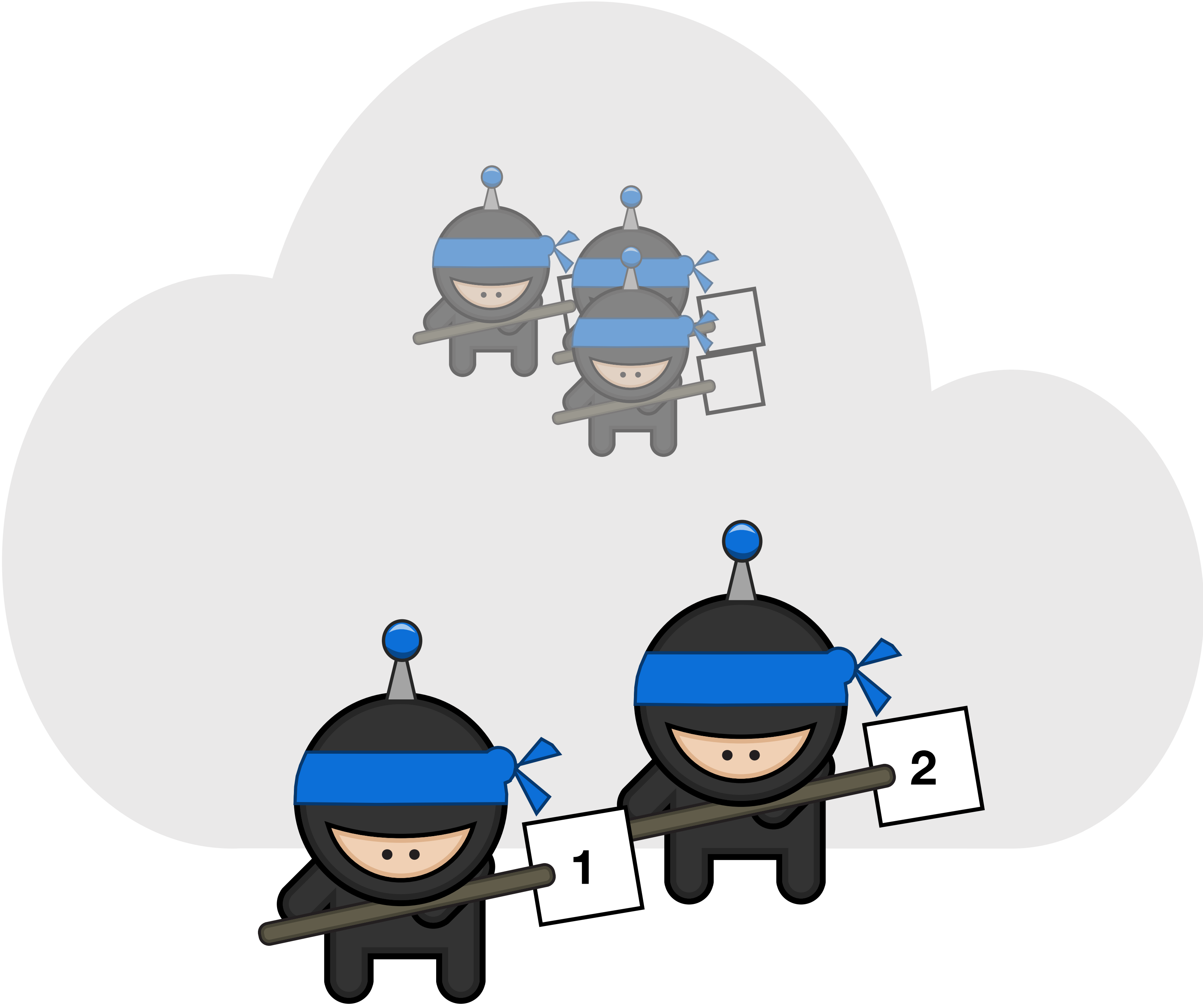
[The computational power of population protocols, Angluin et al.,'06]



Example

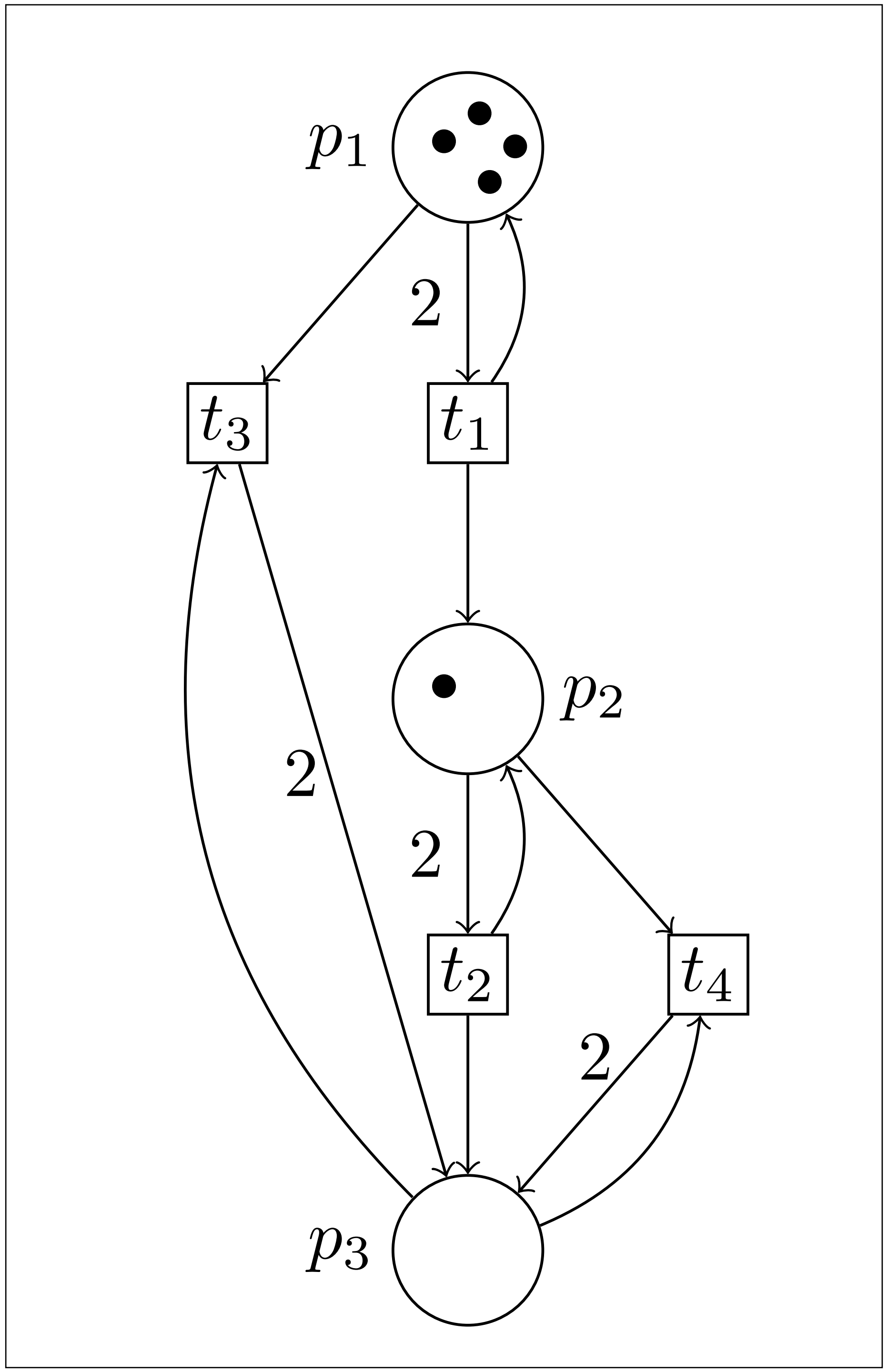


[The computational power of population protocols, Angluin et al.,'06]

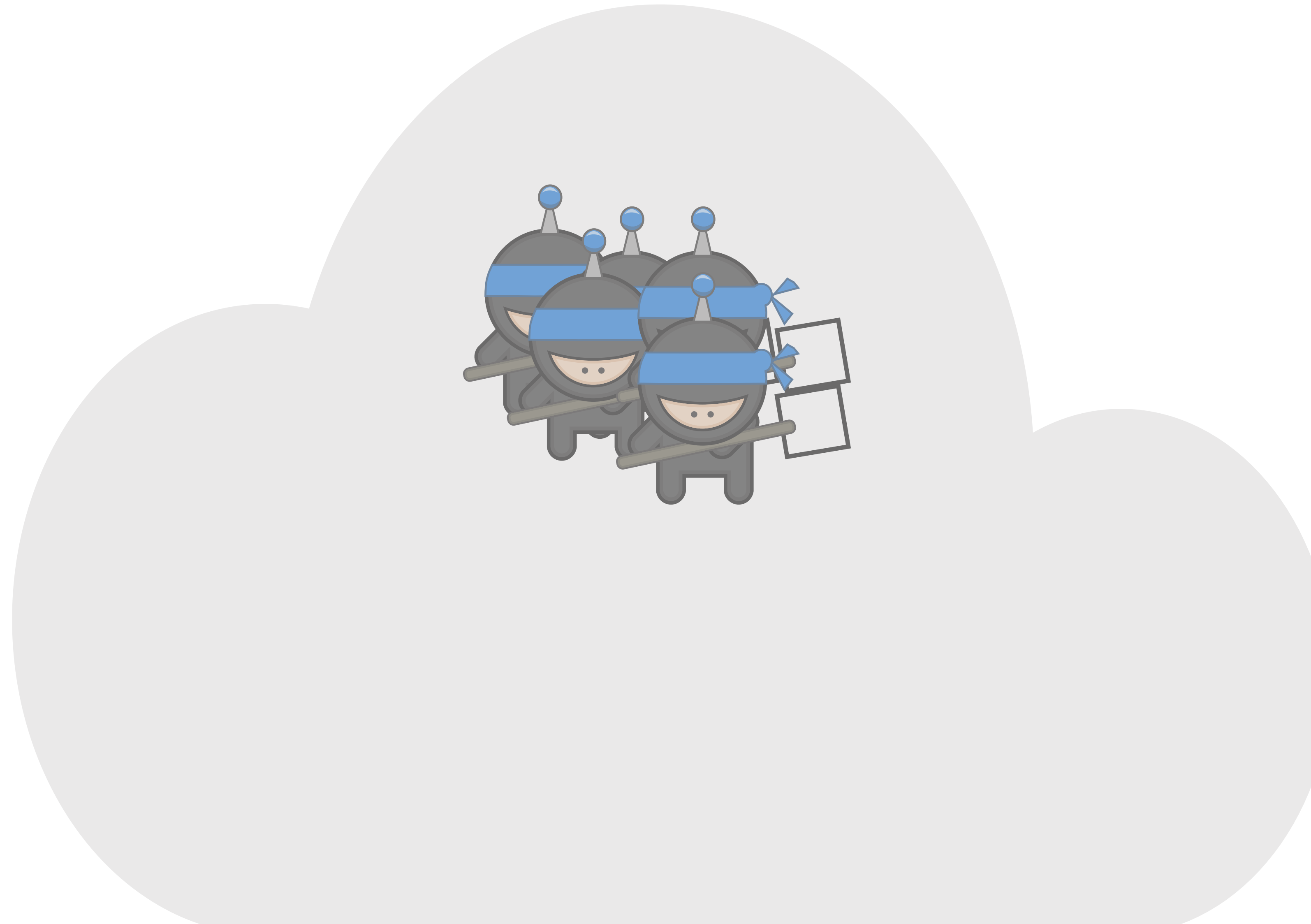


C. Weil-Kennedy, TUM

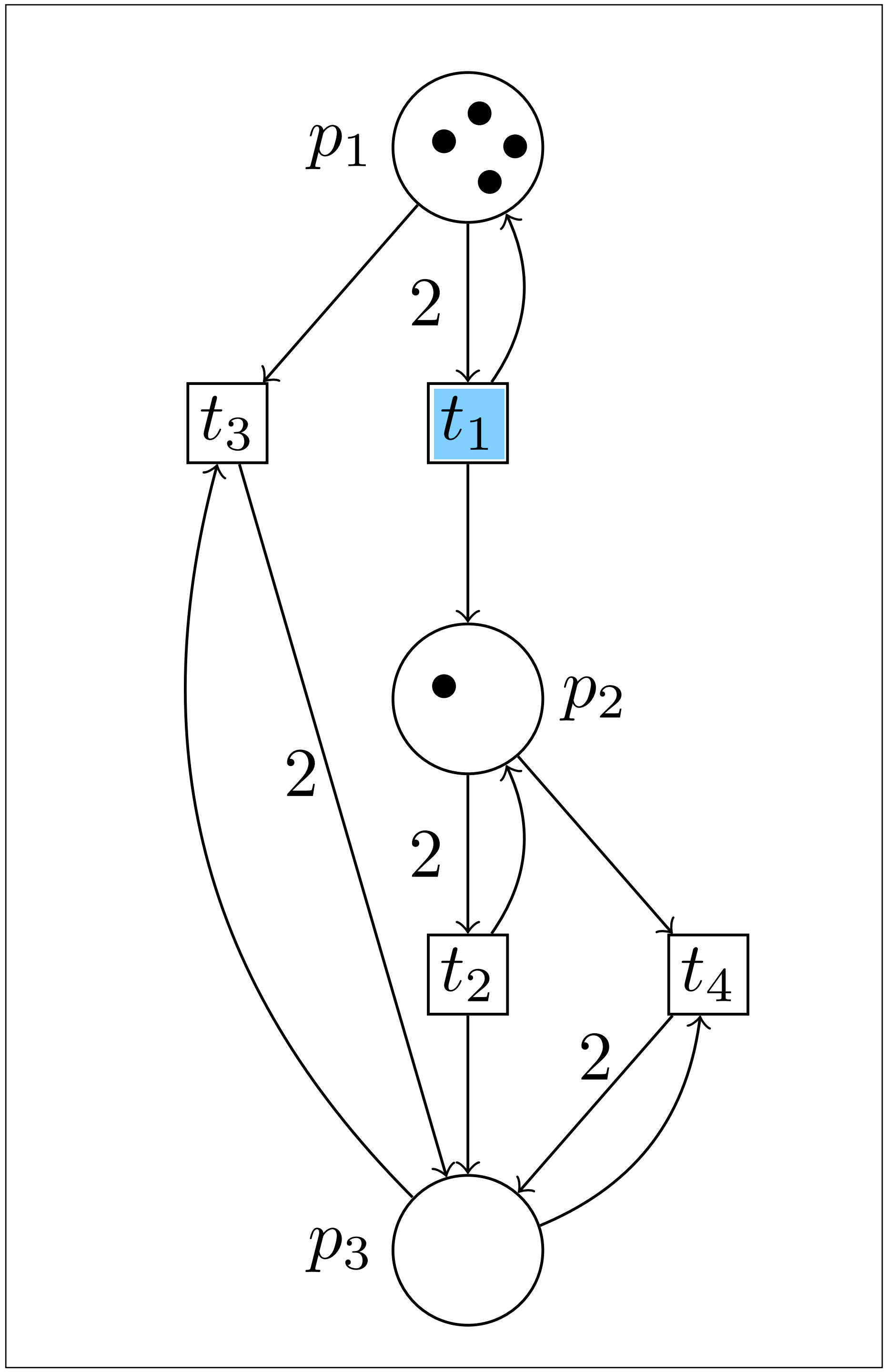
Example



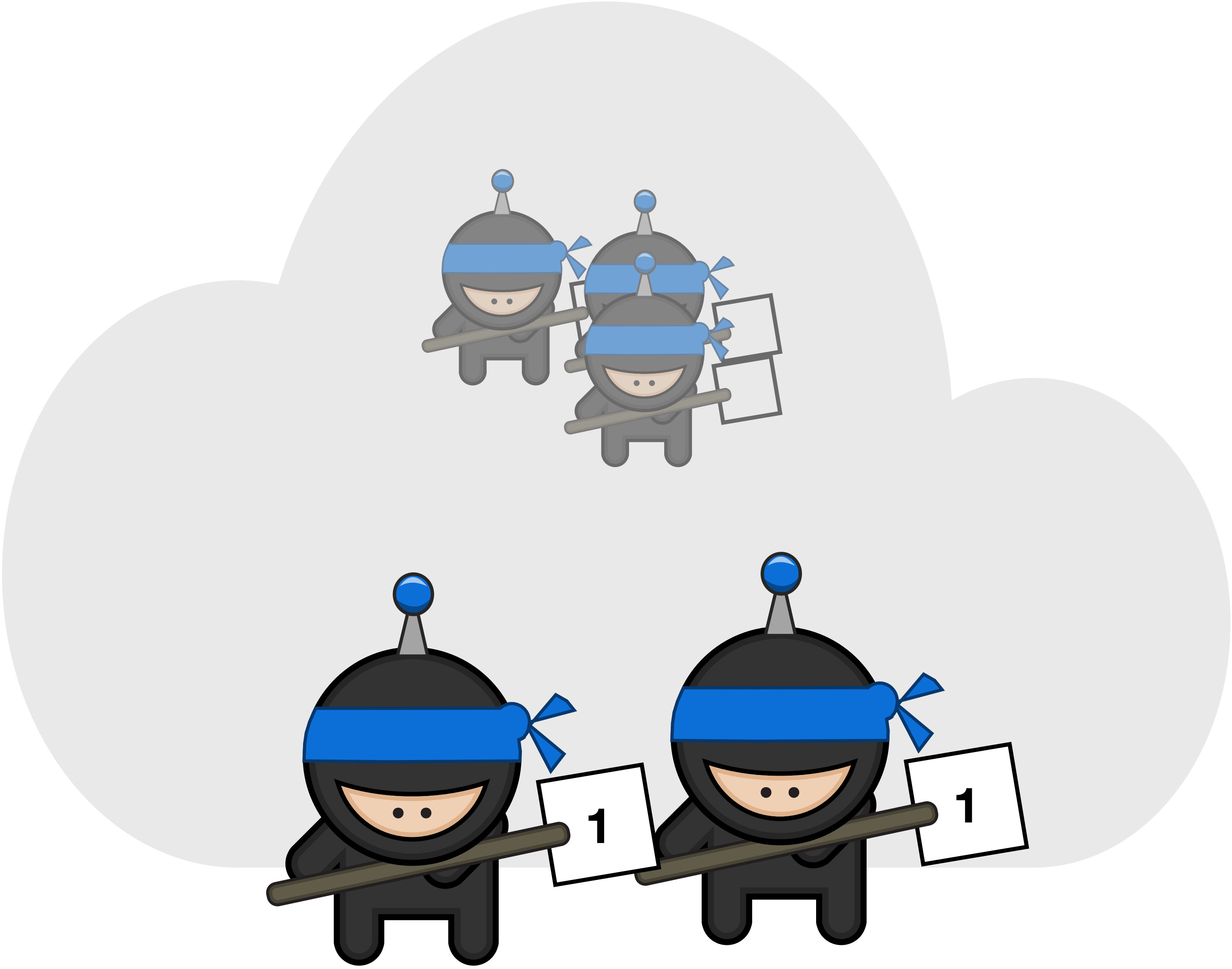
[The computational power of population protocols, Angluin et al.,'06]



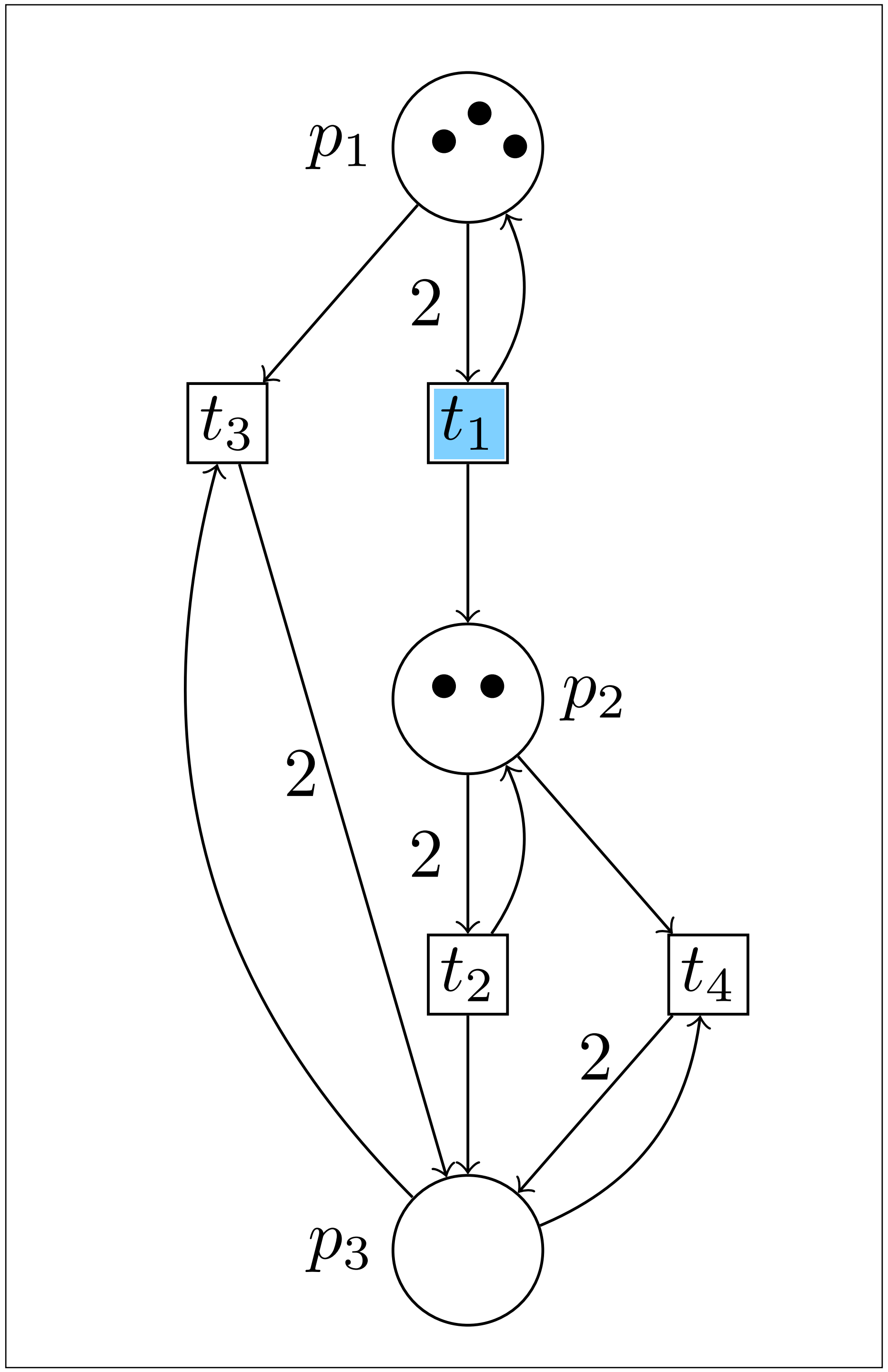
Example



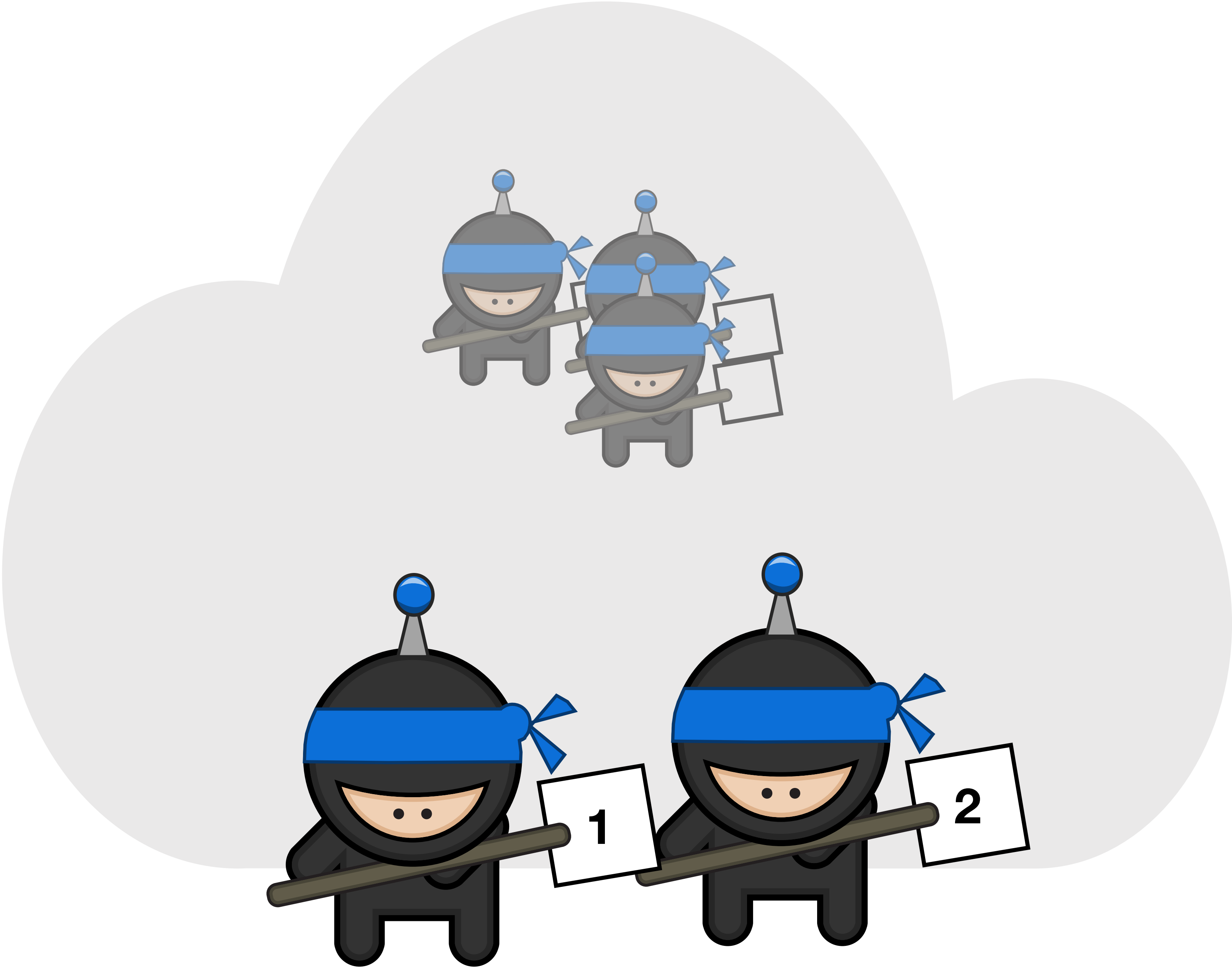
[The computational power of population protocols, Angluin et al.,'06]



Example

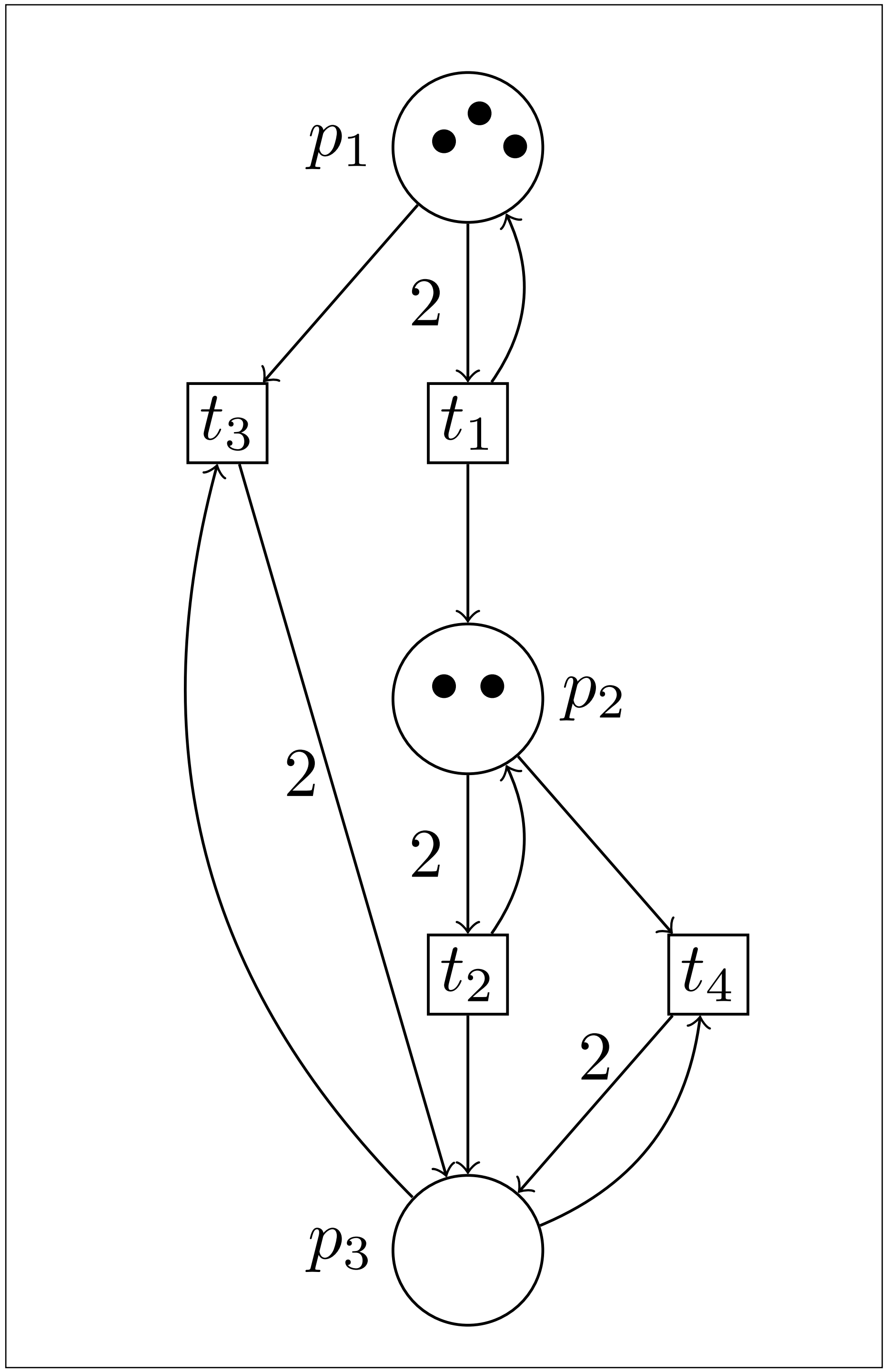


[The computational power of population protocols, Angluin et al.,'06]

