Logics for Continuous Reachability in Petri Nets and Vector Addition Systems with States

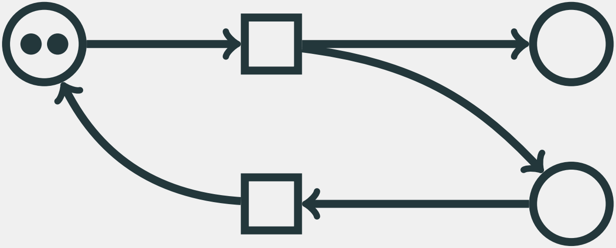
Michael Blondin

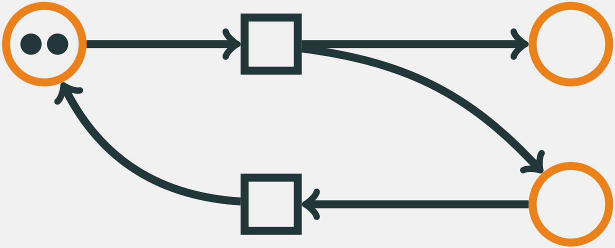
Technical University of Munich

Christoph Haase

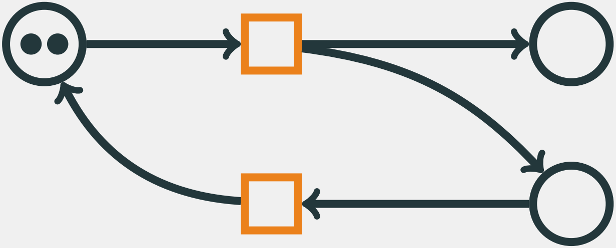
University of Oxford

Petri nets

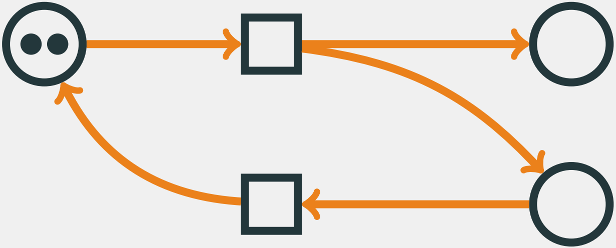




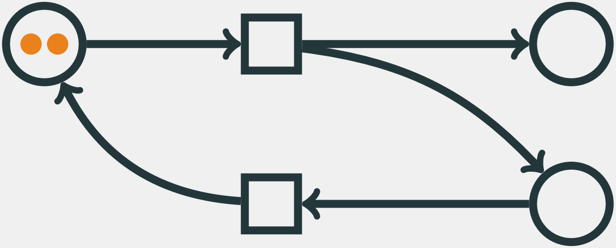
Places



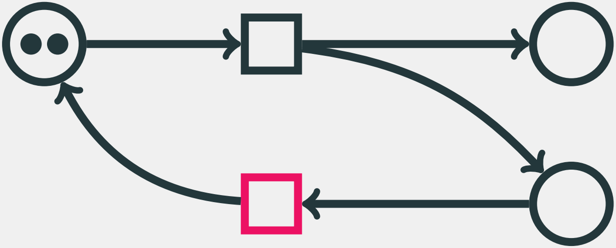
Transitions



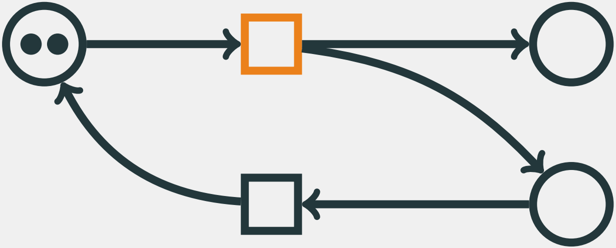
Arcs



Tokens

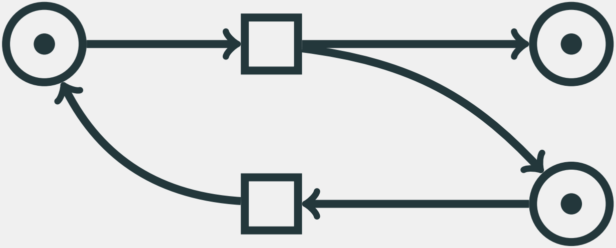


Disabled

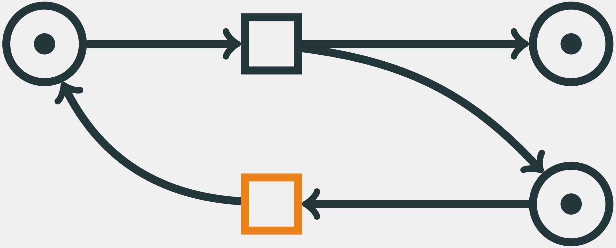