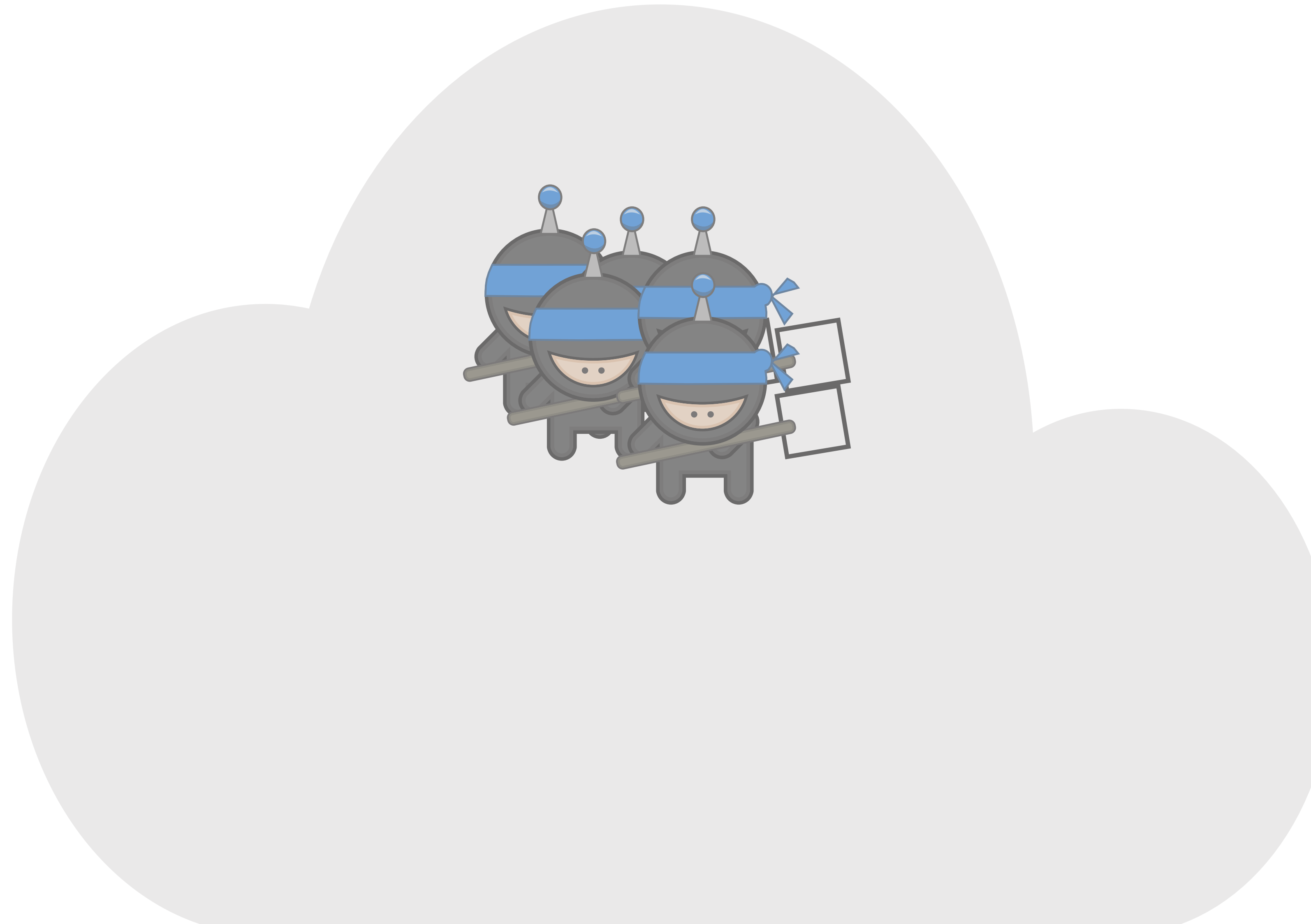


C. Weil-Kennedy, TUM

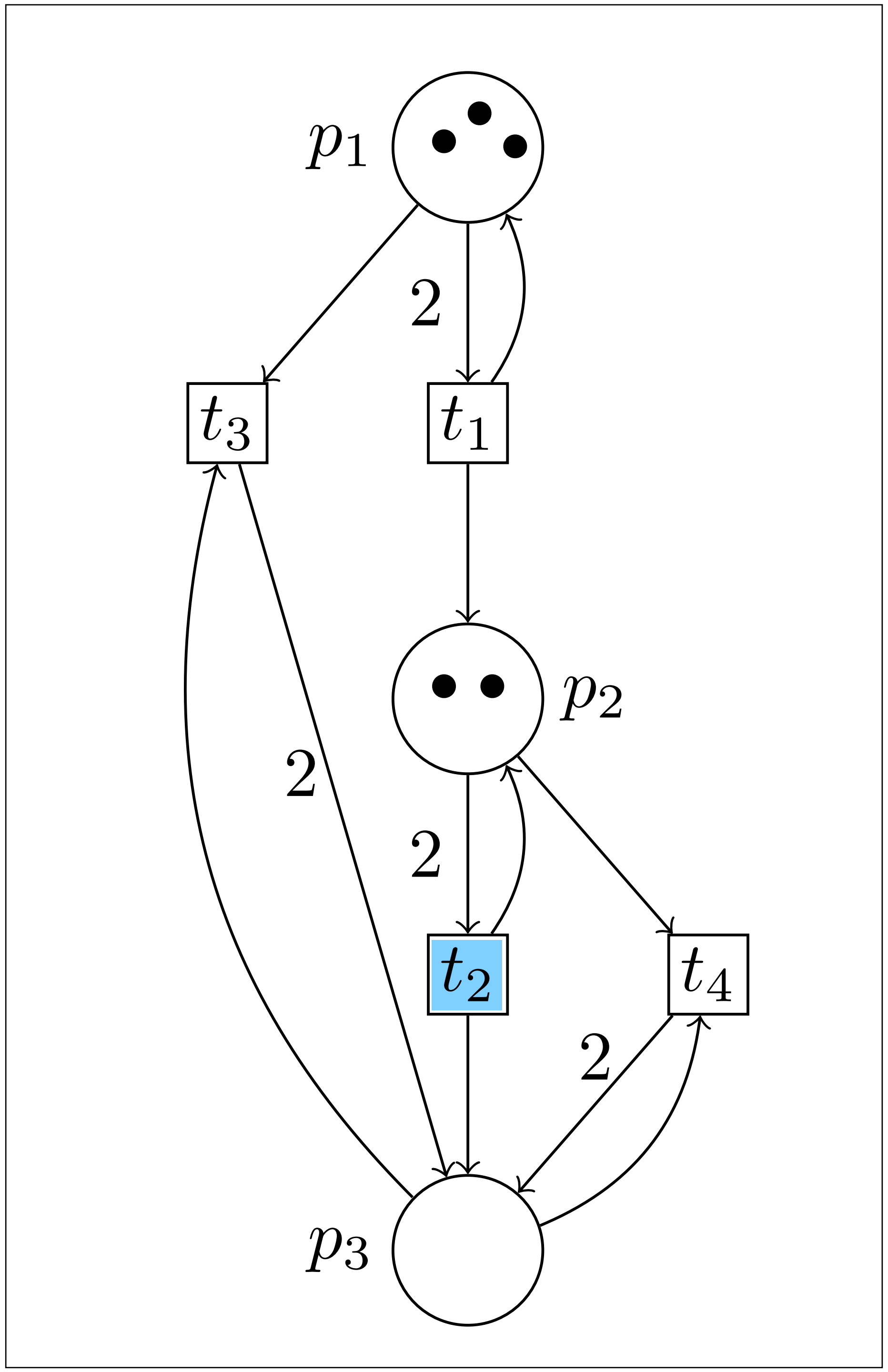
Example



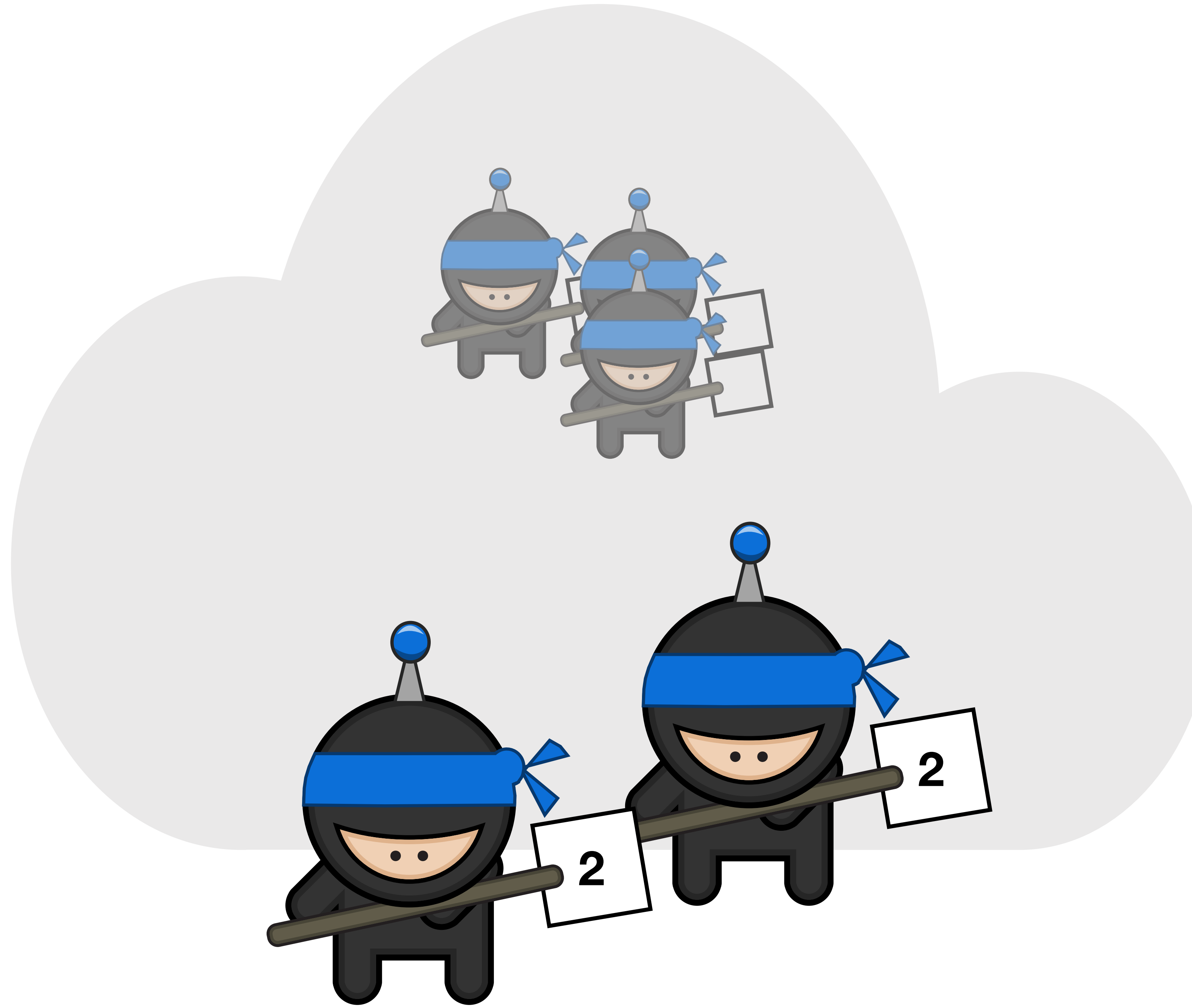
[The computational power of population protocols, Angluin et al.,'06]



Example

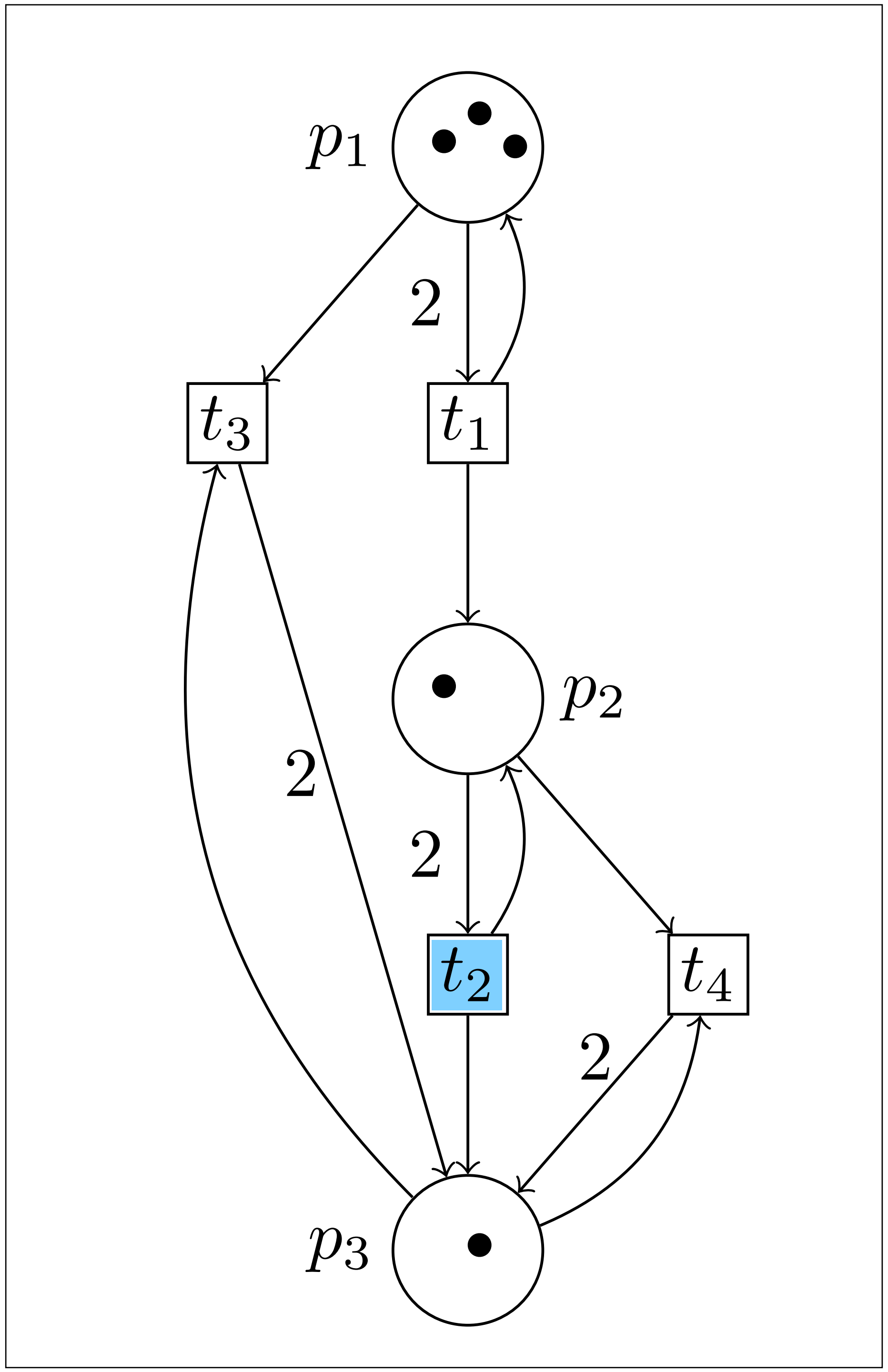


[The computational power of population protocols, Angluin et al.,'06]

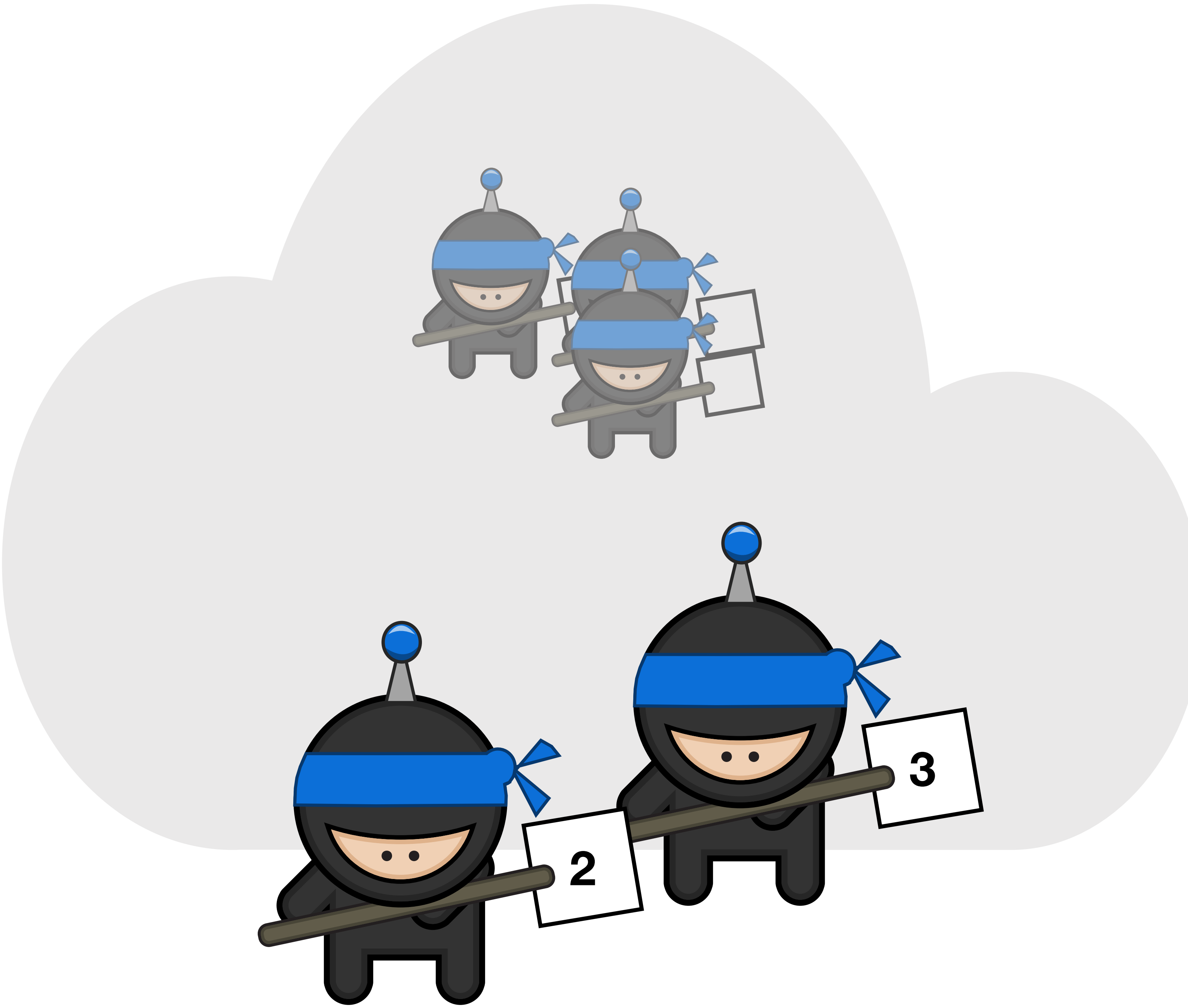


C. Weil-Kennedy, TUM

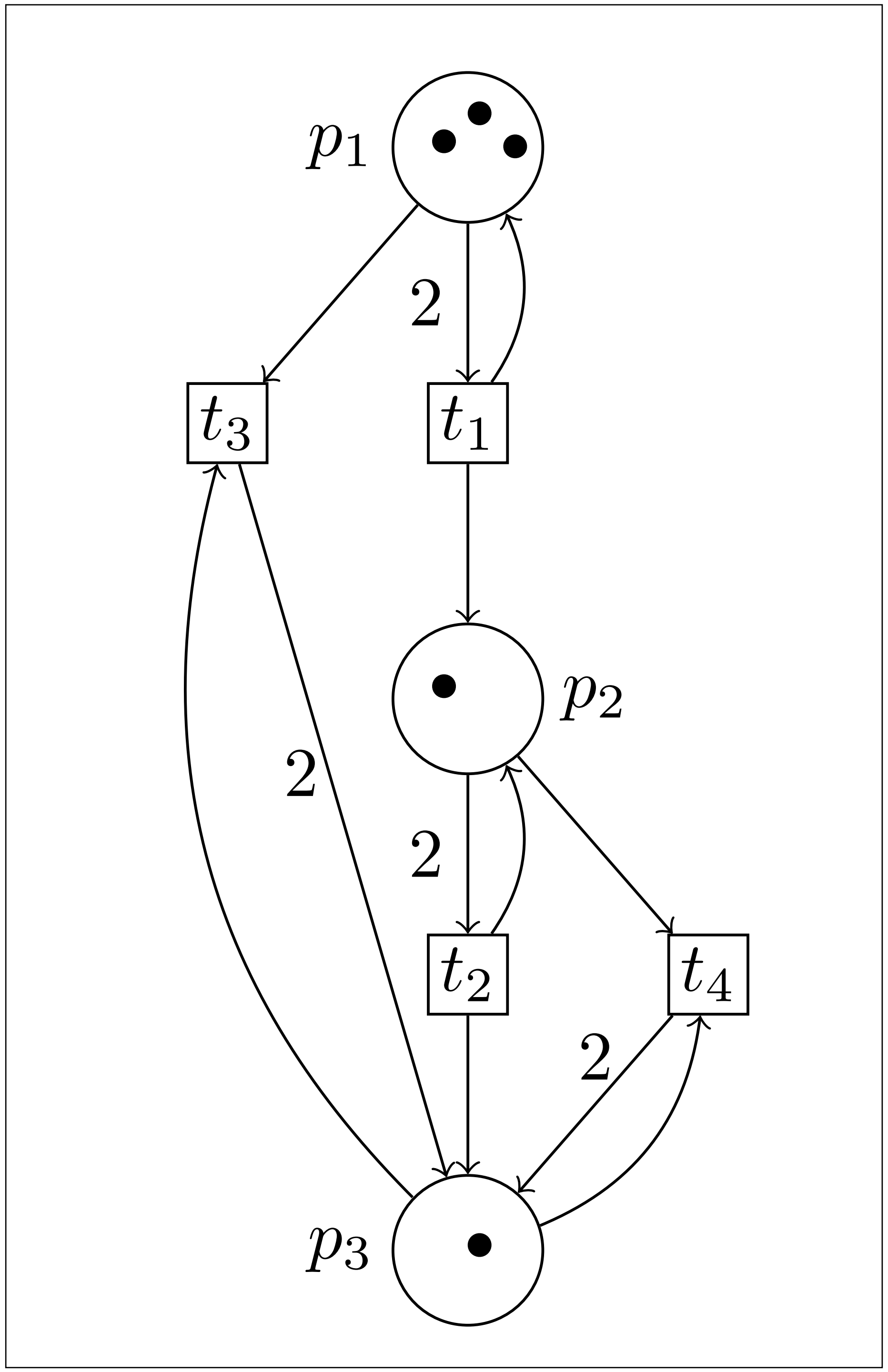
Example



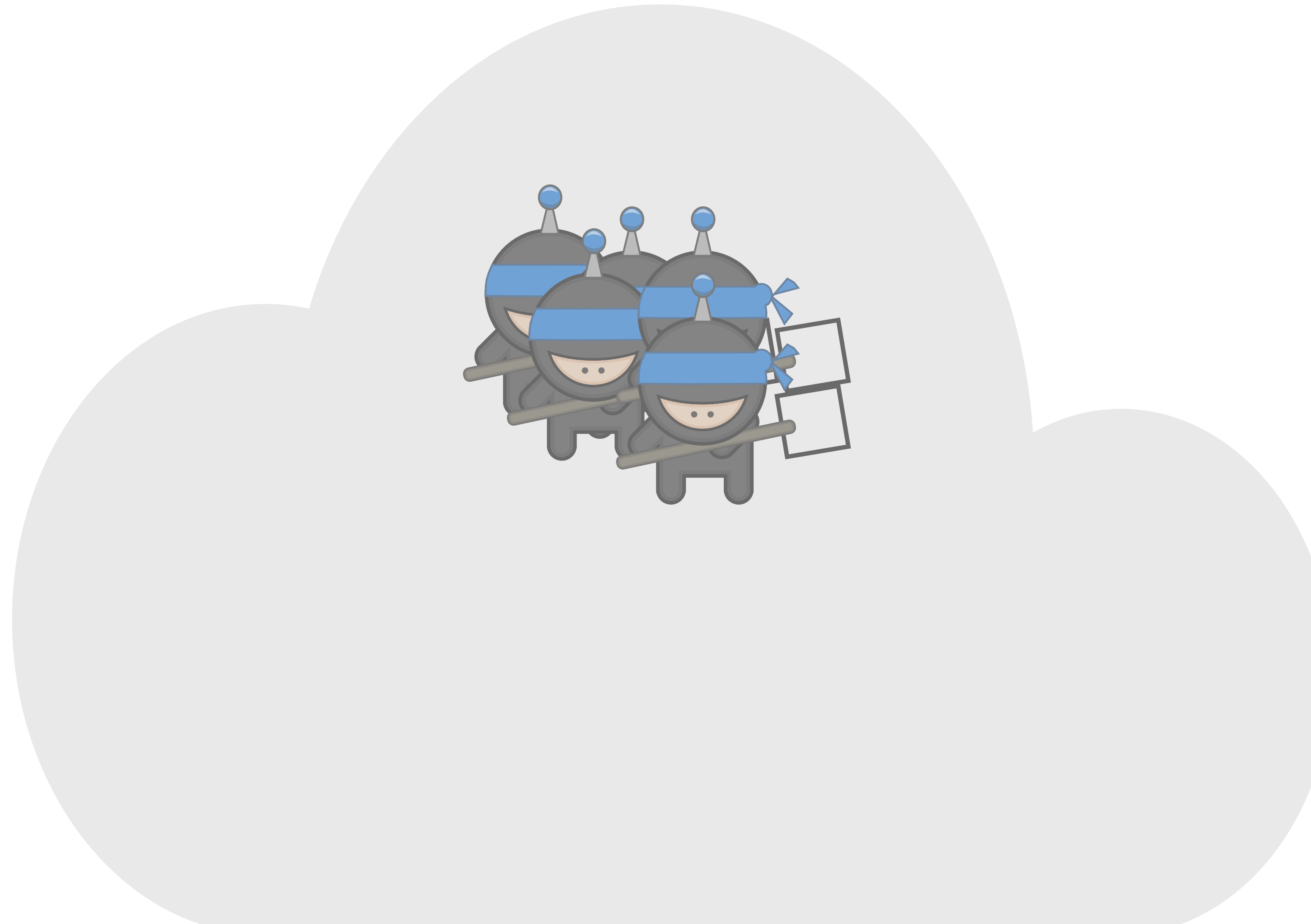
[The computational power of population protocols, Angluin et al.,'06]



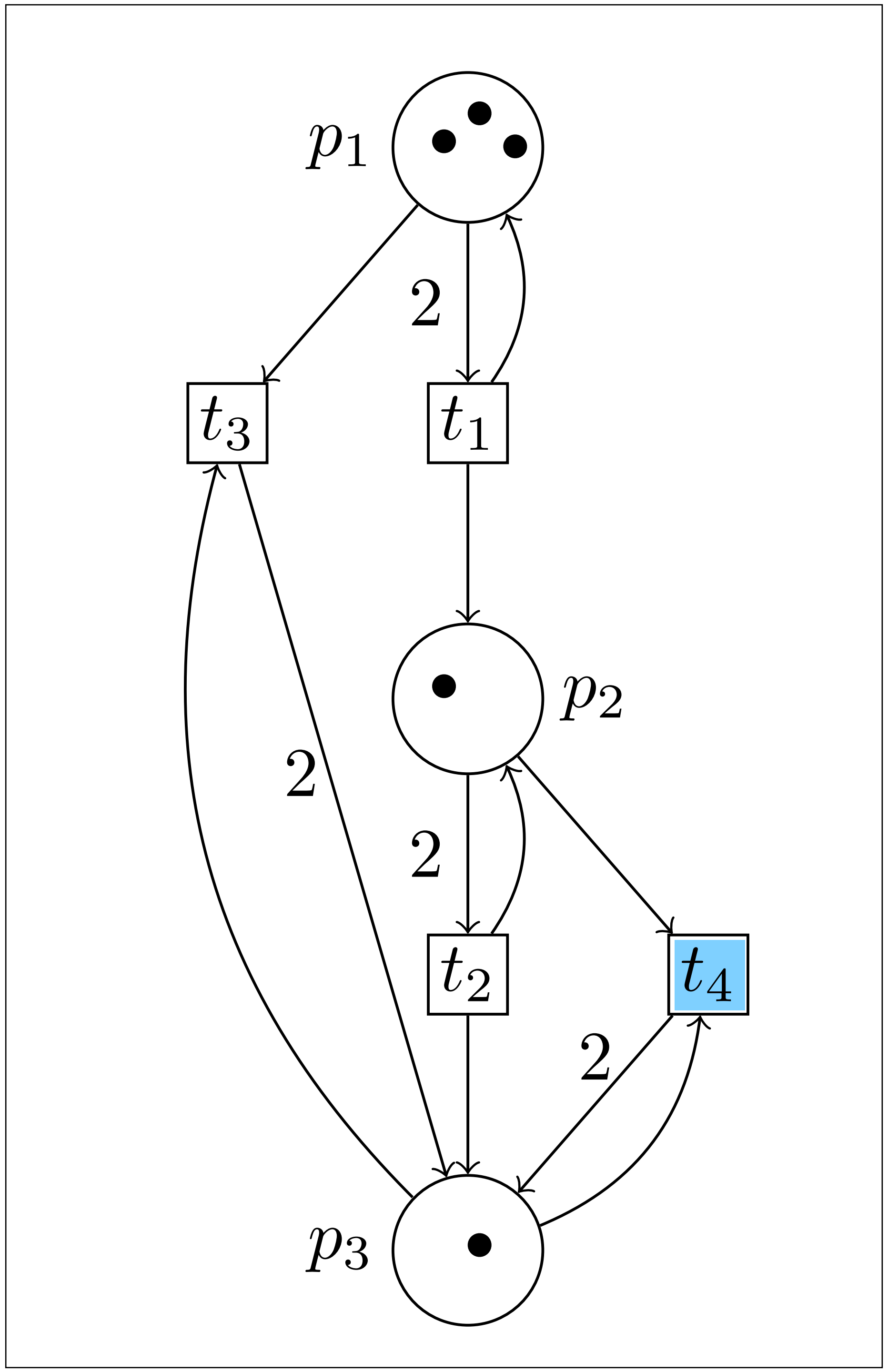
Example



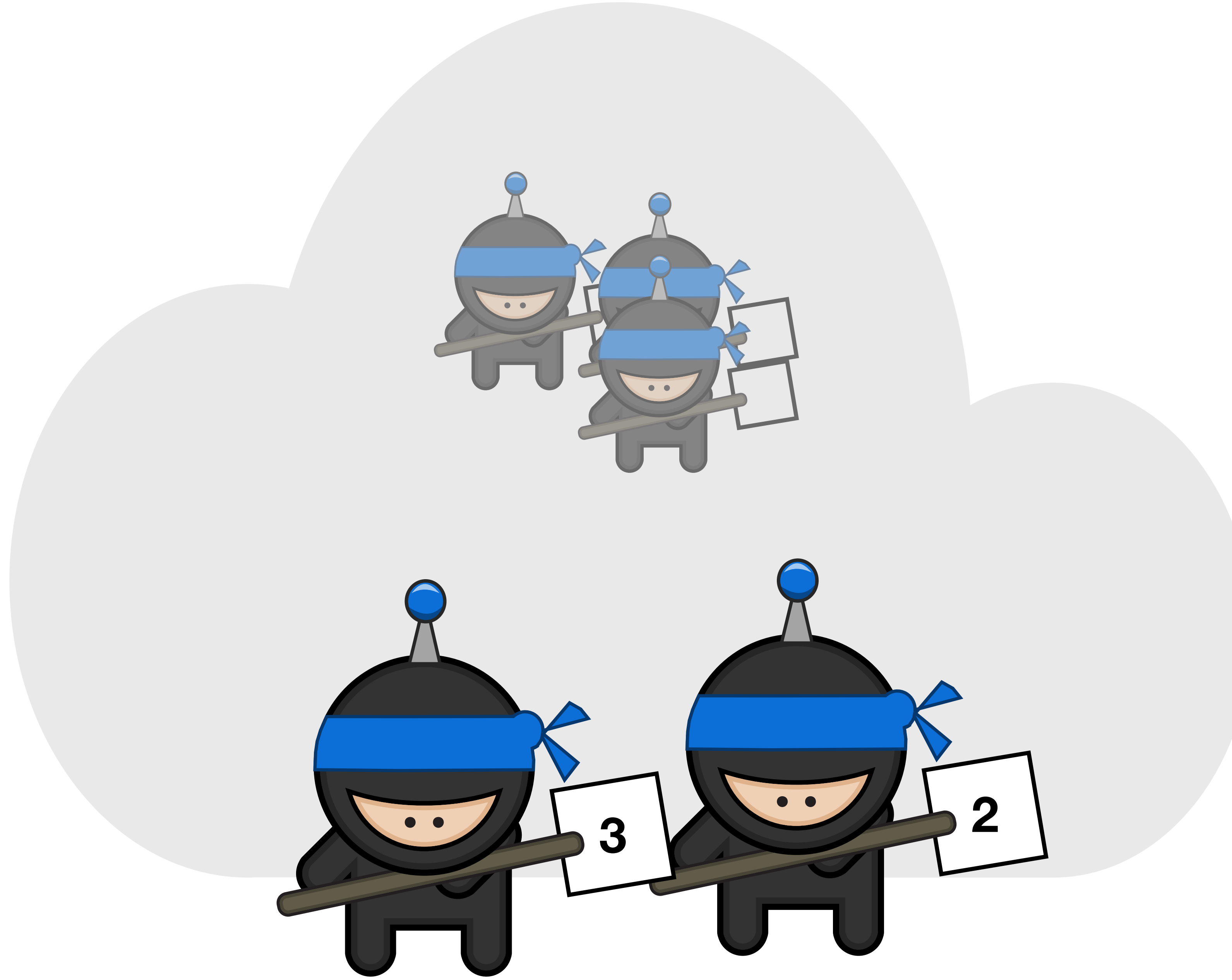
[The computational power of population protocols, Angluin et al.,'06]



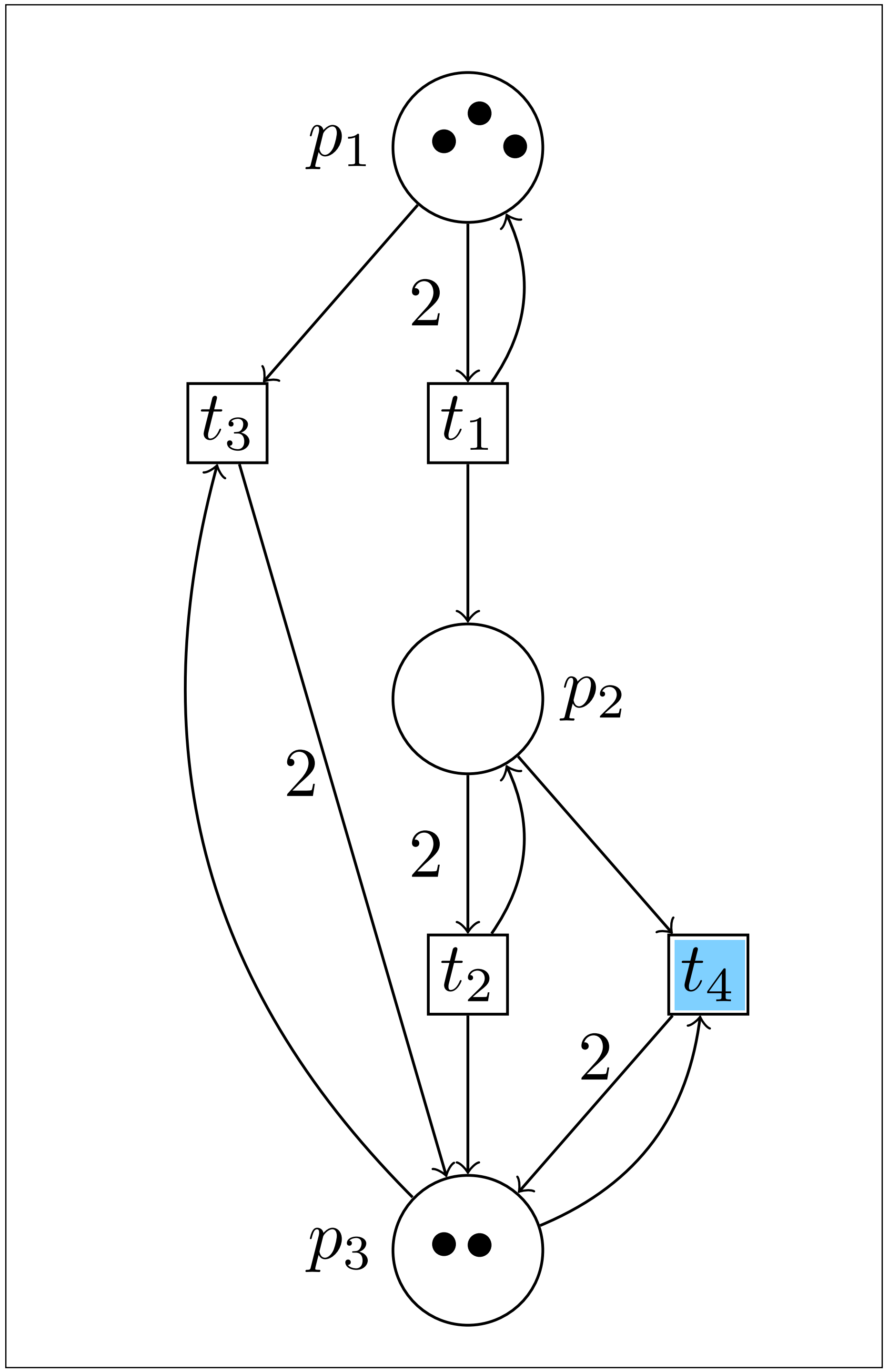
Example



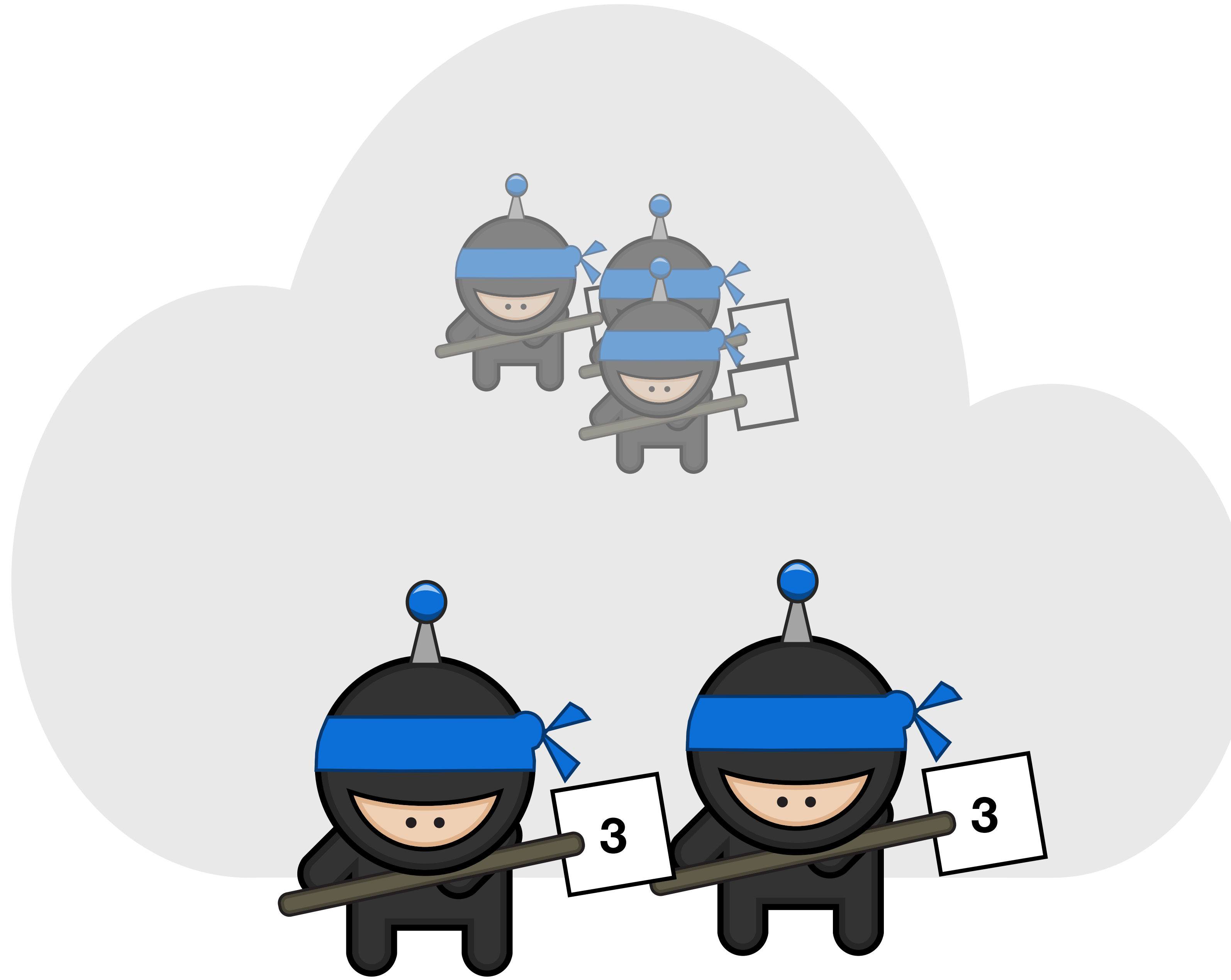
[The computational power of population protocols, Angluin et al.,'06]



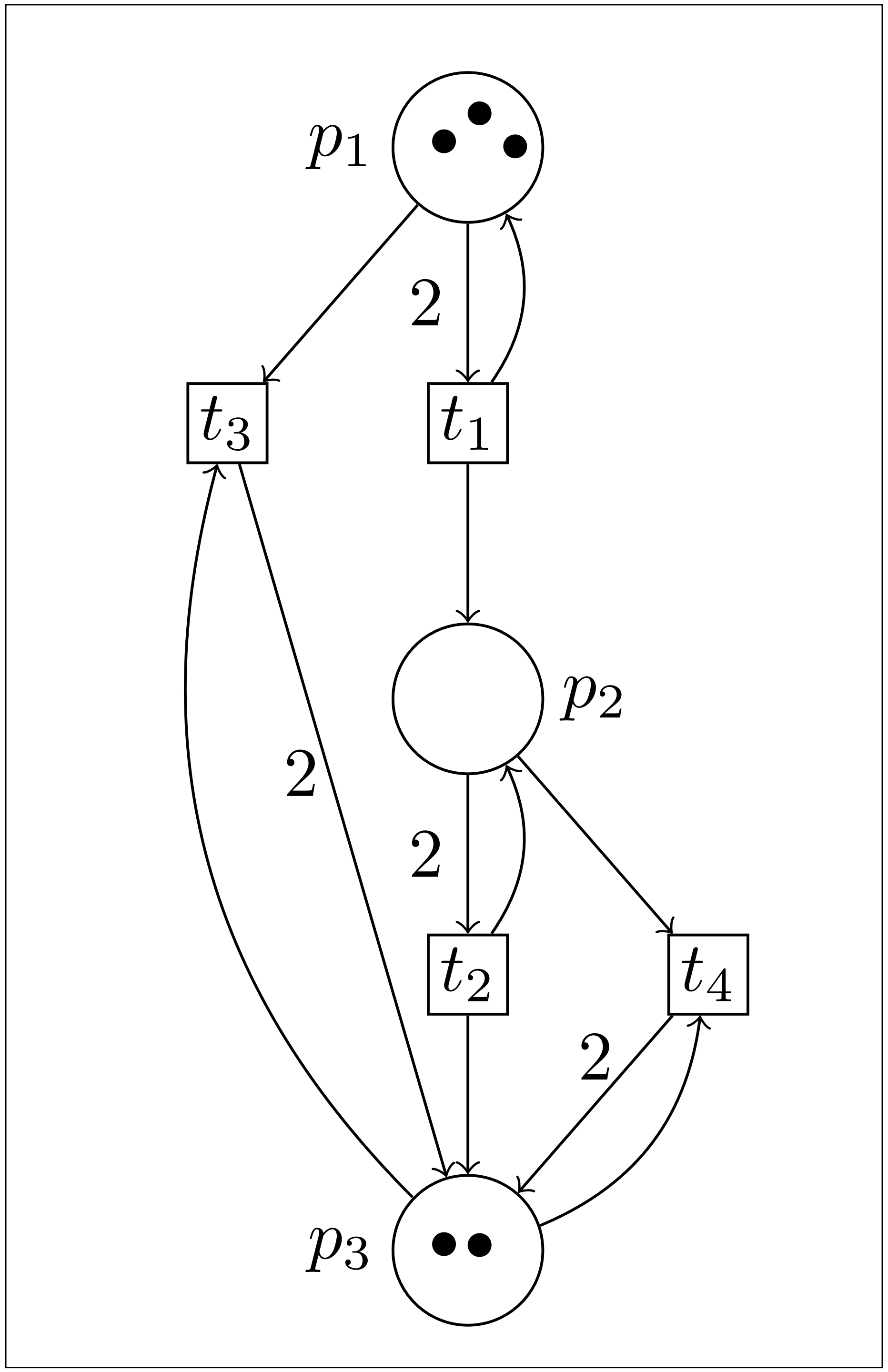
Example



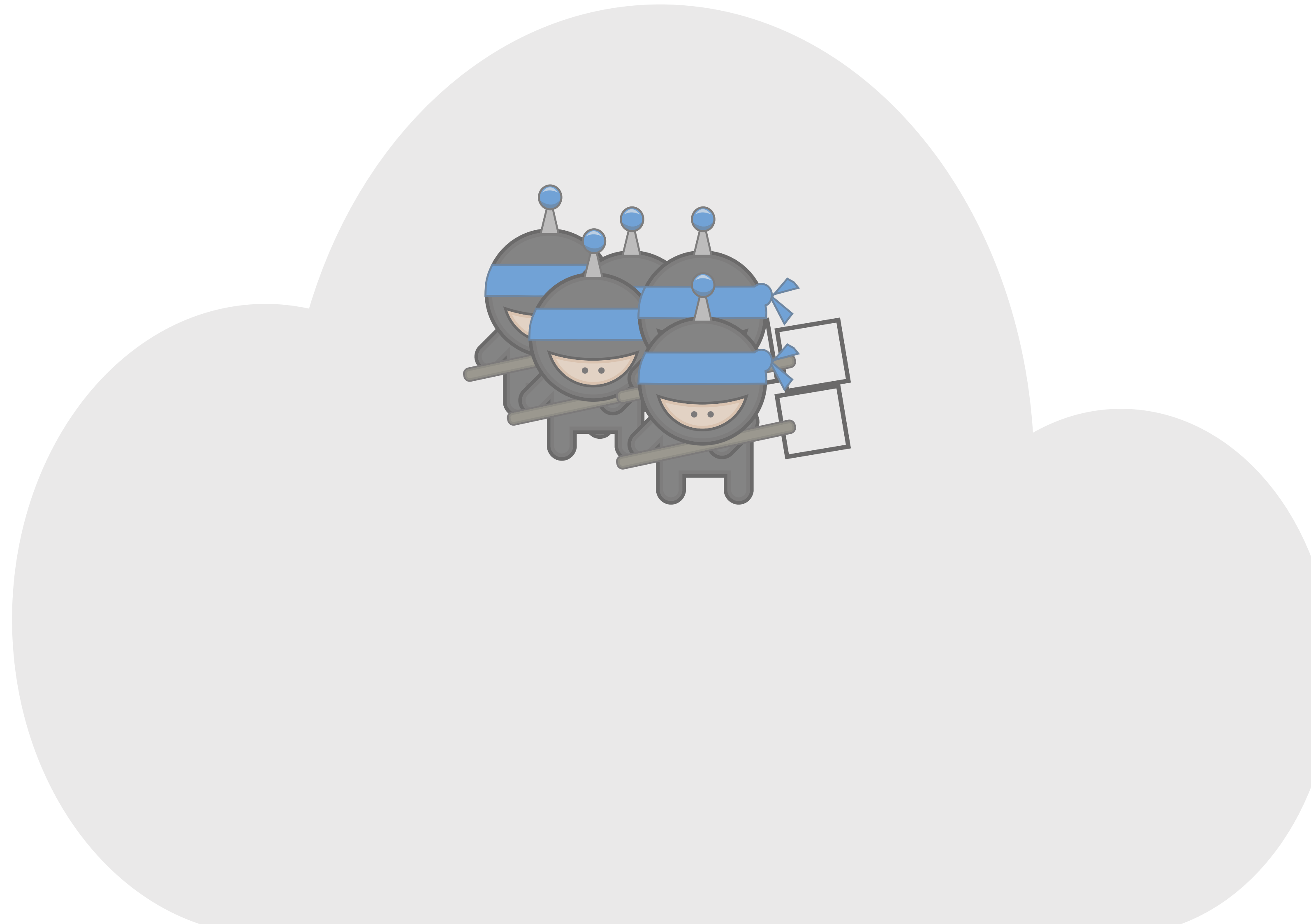
[The computational power of population protocols, Angluin et al.,'06]



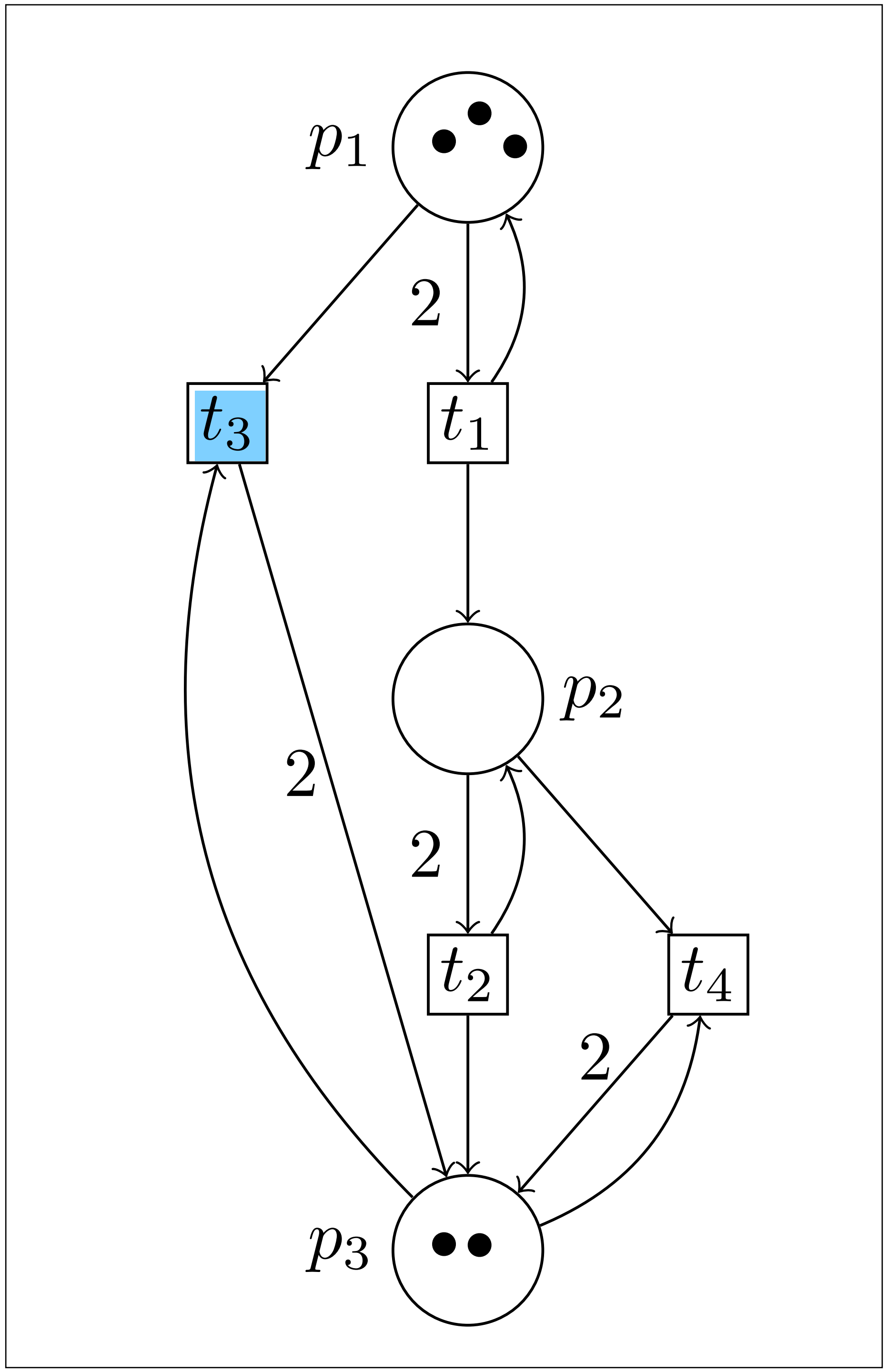
Example



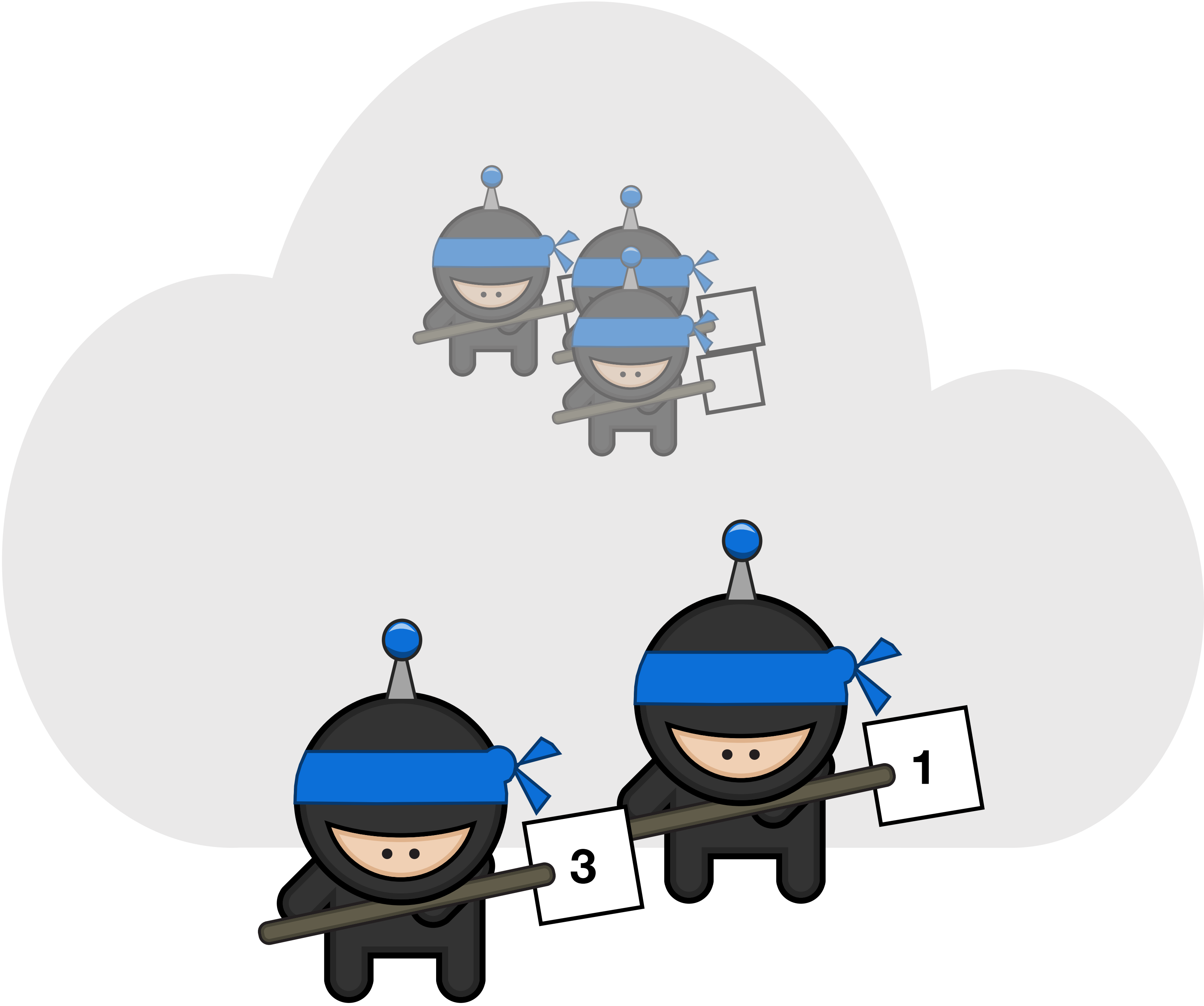
[The computational power of population protocols, Angluin et al.,'06]