Enabled

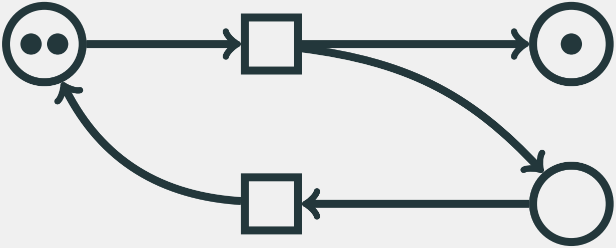
Petri nets

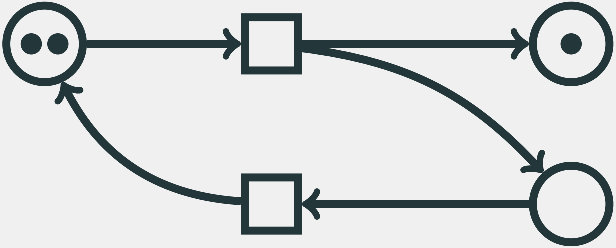


Petri nets

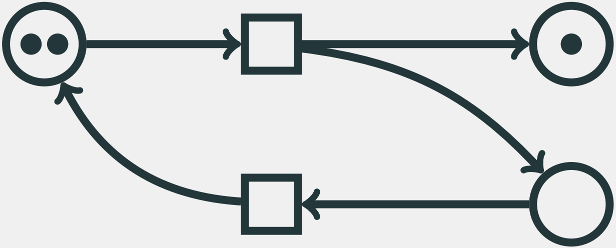


Petri nets





$$(2, 0, 0) \xrightarrow{*}_{\mathbb{N}} (2, 1, 0)$$



Reachability: $\boldsymbol{u} \xrightarrow{*}_{\mathbb{N}} \boldsymbol{v}$?

Petri nets

Concurrent programs

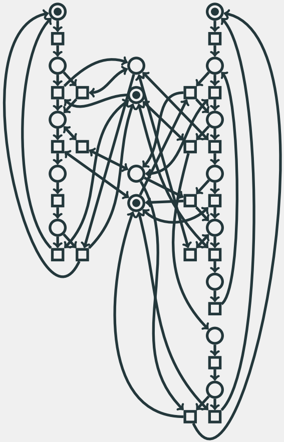
Protocols

Business processes

Biological processes

⋮

correct ? ⟶

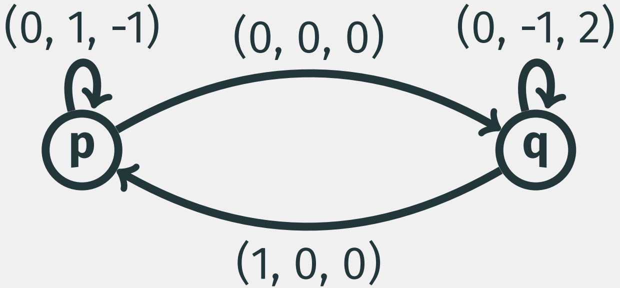


$$\text{Reachability: } \boldsymbol{u} \xrightarrow{*}_{\mathbb{N}} \boldsymbol{v}\,?$$