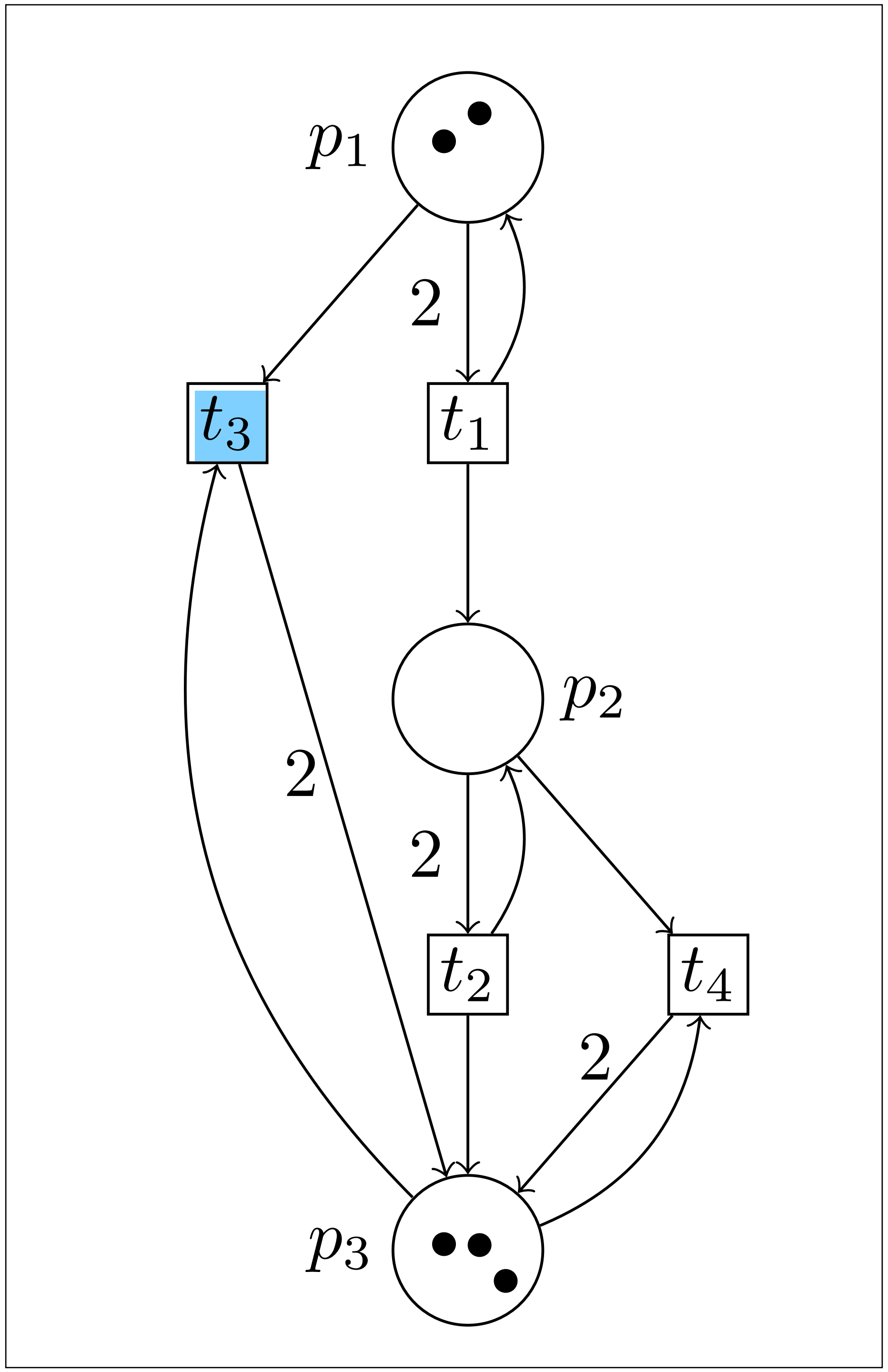
Example



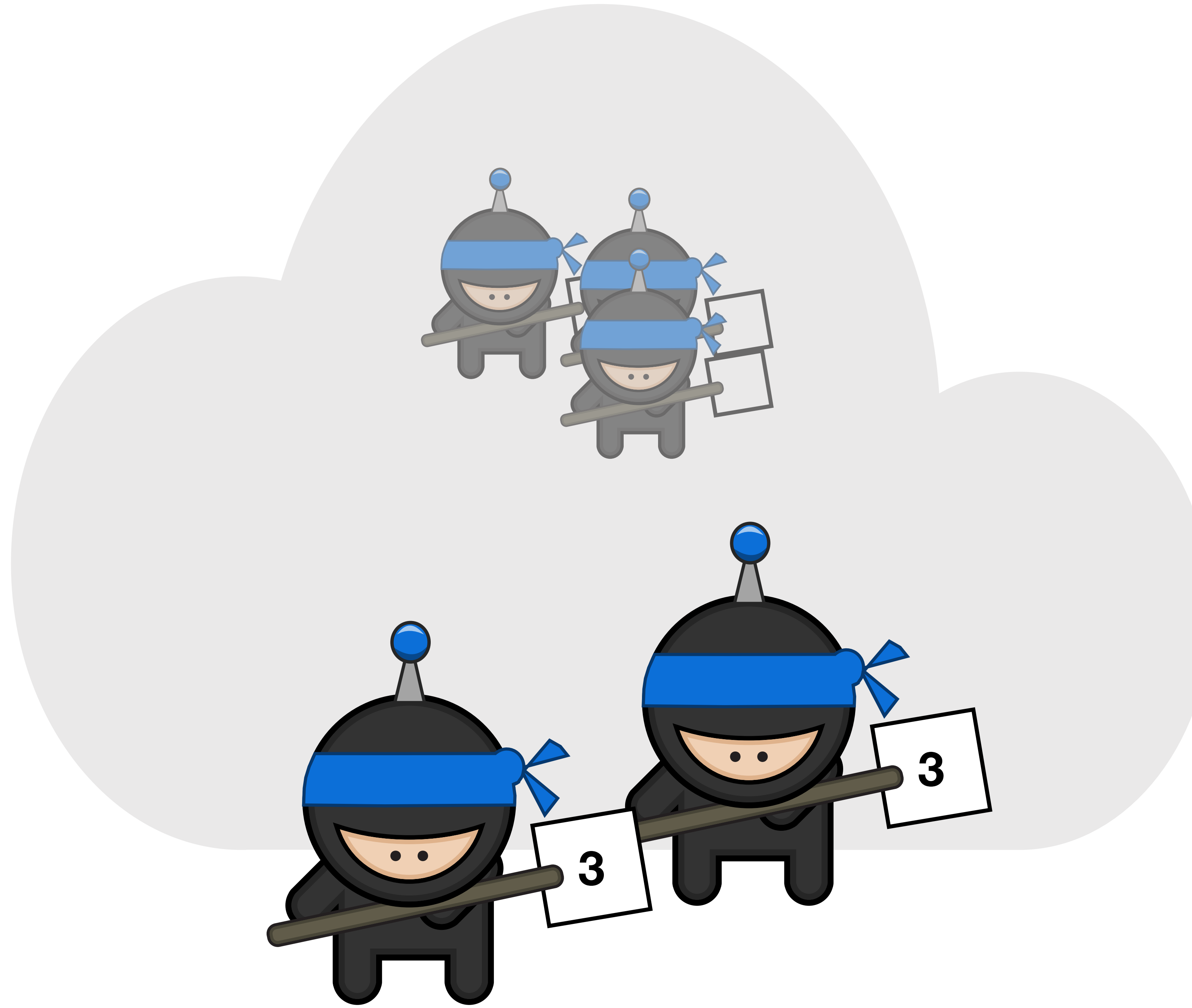
[The computational power of population protocols, Angluin et al.,'06]



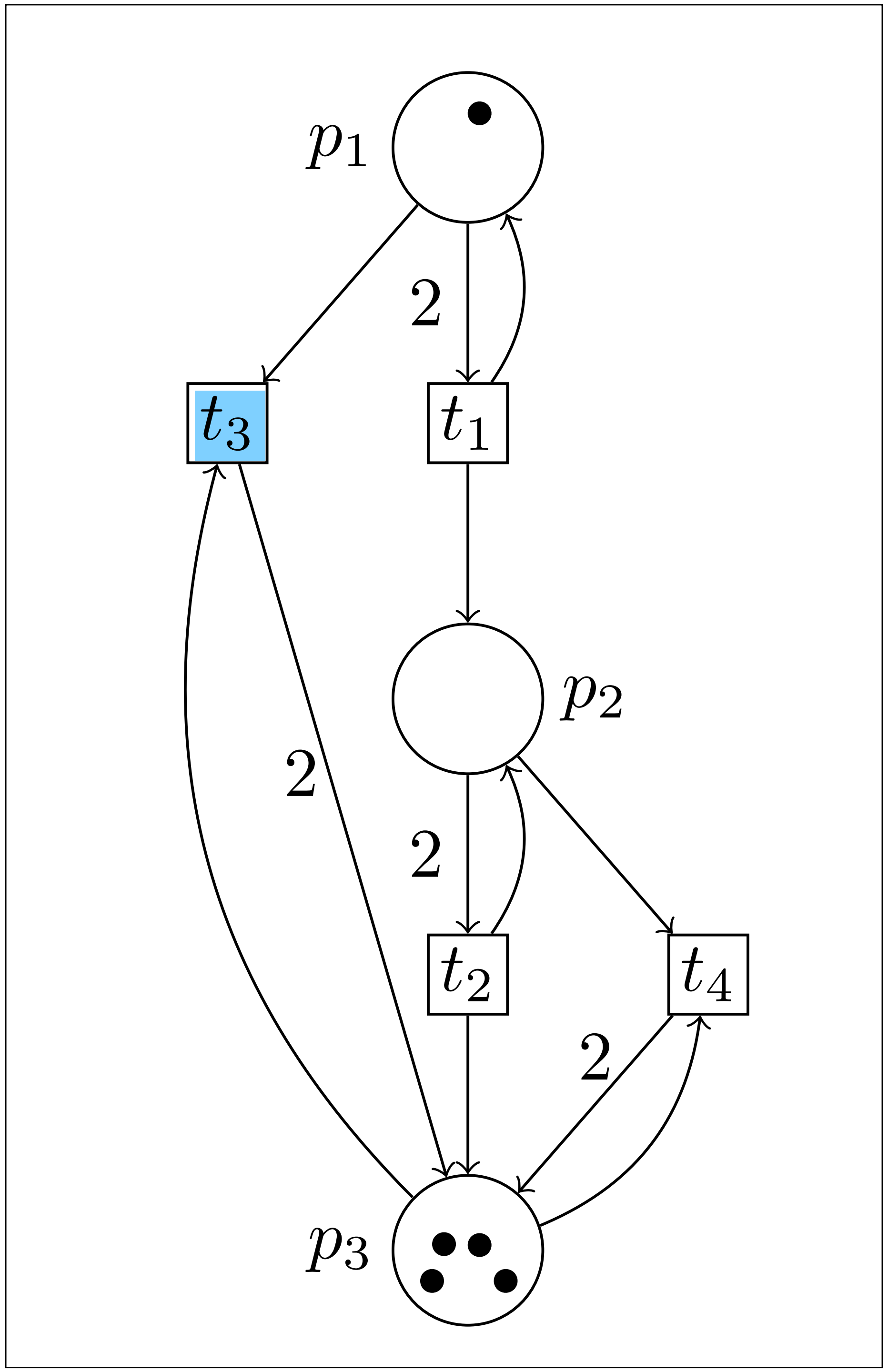
Example



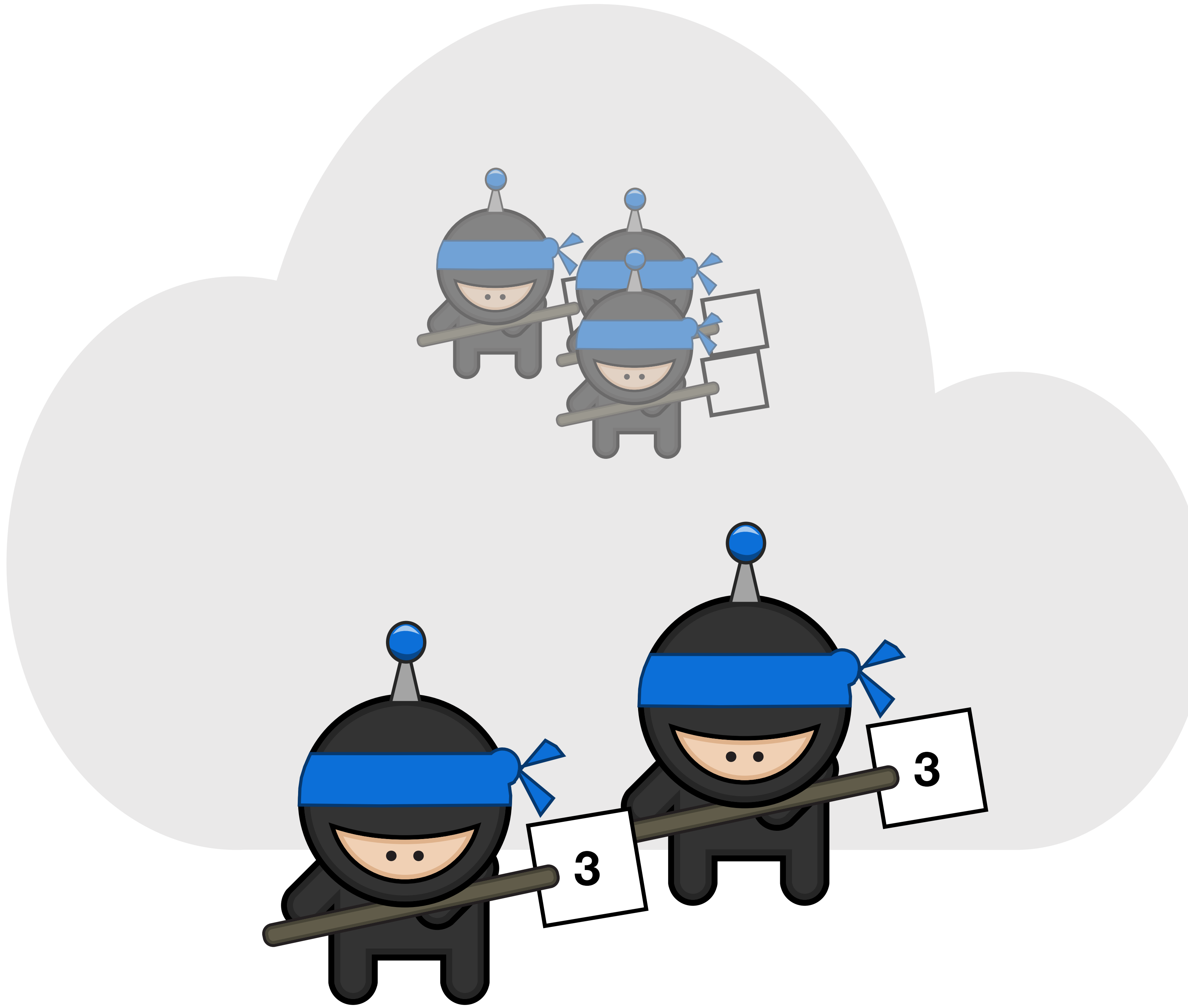
[The computational power of population protocols, Angluin et al.,'06]



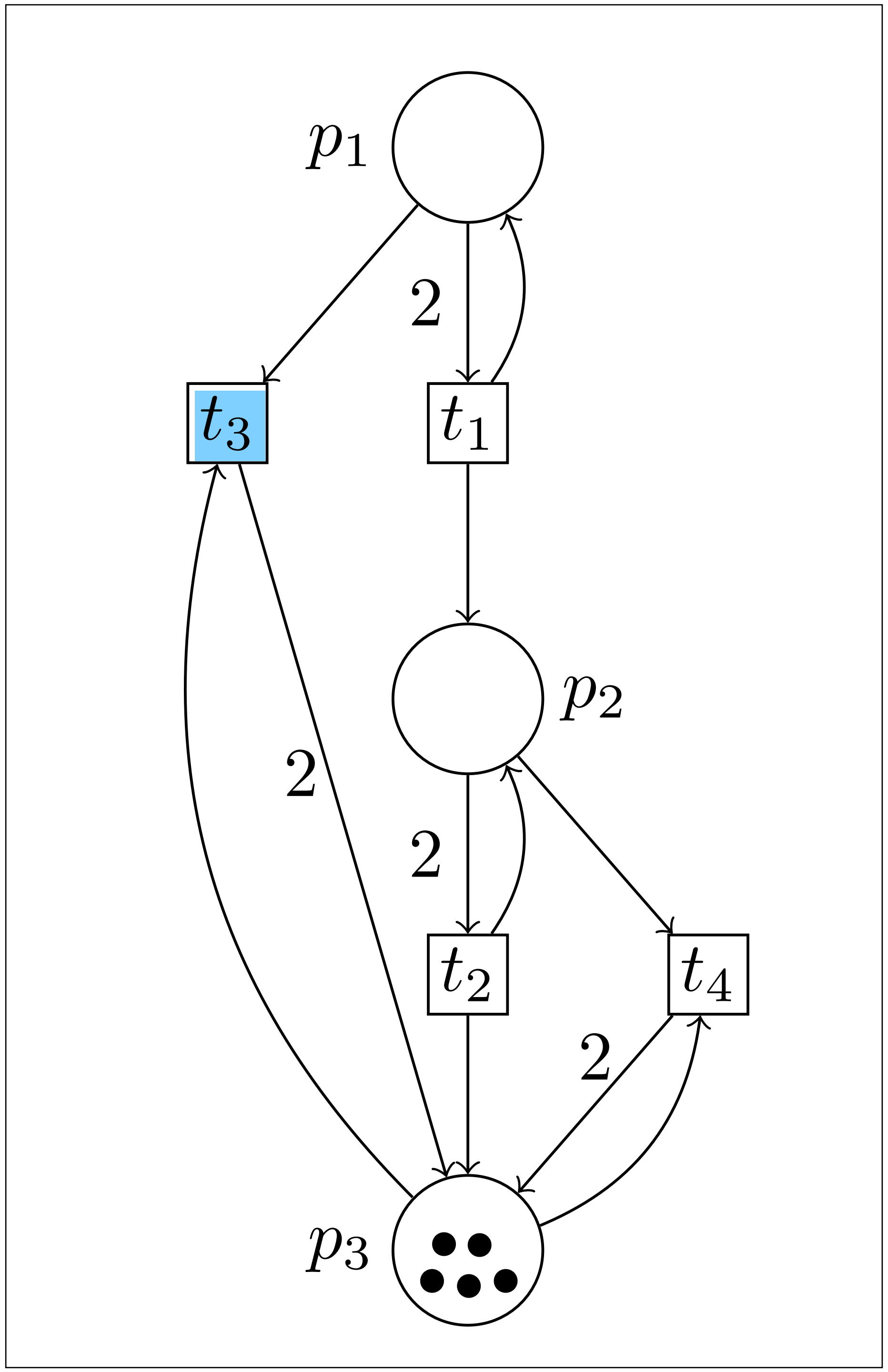
Example



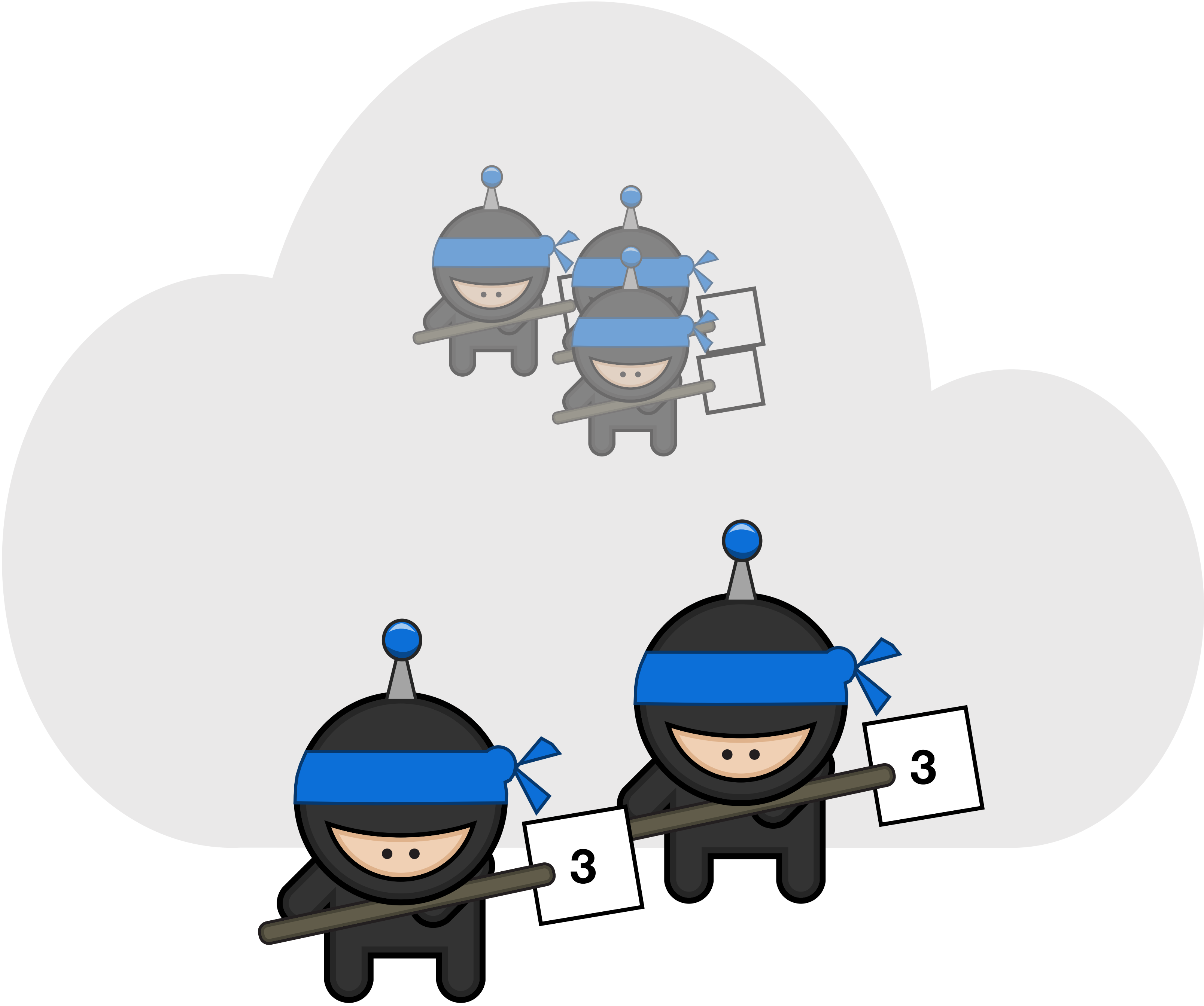
[The computational power of population protocols, Angluin et al.,'06]



Example



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



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

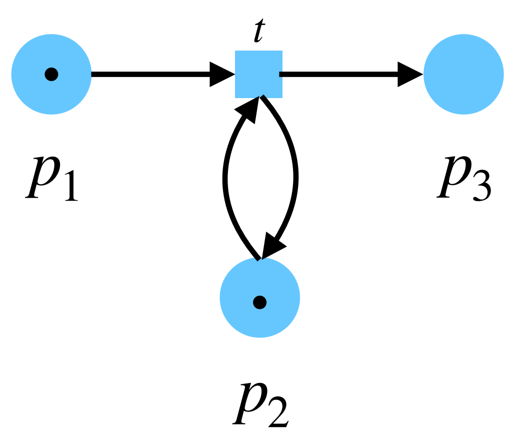
and BIO nets are expressive

Part 1:
Immediate observation nets

Immediate Observation nets

[Esparza, Raskin, *W.-K.*, ’19]

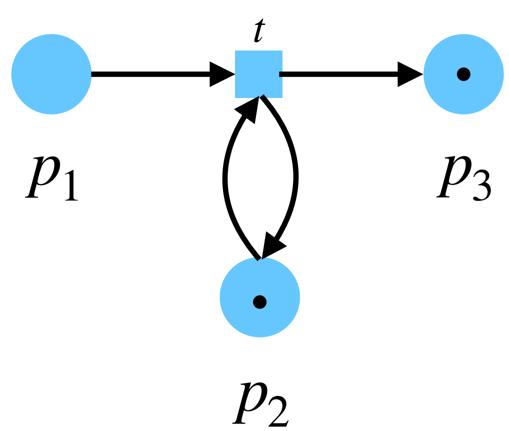
Immediate Observation nets (IO)



Immediate Observation nets

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

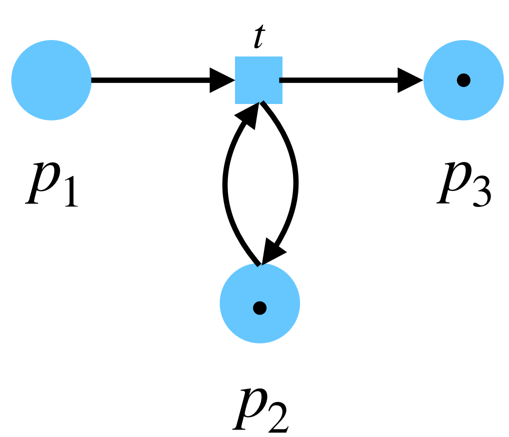
Immediate Observation nets (IO)



Immediate Observation nets

[Esparza, Raskin, *W.-K.*, ’19]

Immediate Observation nets (IO)



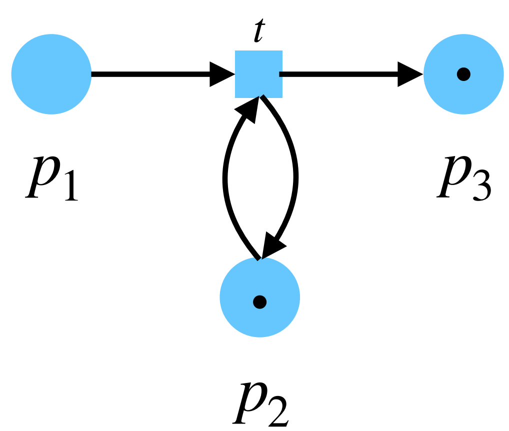
- introduced to study **immediate observation** population protocols (distributed computing model).

  [Angluin, Aspnes, Eisenstat, Ruppert, ’07]

Immediate Observation nets

[Esparza, Raskin, *W.-K.*, ’19]

Immediate Observation nets (IO)



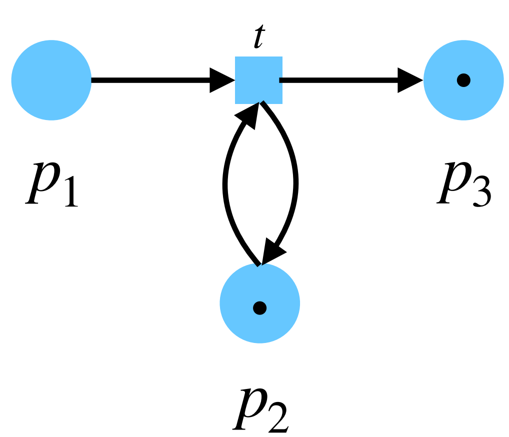
- introduced to study **immediate observation** population protocols (distributed computing model).
  [Angluin, Aspnes, Eisenstat, Ruppert, ’07]

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

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.

Cube-reachability

number of tokens in q

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 $\mathscr{C}$ and $\mathscr{C}'$, does there exist $M \in \mathscr{C}$ and $M' \in \mathscr{C}'$ such that M reaches M' ?

Cube-reachability

number of tokens in q

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

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

non-elementary for conservative Petri nets

Cube-reachability

number of tokens in q

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 $\mathscr{C}$ and $\mathscr{C}'$, does there exist $M \in \mathscr{C}$ and $M' \in \mathscr{C}'$ such that M reaches M' ?

non-elementary for conservative Petri nets

PSPACE-complete for IO nets

Cube-reachability

number of tokens in q

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

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

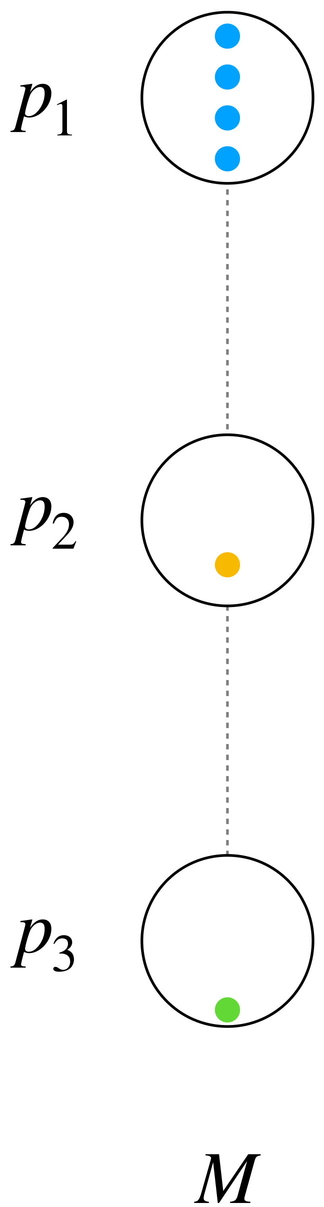
non-elementary for conservative Petri nets

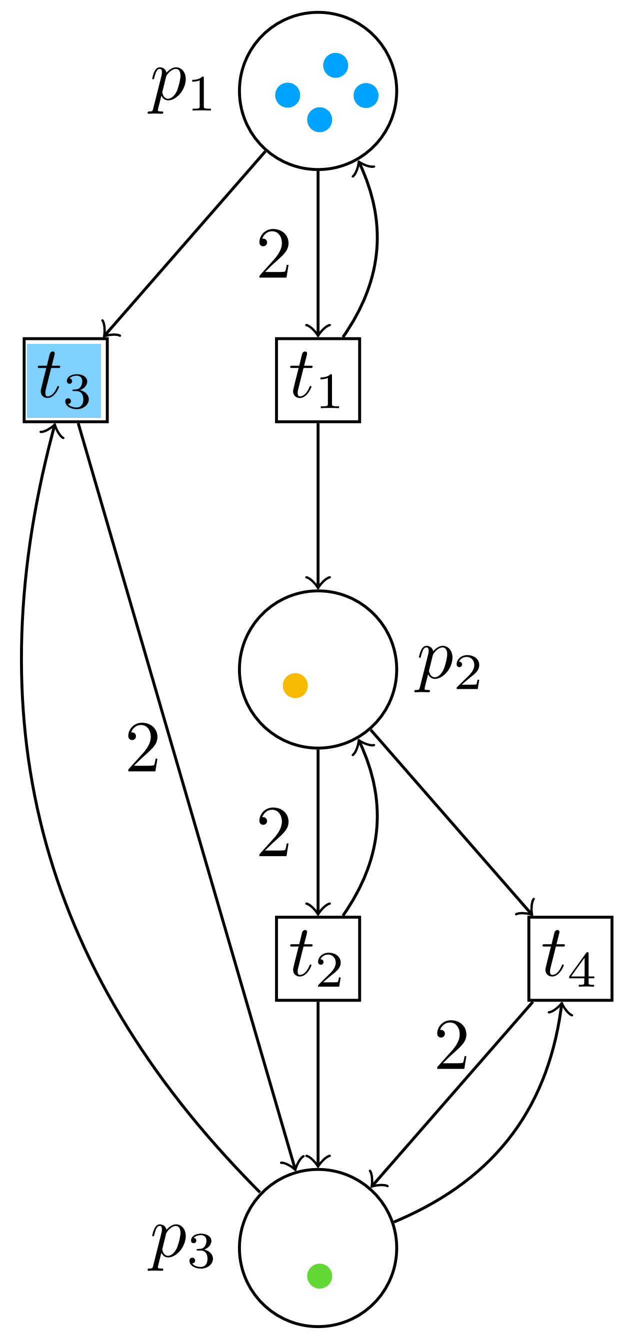
PSPACE-complete for IO nets

➡ correctness of IO population protocols is in PSPACE

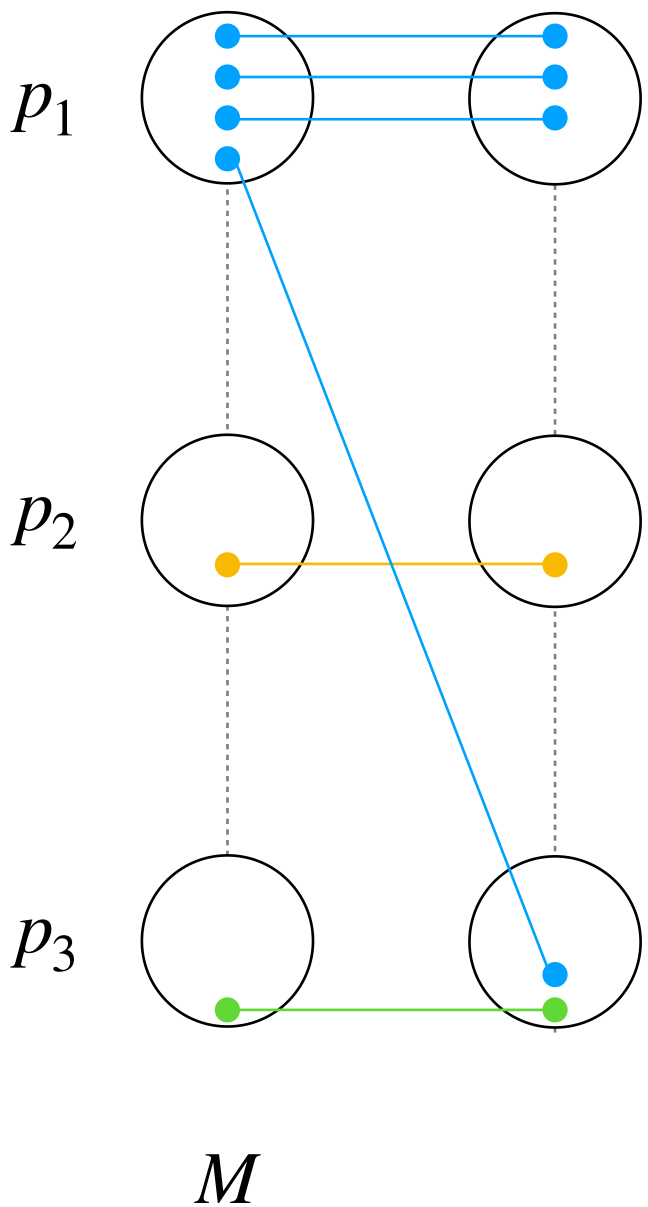
[Esparza, Raskin, *W.-K.*, '19]

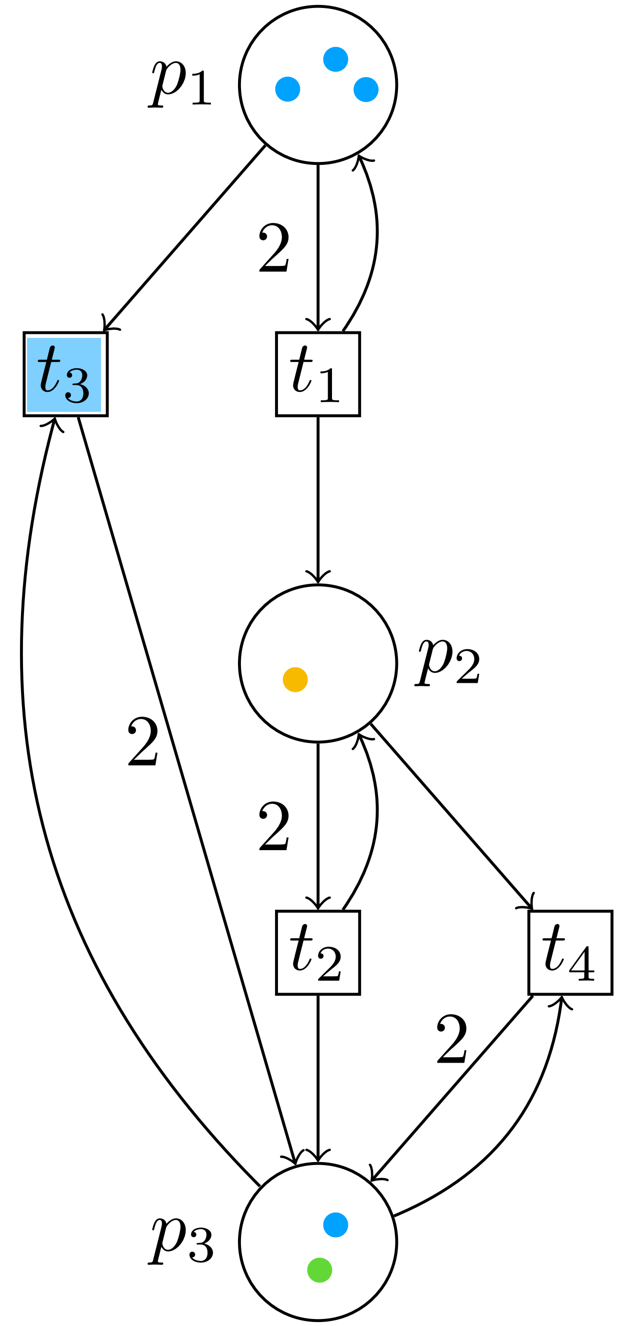
Main idea



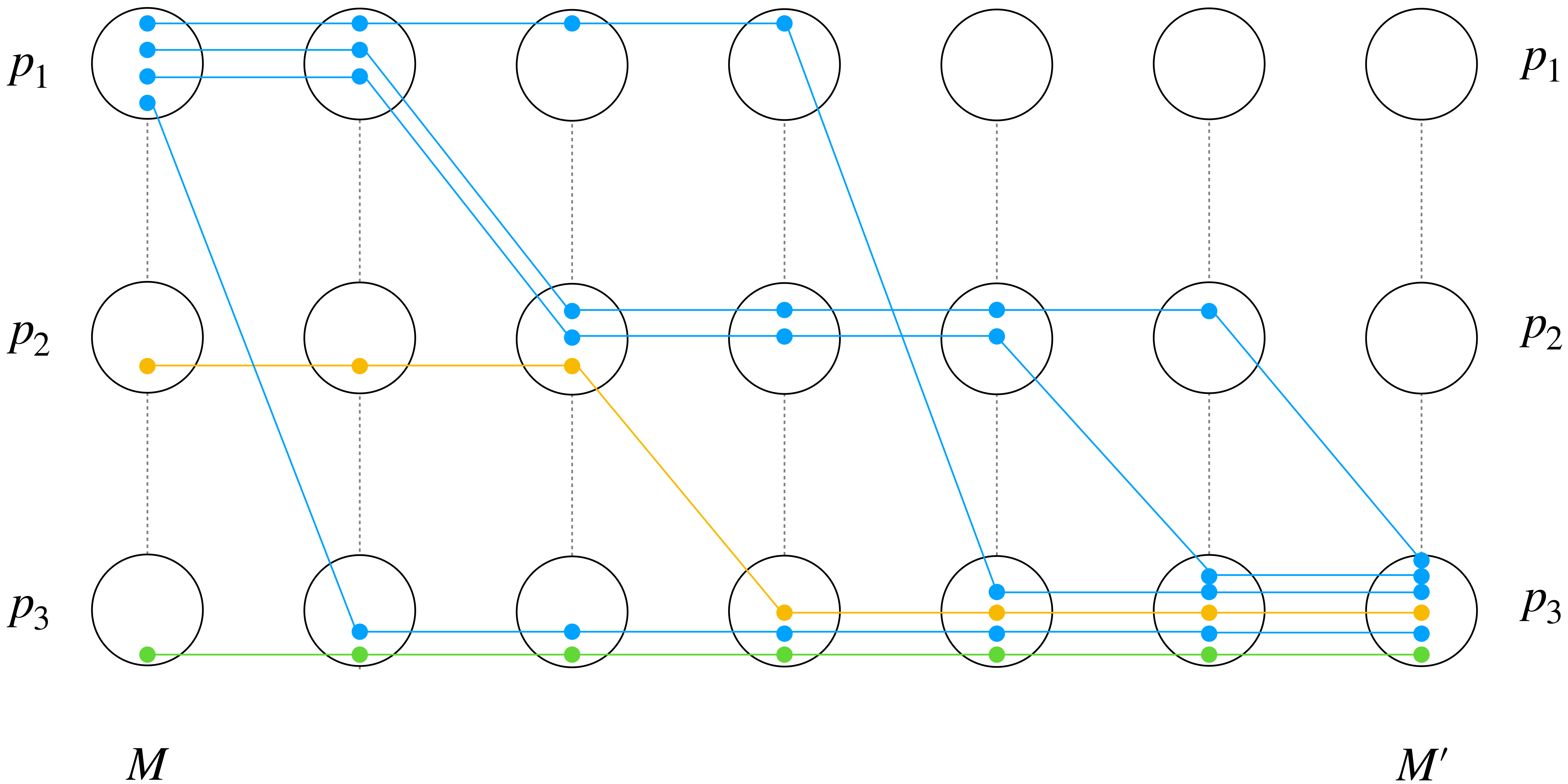


Main idea





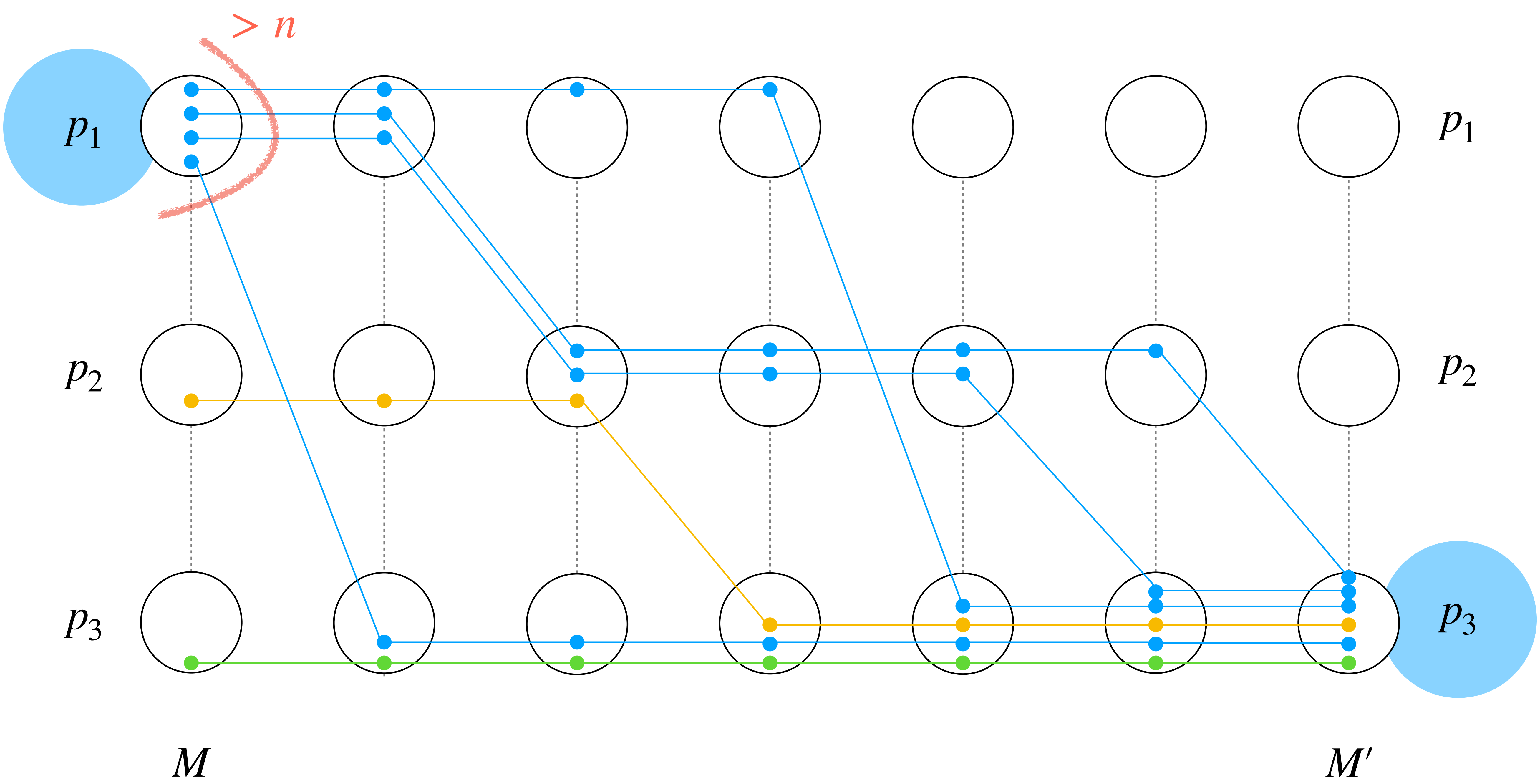
Main idea



C. Weil-Kennedy, TUM

Pruning

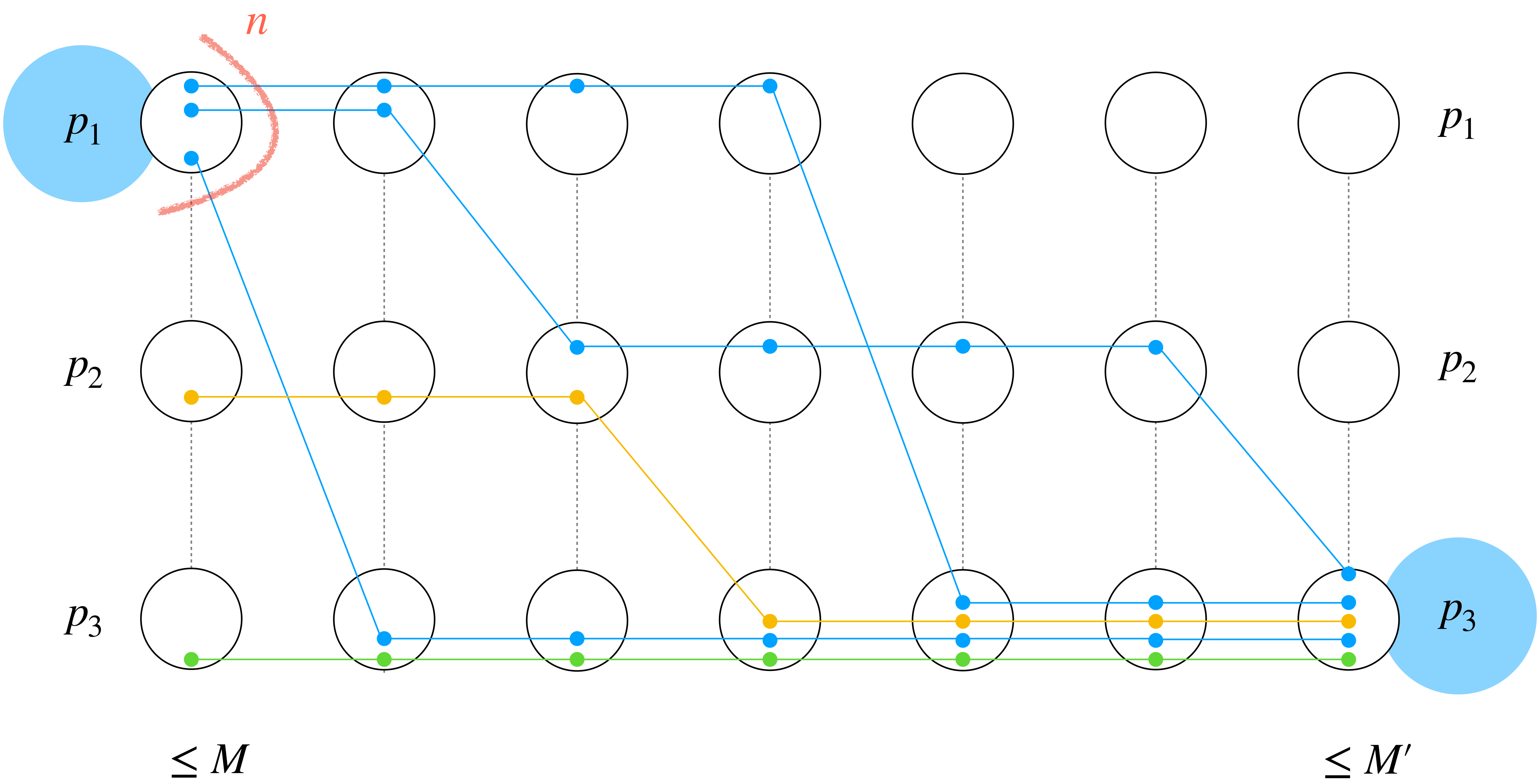
n = number of places



C. Weil-Kennedy, TUM

Pruning

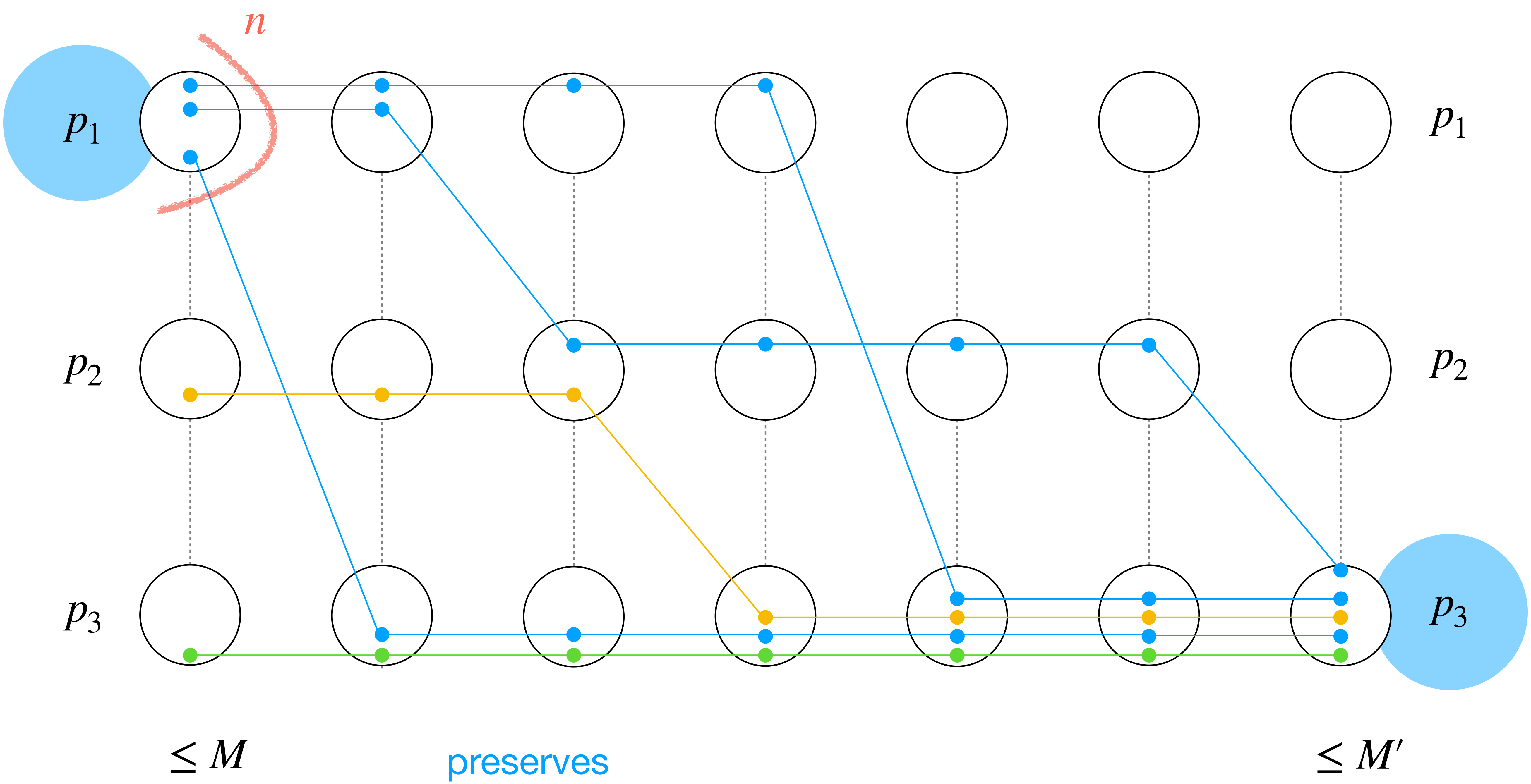
n = number of places



C. Weil-Kennedy, TUM

Pruning

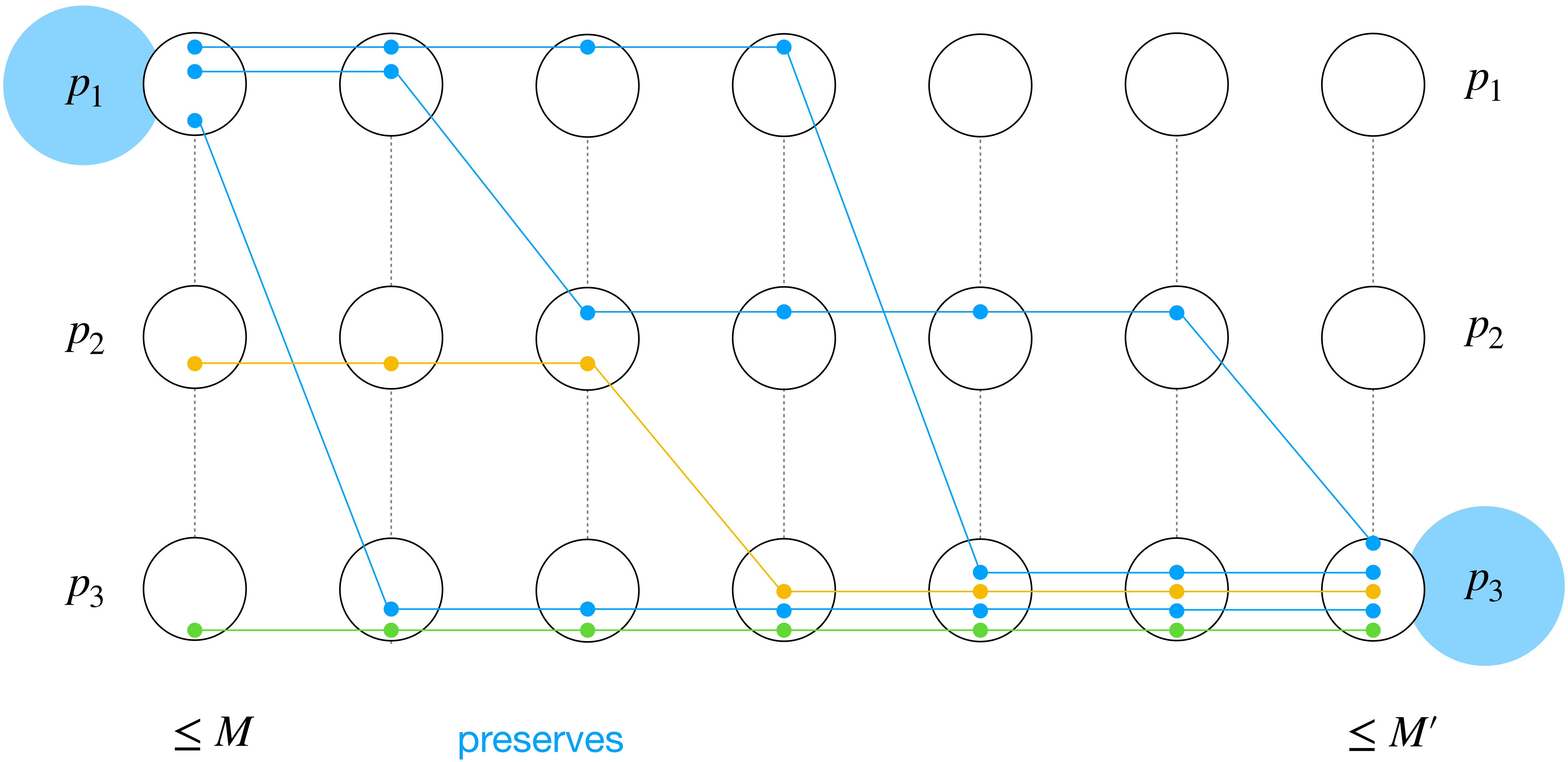
n = number of places



preserves

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

Boosting

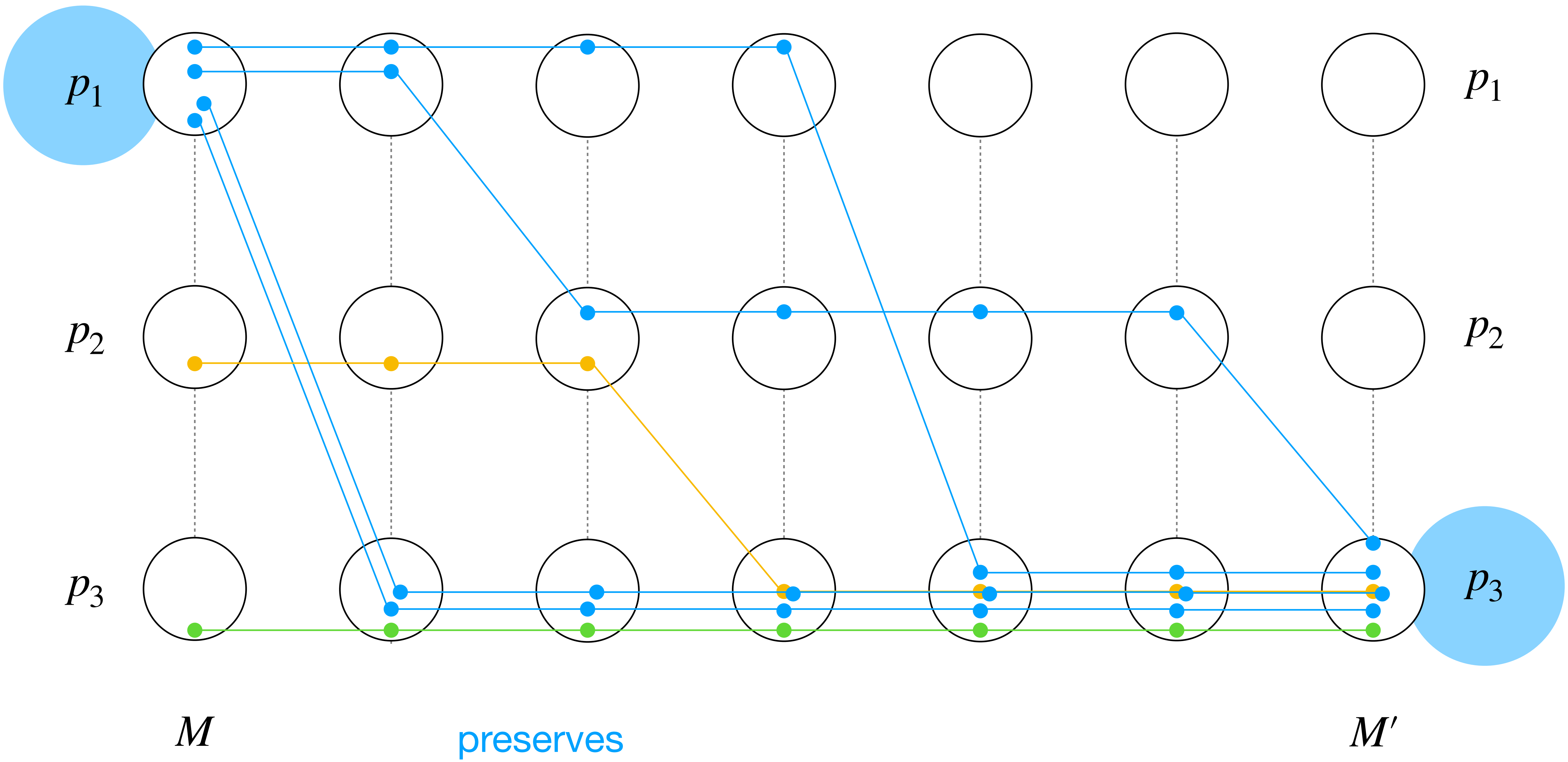


preserves

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

C. Weil-Kennedy, TUM

Boosting

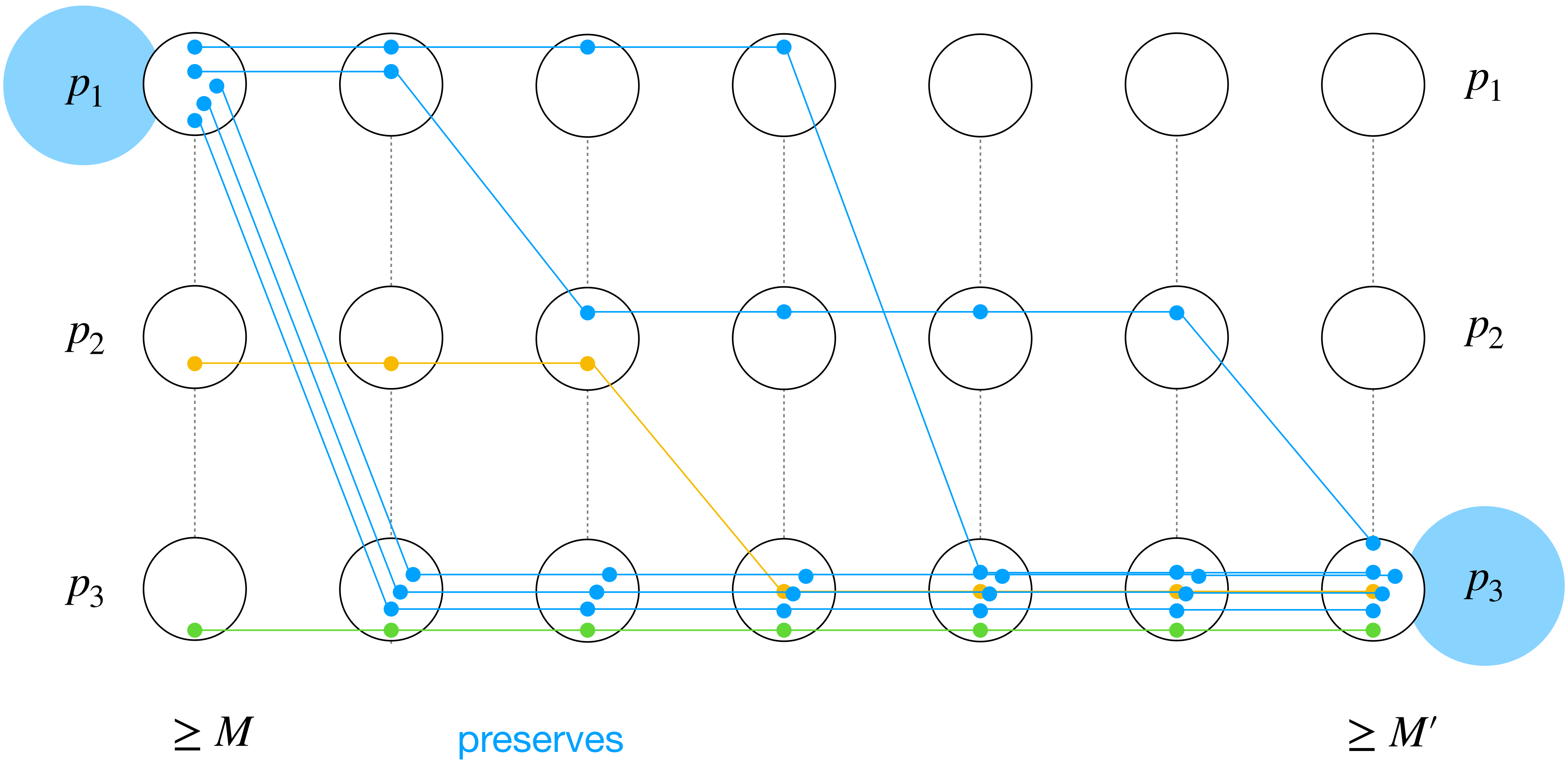


preserves

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

C. Weil-Kennedy, TUM

Boosting



preserves

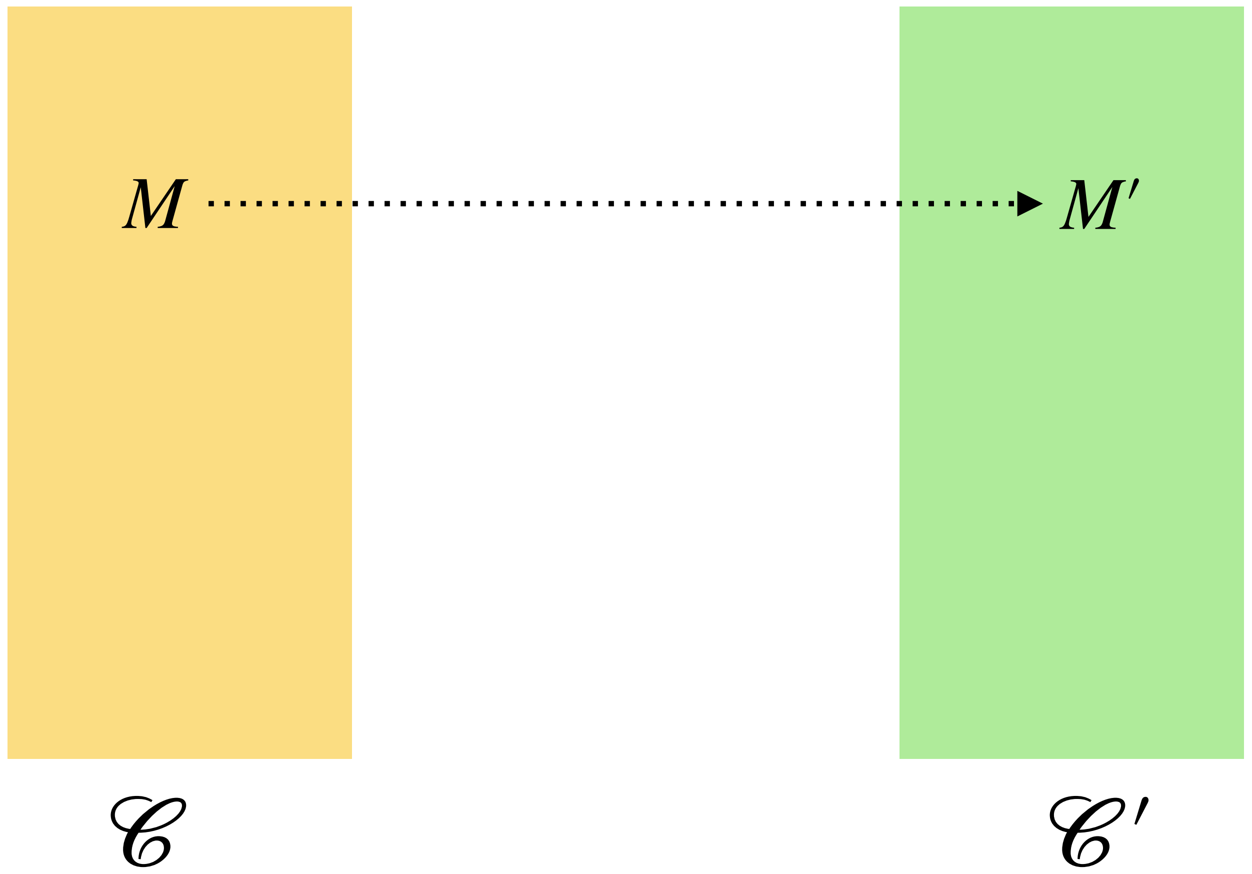
- support of initial and final markings
- validity of firing sequence

C. Weil-Kennedy, TUM

Main idea

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

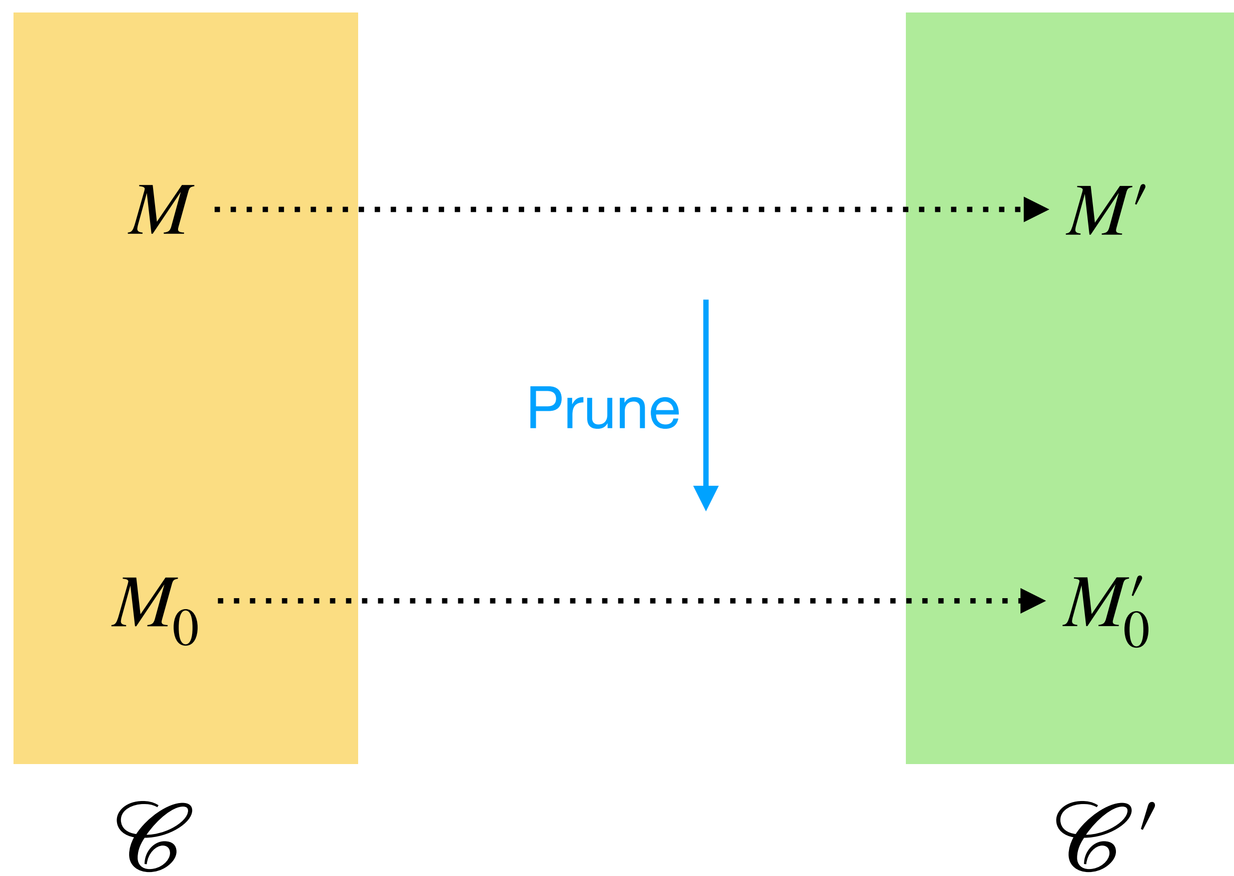
cube-reachability: given cubes $\mathscr{C}$ and $\mathscr{C}'$, does there exist $M \in \mathscr{C}$ and $M' \in \mathscr{C}'$ such that M reaches M' ?



Main idea

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

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



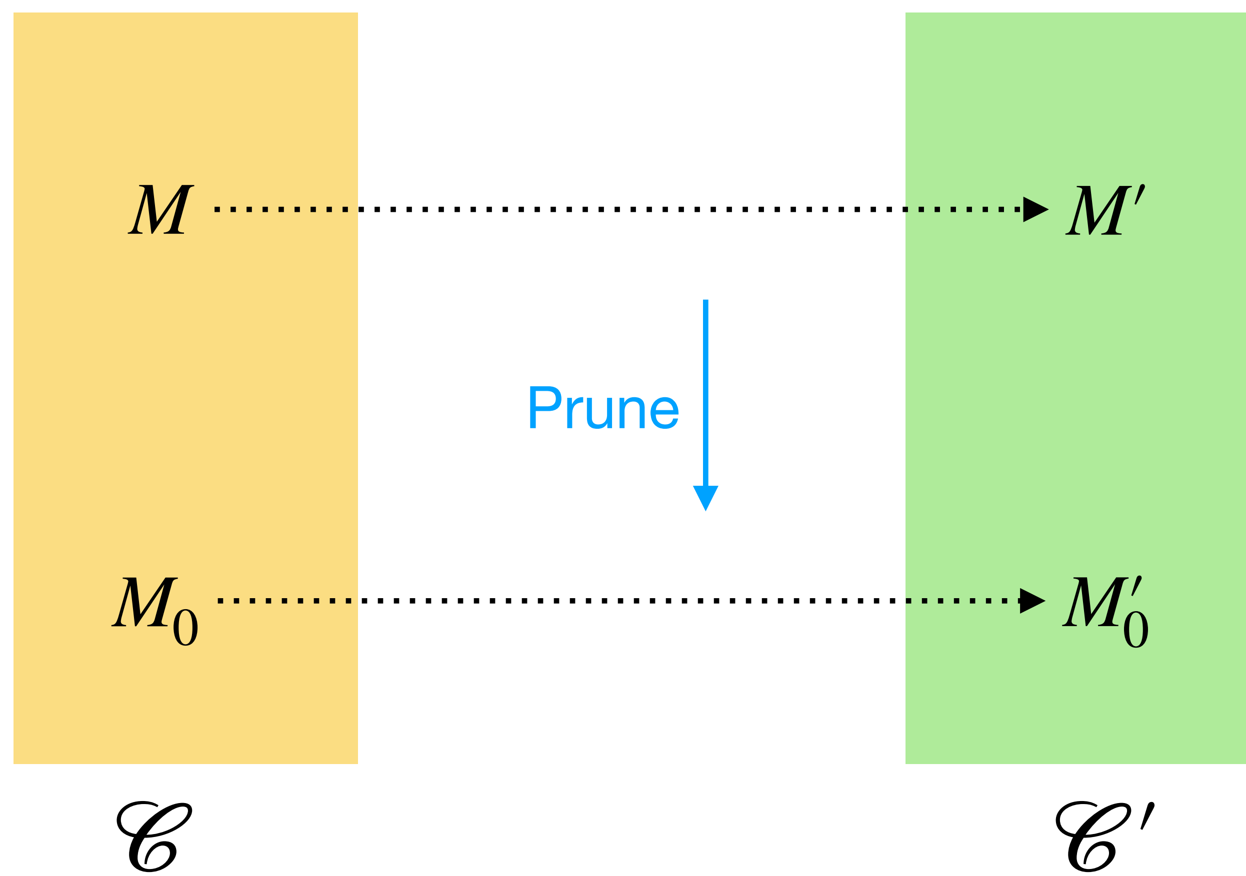
$\leq n \cdot n^2$
+ lower bound $\mathscr{C}$
+ lower bound $\mathscr{C}'$

Main idea

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

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

$\leq n \cdot n^2$
+ lower bound $\mathscr{C}$
+ lower bound $\mathscr{C}'$

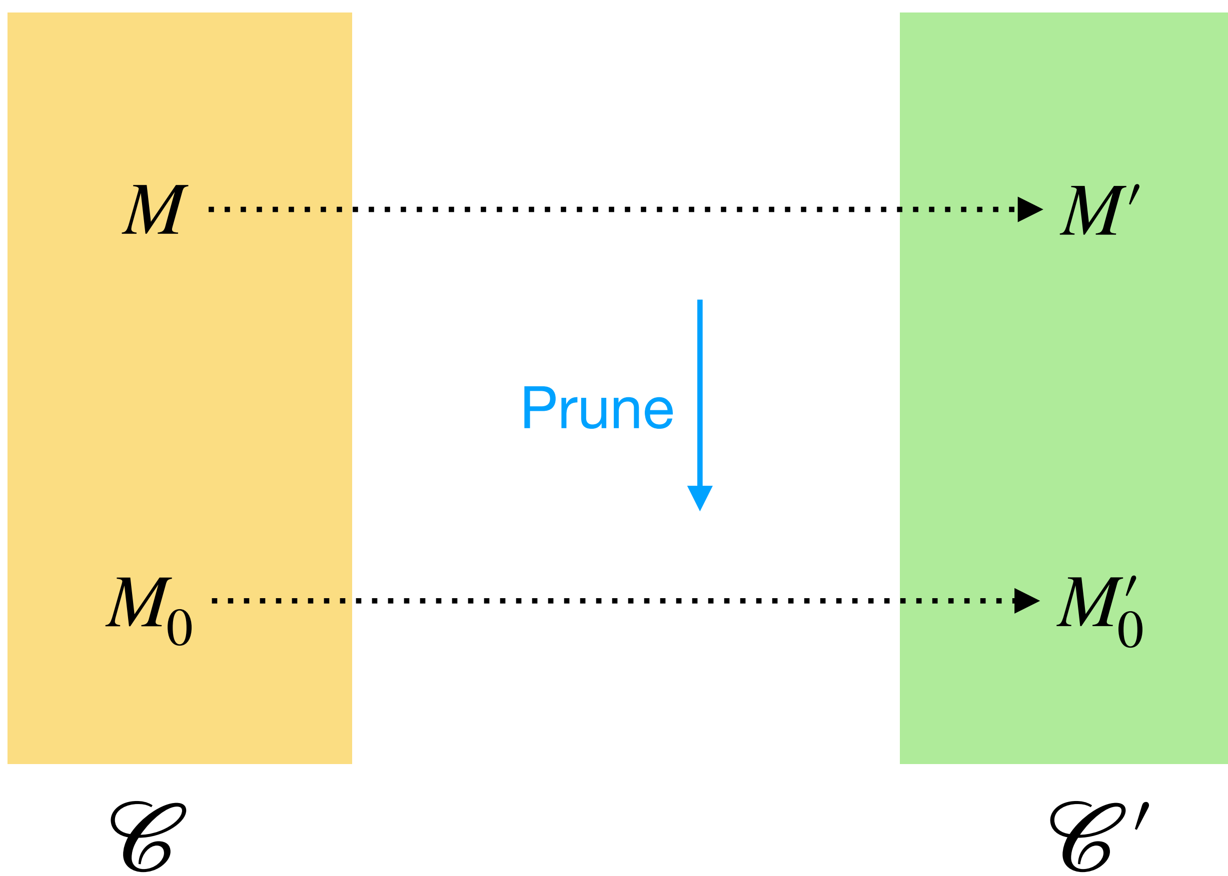


- NPSPACE = PSPACE
- non-deterministically pick small markings M_0 and M'_0
- check if M_0 reaches M'_0

Main idea

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

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



$\leq n \cdot n^2$
+ lower bound $\mathscr{C}$
+ lower bound $\mathscr{C}'$

- NPSPACE = PSPACE
- non-deterministically pick small markings M_0 and M'_0
- check if M_0 reaches M'_0

PSPACE

Parameterized problems

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

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

PSPACE

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

PSPACE

Parameterized problems

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

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

PSPACE

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

PSPACE

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

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

Parameterized problems

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

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

PSPACE

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

PSPACE

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

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

e.g. reachability from cube $\mathscr{C}$ to cube $\mathscr{C}'$: $post^*(\mathscr{C}) \cap \mathscr{C}' \neq \emptyset$

Parameterized problems

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

cube-reachability: given cubes $\mathscr{C}$ and $\mathscr{C}'$, does there exist $M \in \mathscr{C}$ and $M' \in \mathscr{C}'$ 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 $\mathscr{C}_{init}$ to cube $\mathscr{C}_{final}$

Parameterized problems

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

cube-reachability: given cubes $\mathscr{C}$ and $\mathscr{C}'$, does there exist $M \in \mathscr{C}$ and $M' \in \mathscr{C}'$ 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 $\mathscr{C}_{init}$ to cube $\mathscr{C}_{final}$

$$post^*(\mathscr{C}_{init}) \subseteq pre^*(\mathscr{C}_{final})$$

IO nets are flat

[Leroux, Sutre, '05]

Flat

$\exists$ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0 \forall M$, $M_0 \xrightarrow{*} M$ iff $M_0 \xrightarrow{t_1^{k_1} t_2^{k_2} \ldots t_\ell^{k_\ell}} M$

IO nets are flat

[Leroux, Sutre, ’05]

<u>Flat</u>

$\exists$ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0 \forall M,\ M_0 \xrightarrow{*} M$ iff $M_0 \xrightarrow{t_1^{k_1} t_2^{k_2} \ldots t_\ell^{k_\ell}} M$

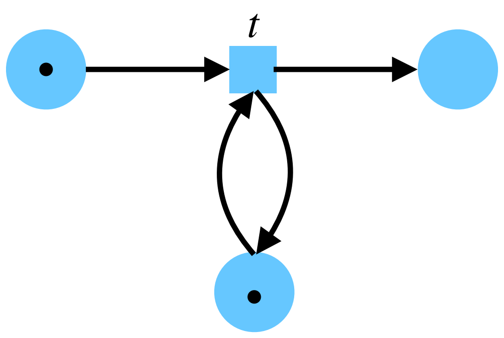
IO nets are flat

$\longrightarrow$ 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

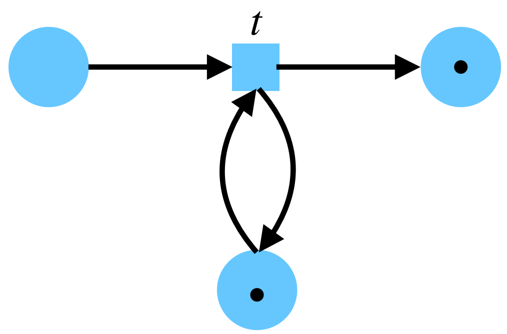
Immediate Observation nets (IO)



- Conservative
- Communication

Branching immediate observation nets

Immediate Observation nets (IO)

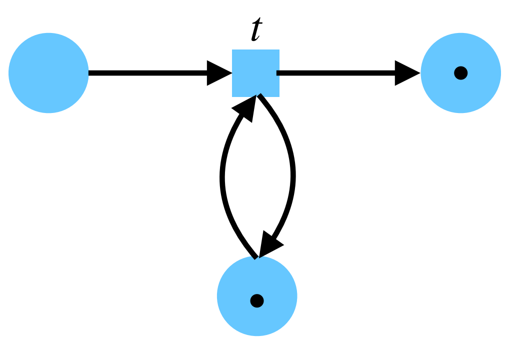


- Conservative
- Communication

Branching immediate observation nets

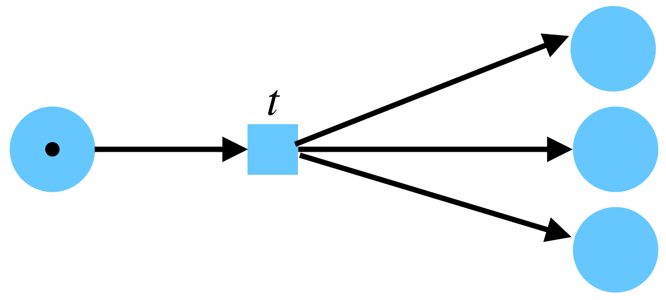
[Christensen et al., ’93] [Yen, ’97] [Lasota, ’09] [Mayr, Weihmann, ’15]

Immediate Observation nets (IO)



- Conservative
- Communication

Branching Parallel Processes (BPP)

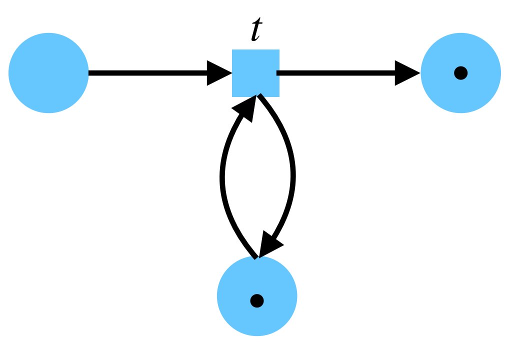


- Token creation and destruction
- Communication-free

Branching immediate observation nets

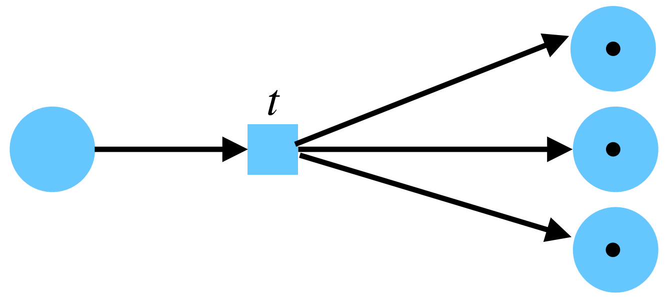
[Christensen et al., ’93] [Yen, ’97] [Lasota, ’09] [Mayr, Weihmann, ’15]

Immediate Observation nets (IO)



- Conservative
- Communication

Branching Parallel Processes (BPP)

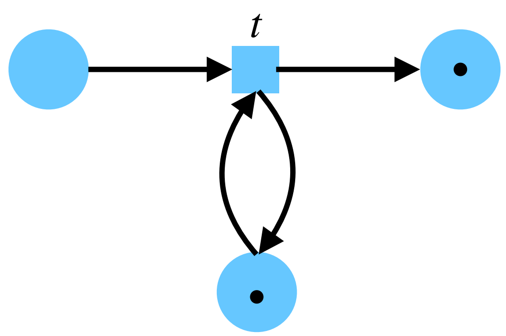


- Token creation and destruction
- Communication-free

Branching immediate observation nets

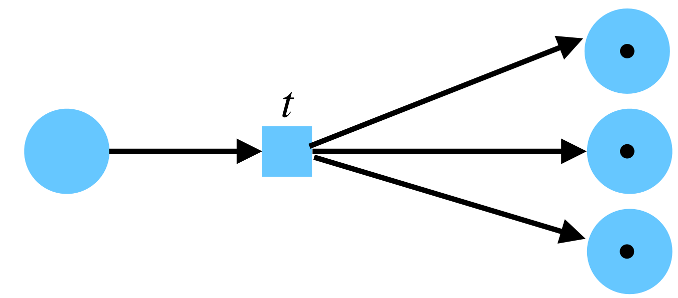
[Christensen et al., ’93] [Yen, ’97] [Lasota, ’09] [Mayr, Weihmann, ’15]

Immediate Observation nets (IO)



- Conservative
- Communication

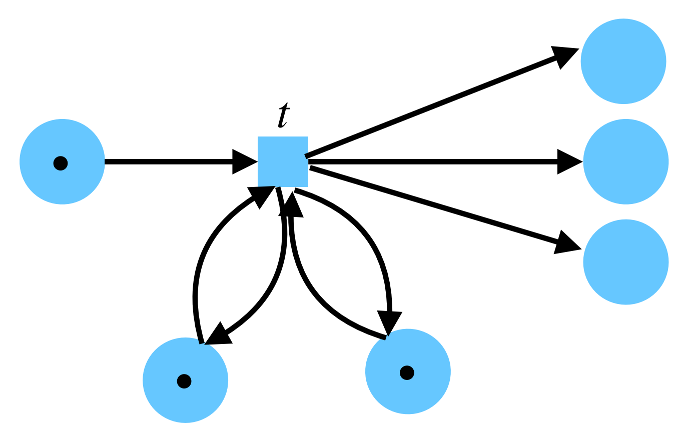
Branching Parallel Processes (BPP)



- Token creation and destruction
- Communication-free

Branching Immediate Observation nets (BIO)

- Token creation and destruction
- Communication

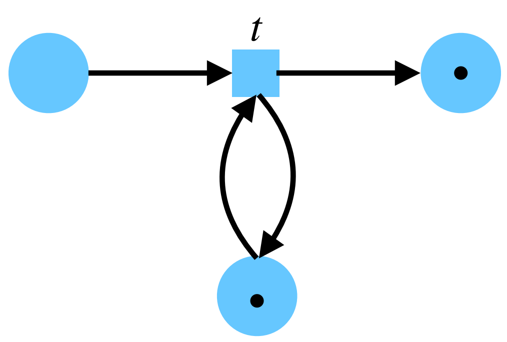


[Esparza, Raskin, *W.-K.*, ’20]

Branching immediate observation nets

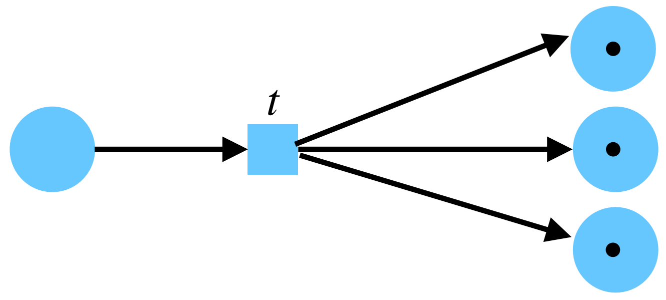
[Christensen et al., ’93] [Yen, ’97] [Lasota, ’09] [Mayr, Weihmann, ’15]

Immediate Observation nets (IO)



- Conservative
- Communication

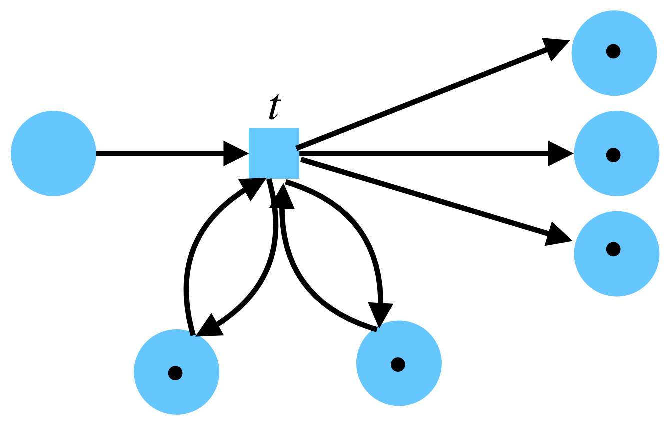
Branching Parallel Processes (BPP)



- Token creation and destruction
- Communication-free

Branching Immediate Observation nets (BIO)

- Token creation and destruction
- Communication



[Esparza, Raskin, *W.-K.*, ’20]

C. Weil-Kennedy, TUM

Cube-reachability

number of tokens in q

A **cube** is a boolean combination of constraints $\quad a \leq \#q \leq b$

$\in \mathbb{N} \qquad \in \mathbb{N} \cup \infty$

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

Cube-reachability

number of tokens in q

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

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

still
PSPACE-complete!

Cube-reachability

number of tokens in q

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

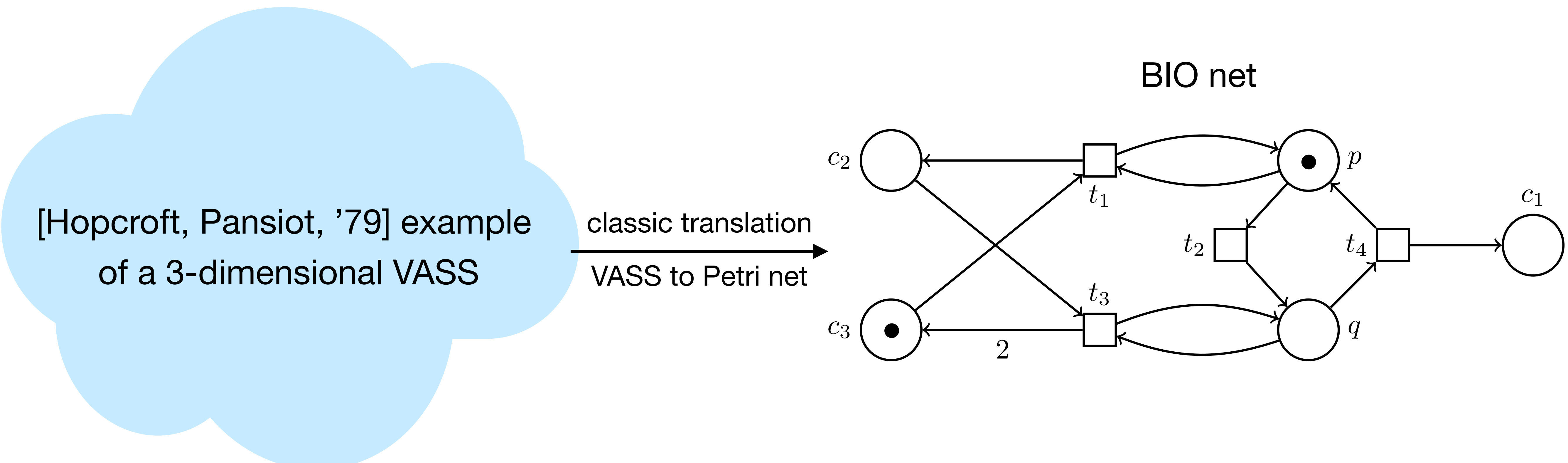
cube-reachability: given cubes $\mathscr{C}$ and $\mathscr{C}'$, does there exist $M \in \mathscr{C}$ and $M' \in \mathscr{C}'$ such that M reaches M' ?

still
PSPACE-complete!

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

Non-semilinear reachability

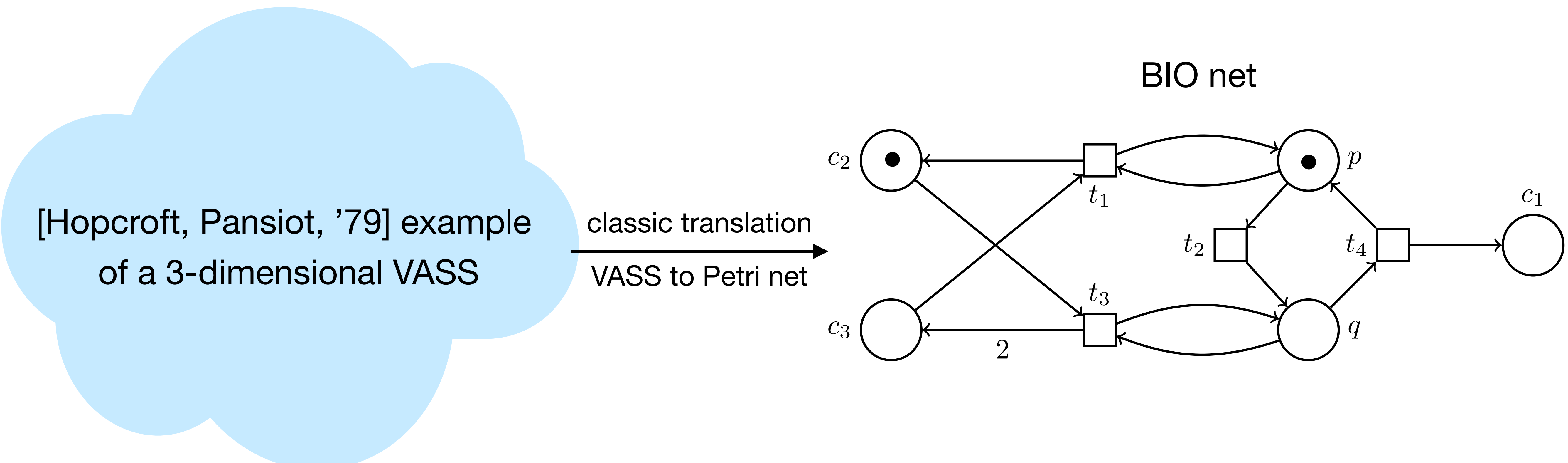
BIO nets can have **non-semilinear** reachability set



C. Weil-Kennedy, TUM

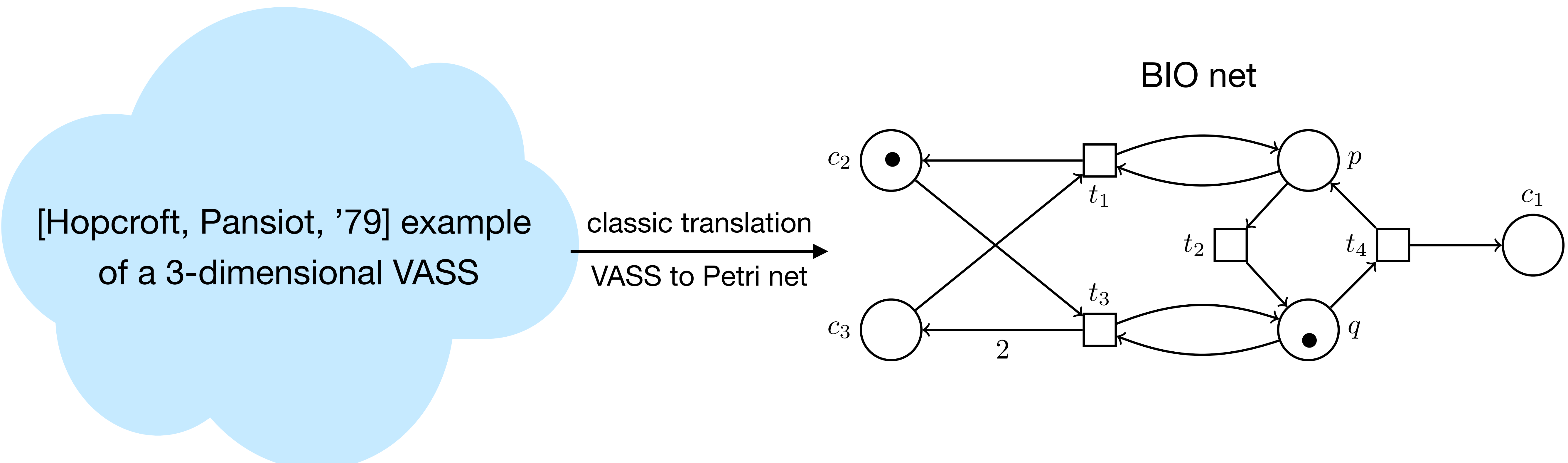
Non-semilinear reachability

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



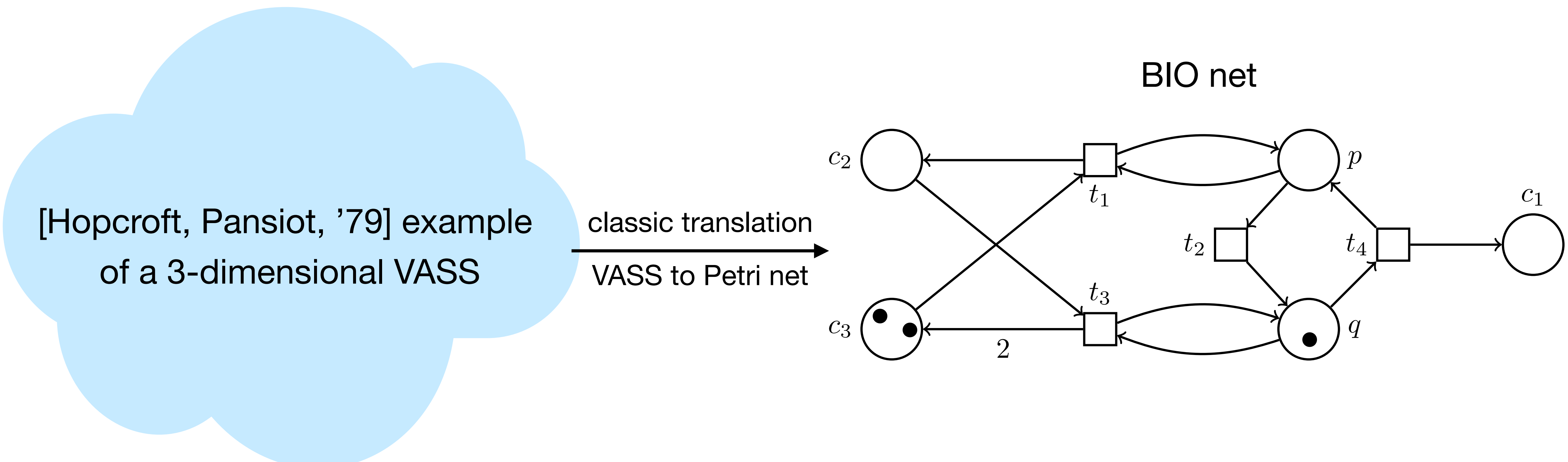
Non-semilinear reachability

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



Non-semilinear reachability

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



Non-semilinear reachability

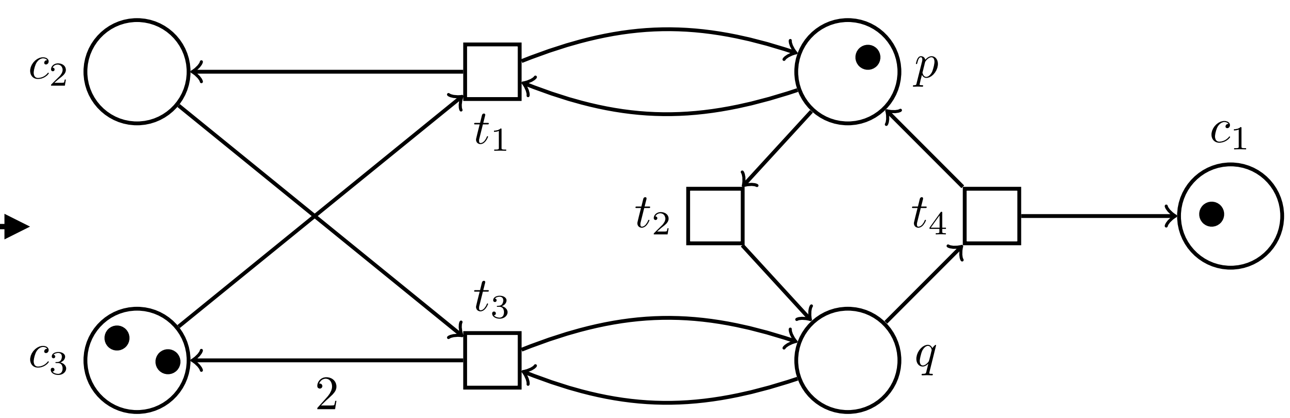
BIO nets can have **non-semilinear** reachability set

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

classic translation

VASS to Petri net

BIO net



Non-semilinear reachability

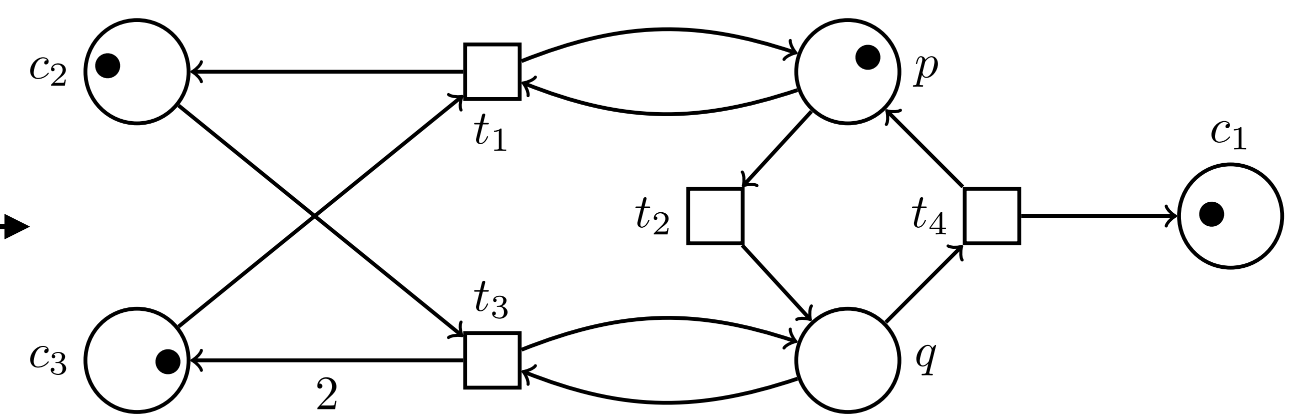
BIO nets can have **non-semilinear** reachability set

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

classic translation

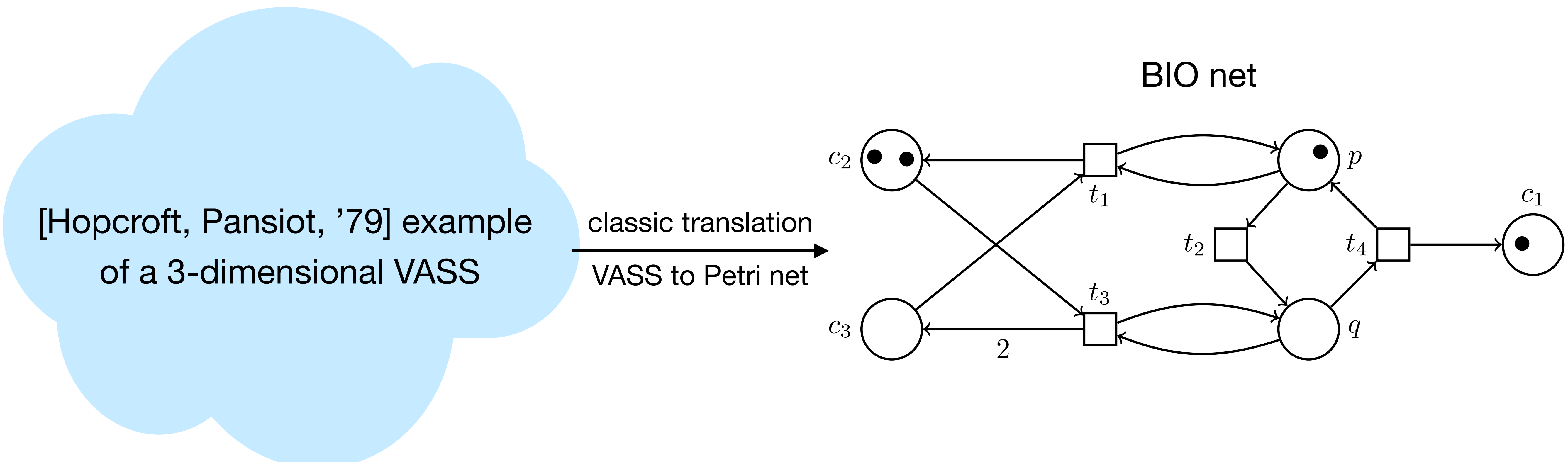
VASS to Petri net

BIO net



Non-semilinear reachability

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



Non-semilinear reachability

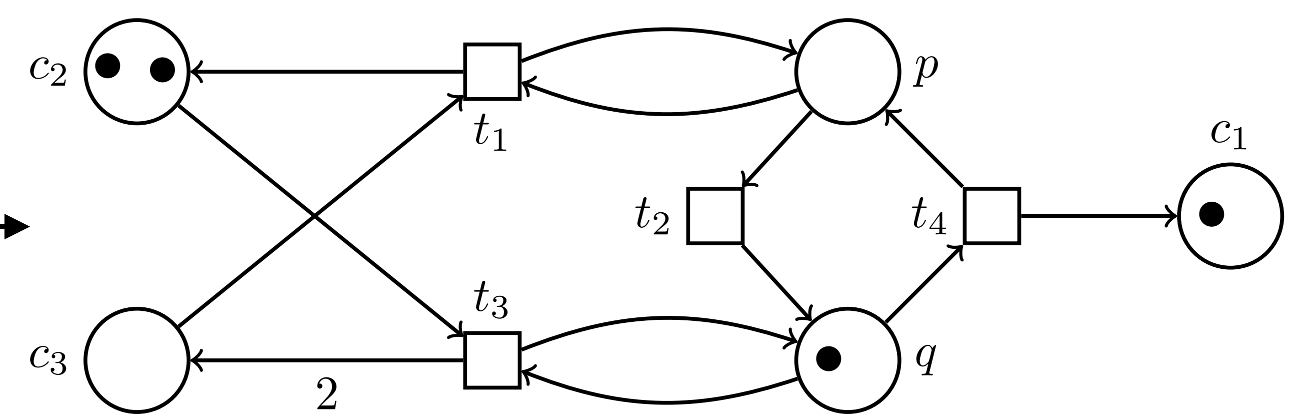
BIO nets can have **non-semilinear** reachability set

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

classic translation

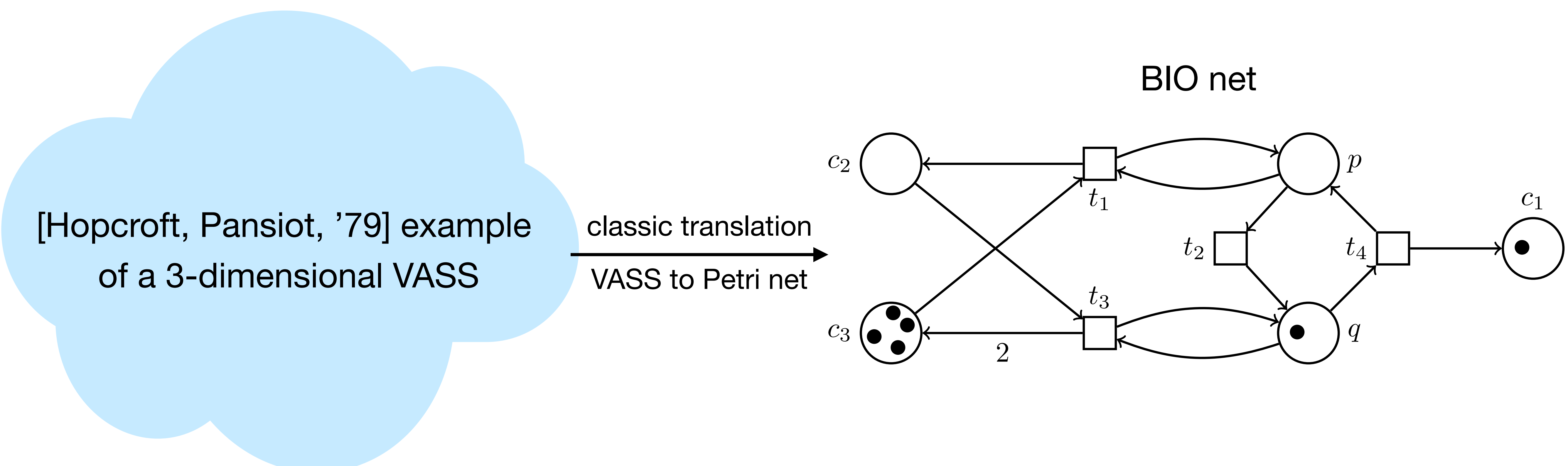
VASS to Petri net

BIO net



Non-semilinear reachability

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



Non-semilinear reachability

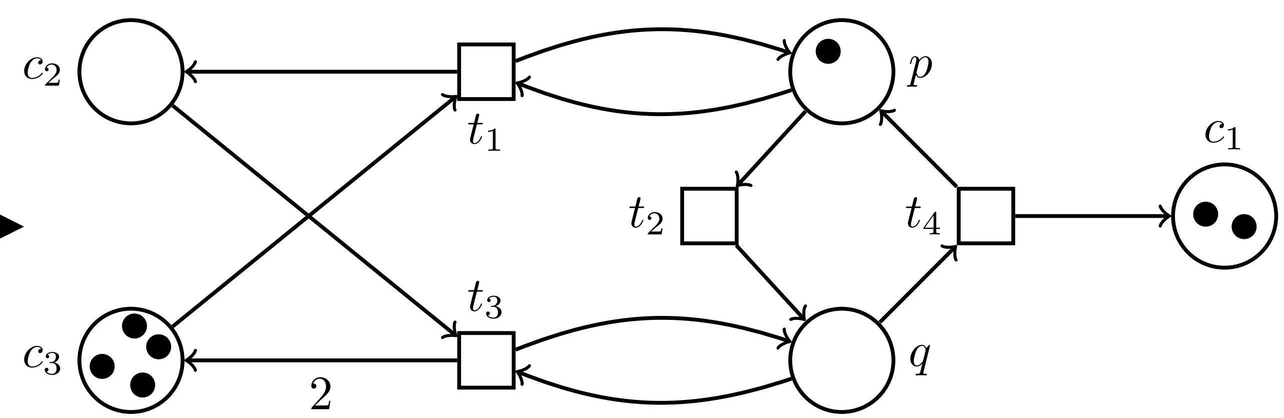
BIO nets can have **non-semilinear** reachability set

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

classic translation

VASS to Petri net

BIO net



Non-semilinear reachability

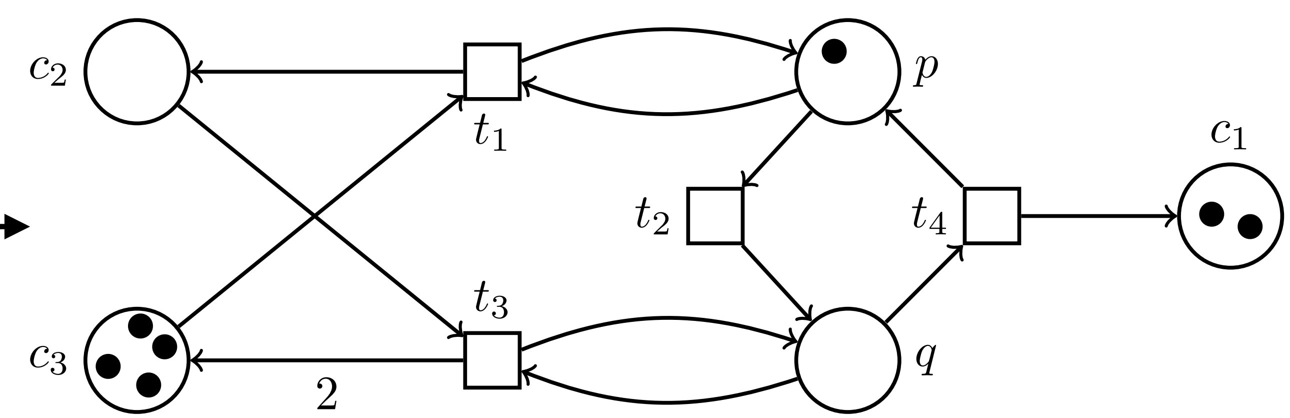
BIO nets can have **non-semilinear** reachability set

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

classic translation

VASS to Petri net

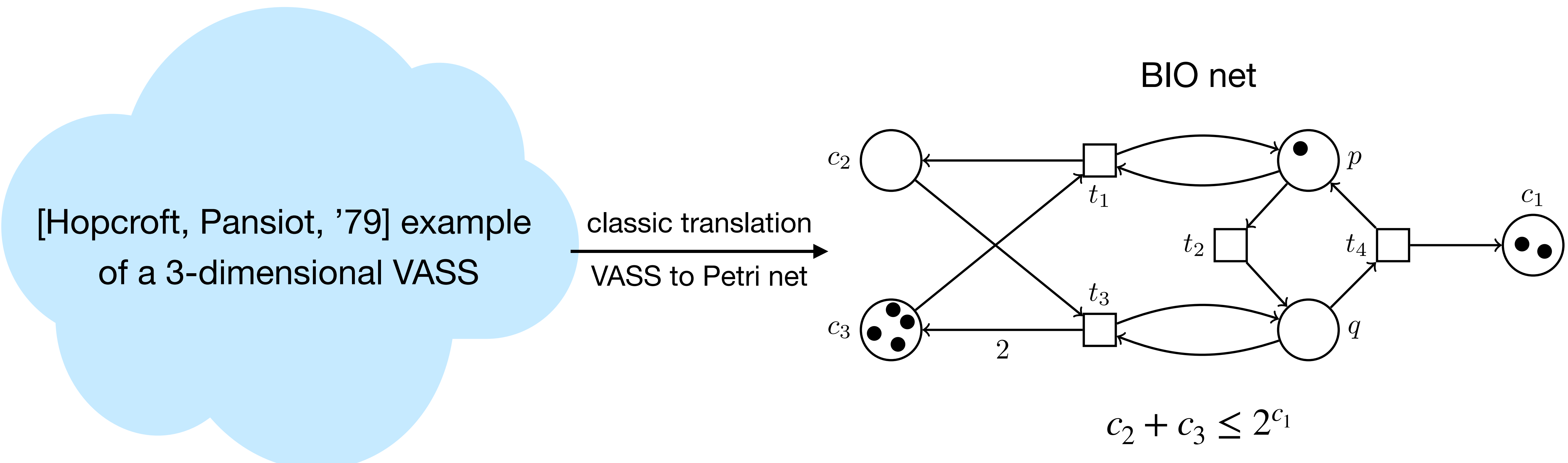
BIO net



$$c_2 + c_3 \le 2^{c_1}$$

Non-semilinear reachability

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



$$c_2 + c_3 \leq 2^{c_1}$$

Until now, unbounded Petri net classes with provably simpler reachability than the general case have semilinear reachability sets

BIO nets are locally flat

[Leroux, Sutre, '05]

Flat

$\exists$ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0 \forall M$, $M_0 \xrightarrow{*} M$ iff $M_0 \xrightarrow{t_1^{k_1} t_2^{k_2} \ldots t_\ell^{k_\ell}} M$

BIO nets are not flat…

BIO nets are locally flat

[Leroux, Sutre, '05]

Flat

$\exists$ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0 \forall M,\ M_0 \xrightarrow{*} M$ iff $M_0 \xrightarrow{t_1^{k_1} t_2^{k_2} \ldots t_\ell^{k_\ell}} M$

BIO nets are not flat…

[Leroux, Sutre, '05]

Locally flat

$\forall M,\ \exists$ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0,\ M_0 \xrightarrow{*} M$ iff $M_0 \xrightarrow{t_1^{k_1} t_2^{k_2} \ldots t_\ell^{k_\ell}} M$

BIO nets are locally flat

BIO nets are locally flat

<u>Flat</u>

[Leroux, Sutre, '05]

$\exists$ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0 \forall M,\ M_0 \xrightarrow{*} M$ iff $M_0 \xrightarrow{t_1^{k_1} t_2^{k_2} \ldots t_\ell^{k_\ell}} M$

BIO nets are not flat…

<u>Locally flat</u>

[Leroux, Sutre, '05]

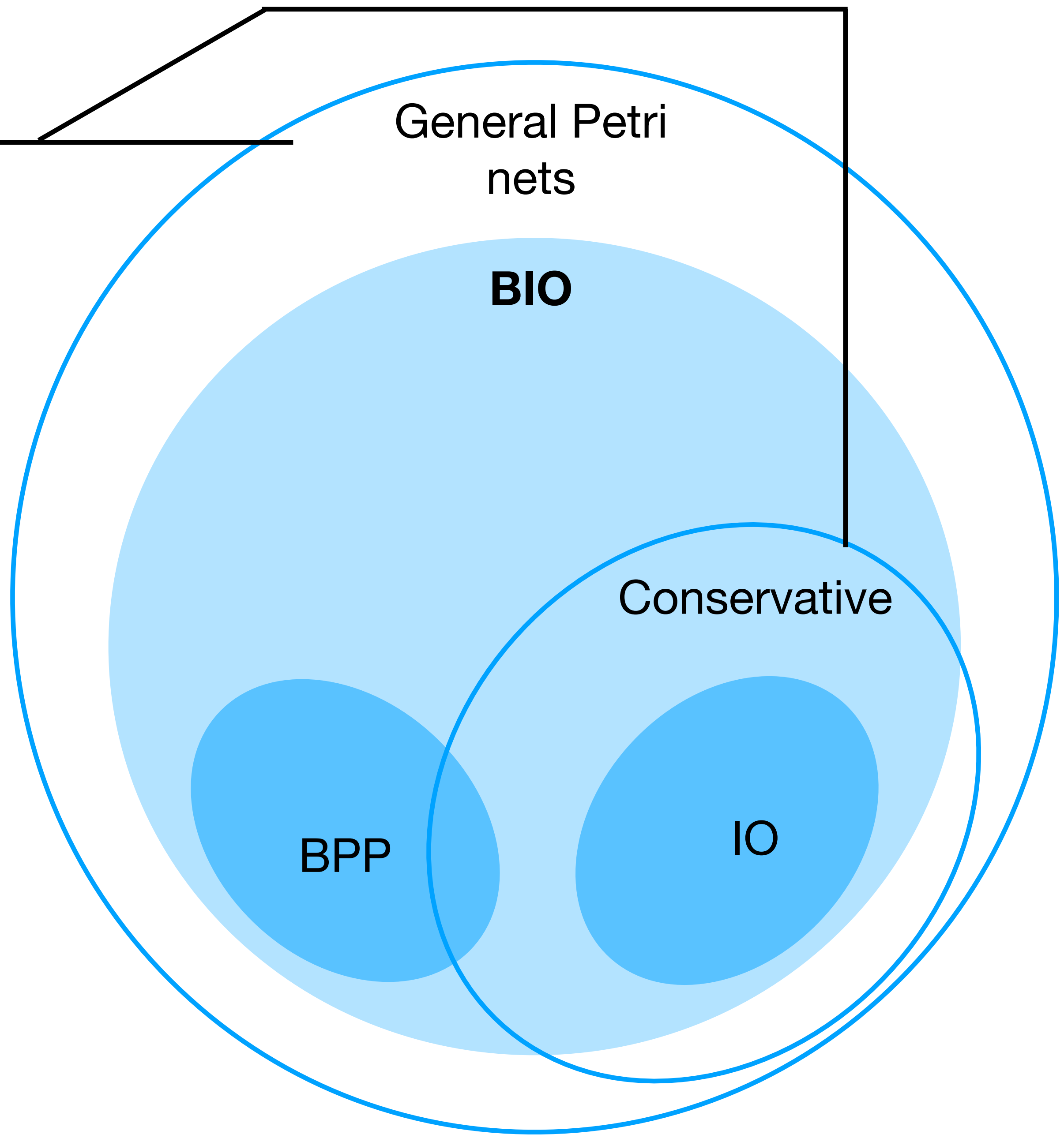
$\forall M,\ \exists$ sequence $t_1^* t_2^* \ldots t_\ell^*$ such that $\forall M_0,\ M_0 \xrightarrow{*} M$ iff $M_0 \xrightarrow{t_1^{k_1} t_2^{k_2} \ldots t_\ell^{k_\ell}} M$

BIO nets are locally flat

$\longrightarrow$ check **reachability properties** with
model checking **tools** that use acceleration techniques
e.g. FAST [Bardin, Finkel, Leroux, Petrucci, '03]

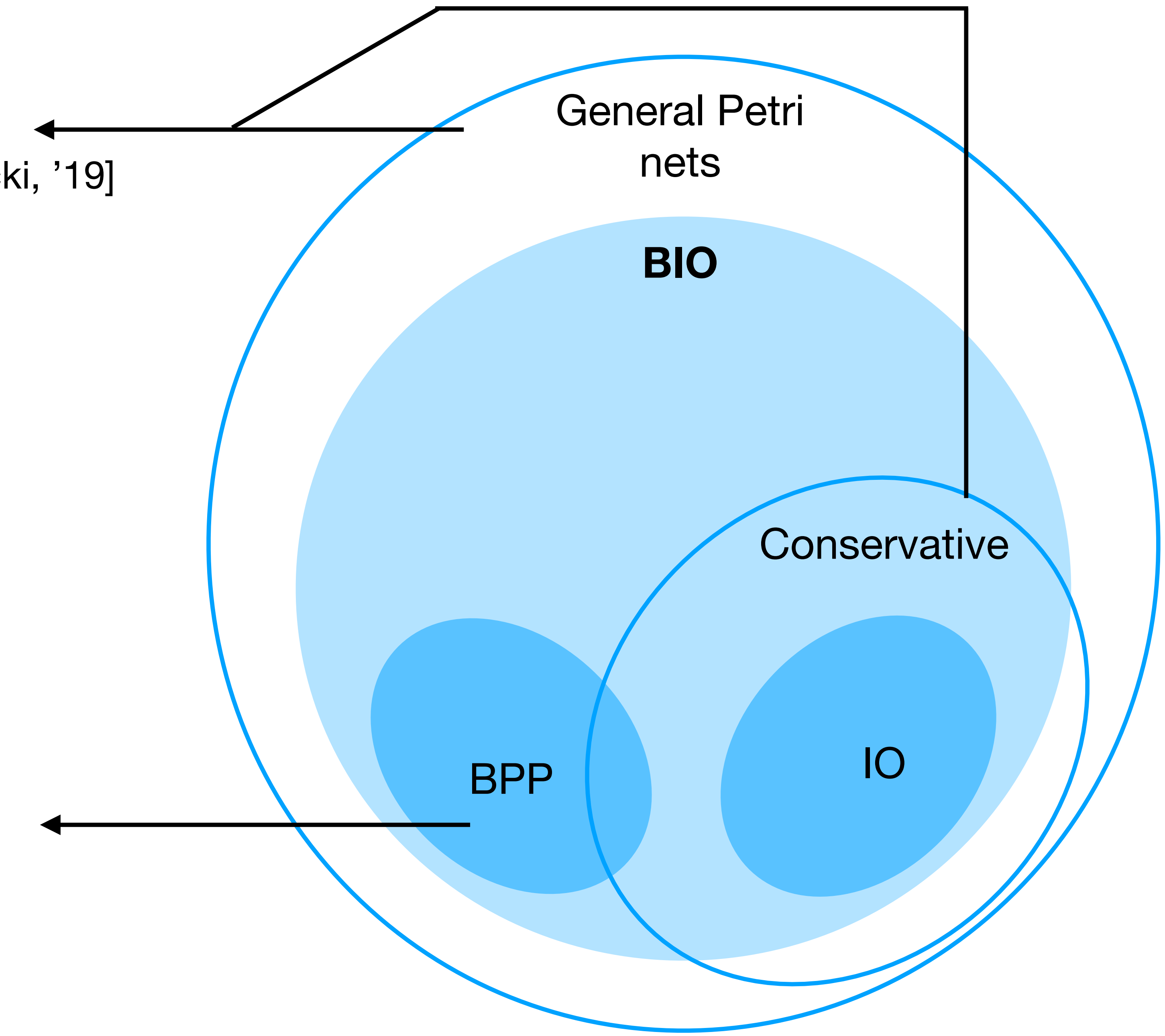
Cube-reachability summary

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



Cube-reachability summary

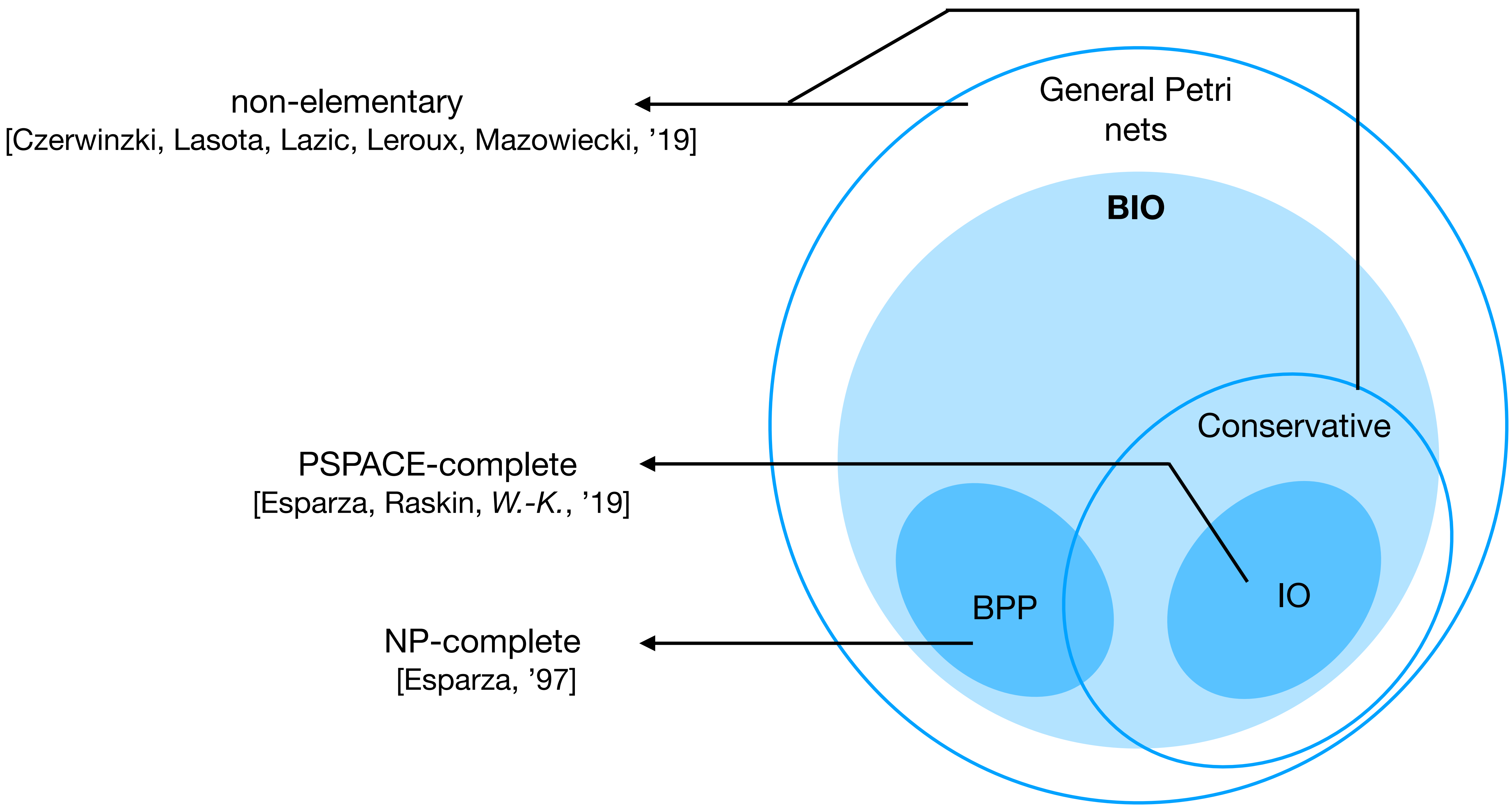
non-elementary
[Czerwinzki, Lasota, Lazic, Leroux, Mazowiecki, ’19]



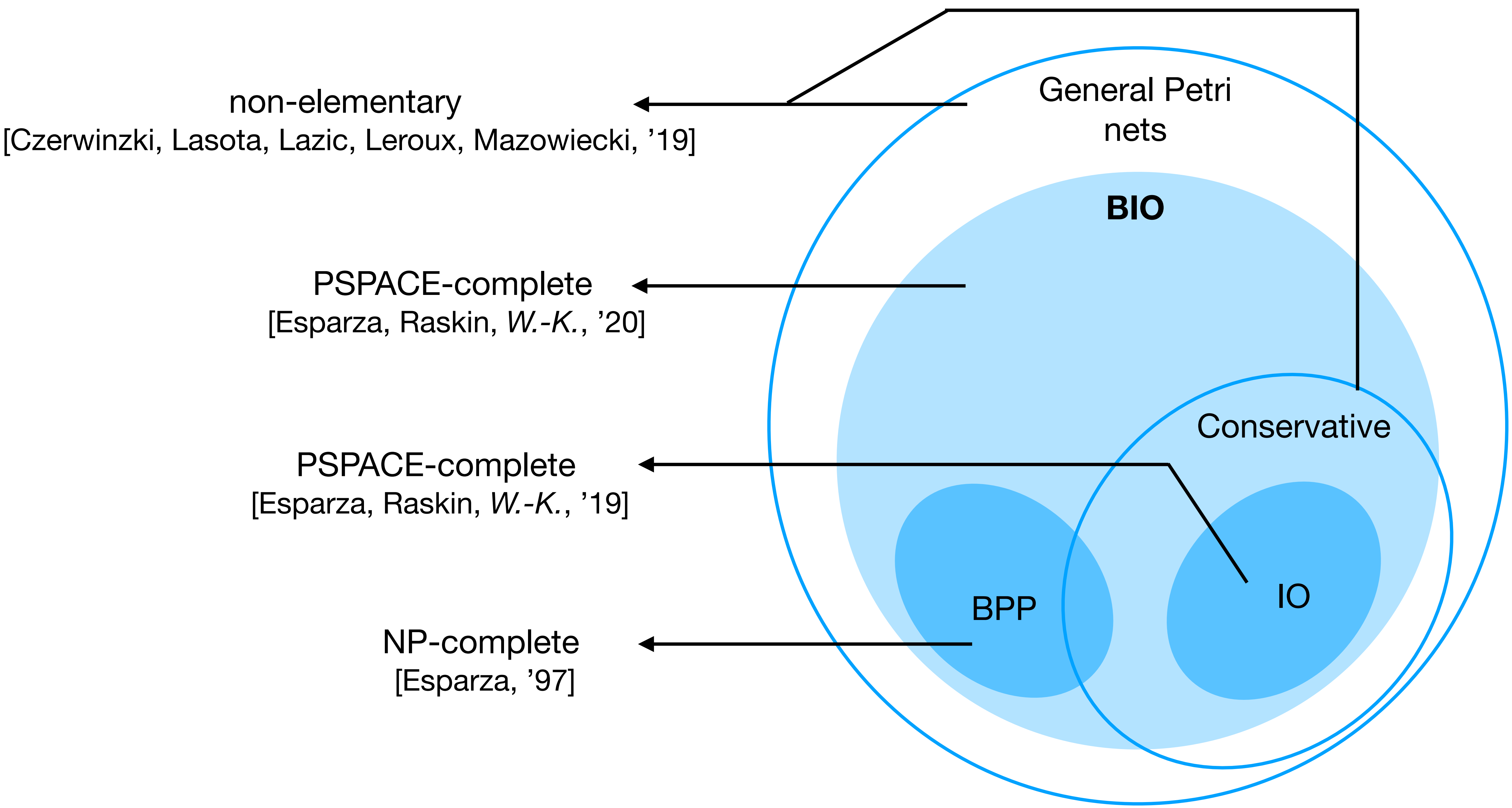
NP-complete
[Esparza, ’97]

C. Weil-Kennedy, TUM

Cube-reachability summary

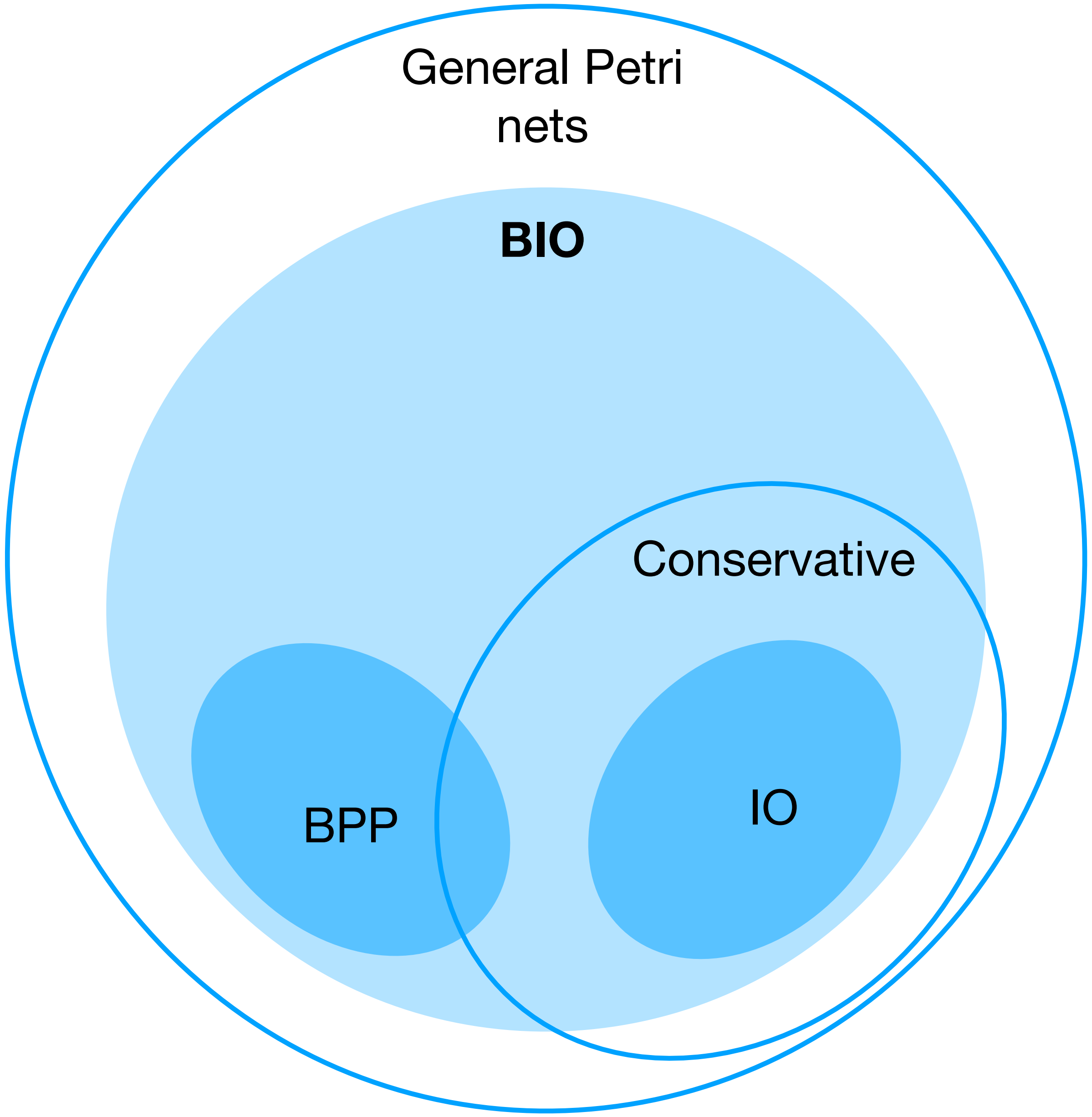


Cube-reachability summary

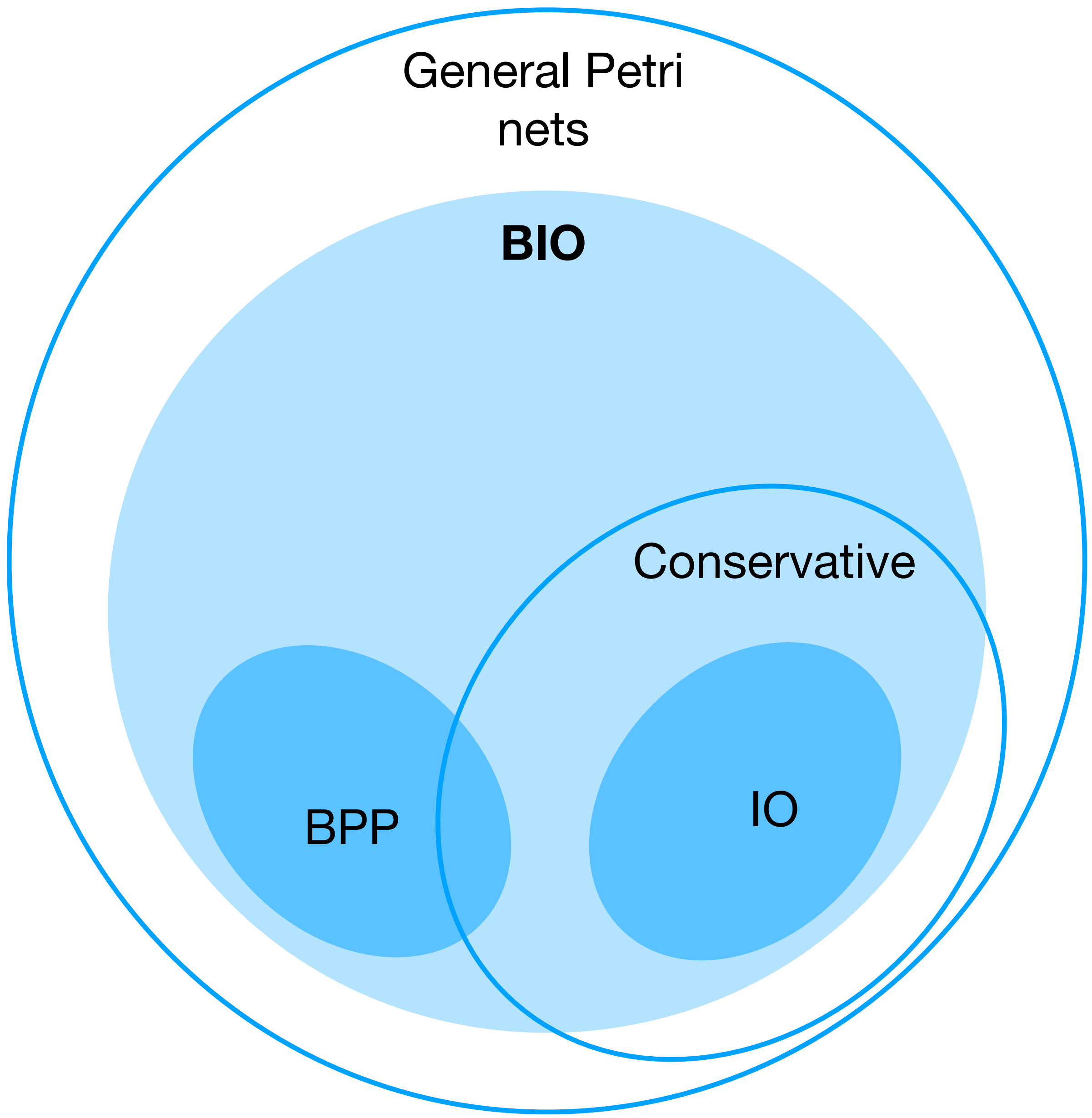


Conclusion

- 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

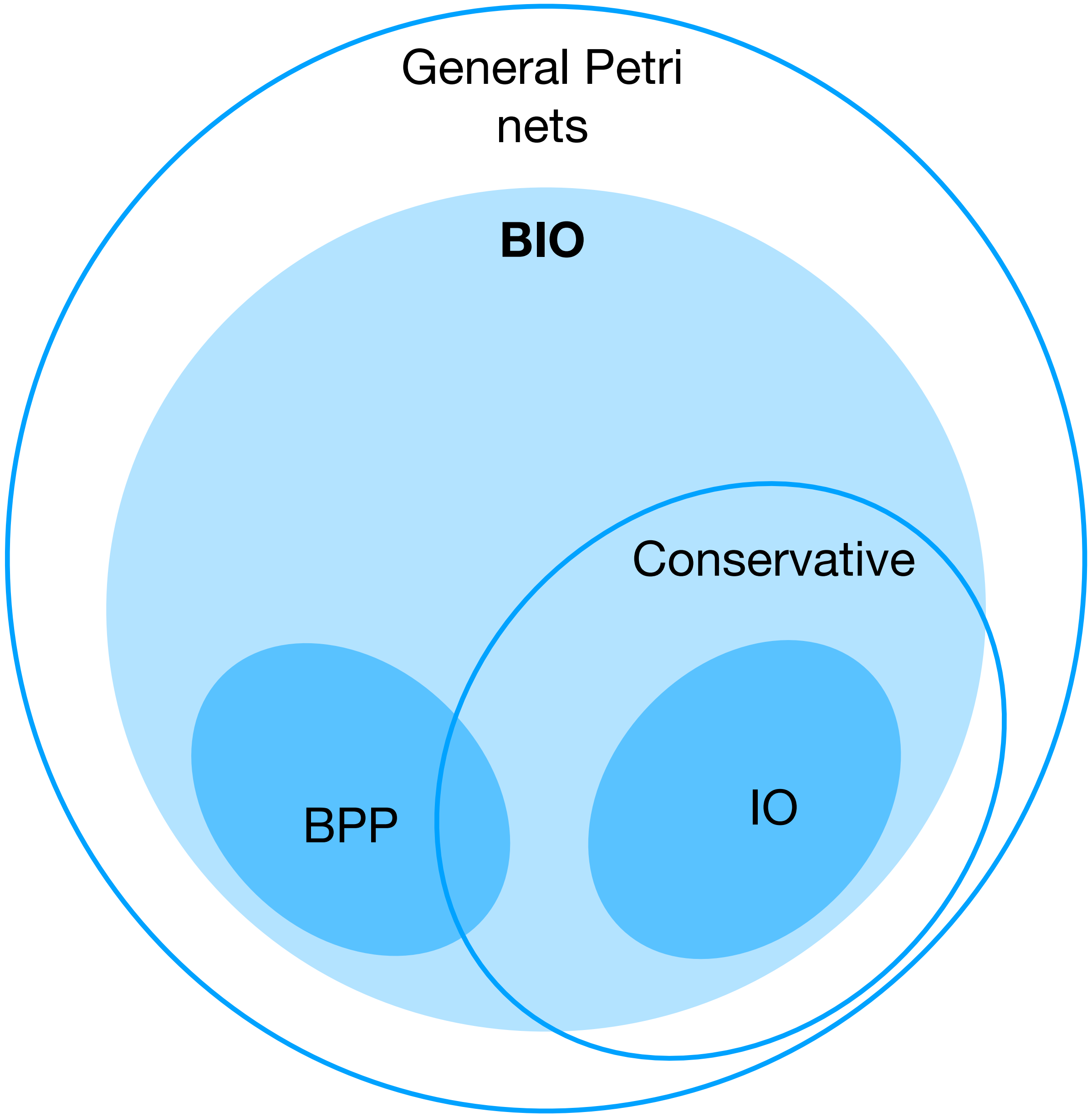


Conclusion



- 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!