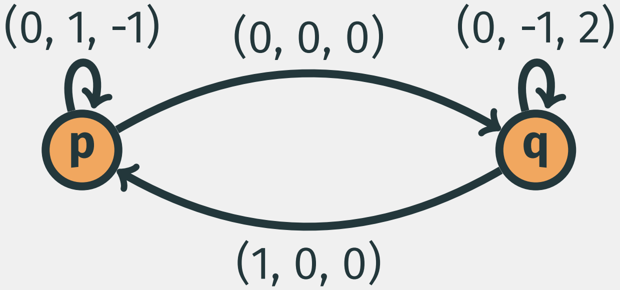
Verifying multi-threaded programs

Counters: number of threads

States: shared resources

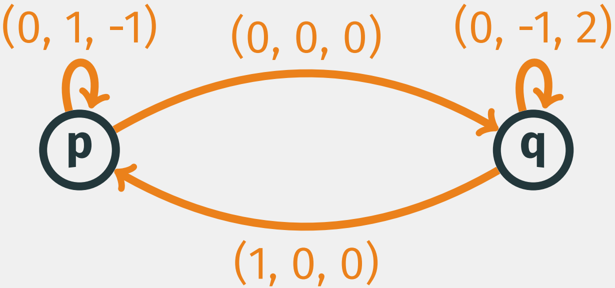

(0, 1, -1)
(0, 0, 0)
(0, -1, 2)
p
q
(1, 0, 0)

Petri nets / Vector addition systems with states (VASS)



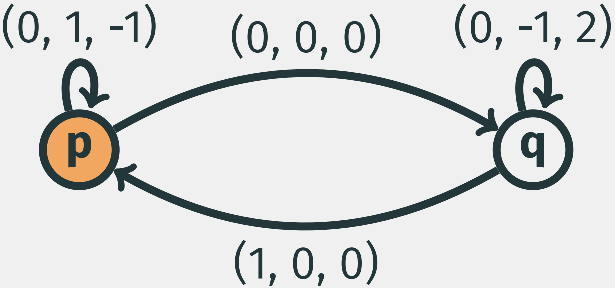
Control-states

Petri nets / Vector addition systems with states (VASS)



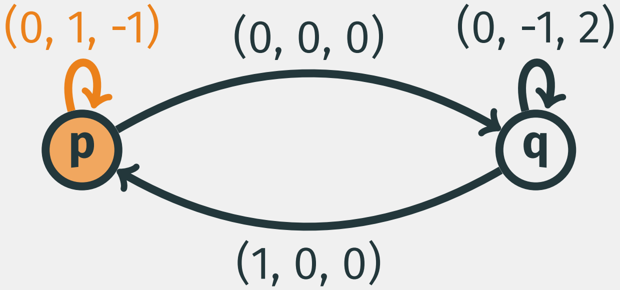
Transitions

Petri nets / Vector addition systems with states (VASS)

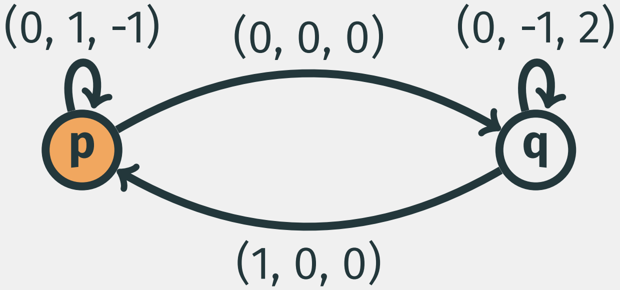


p(0, 0, 1)

Petri nets / Vector addition systems with states (VASS)

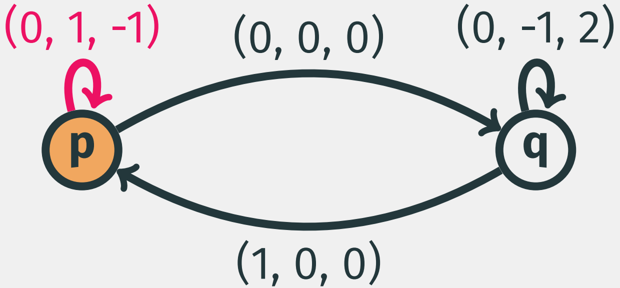


p(0, 0, 1)



p(0, 1, 0)

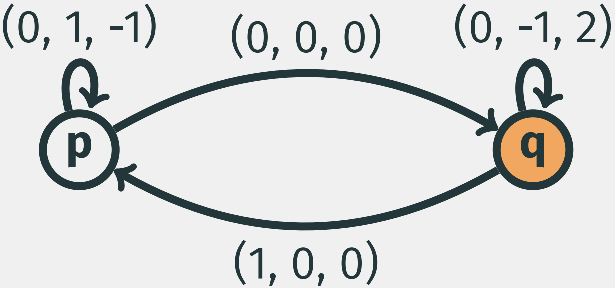
Petri nets / Vector addition systems with states (VASS)



p(0, 1, 0)

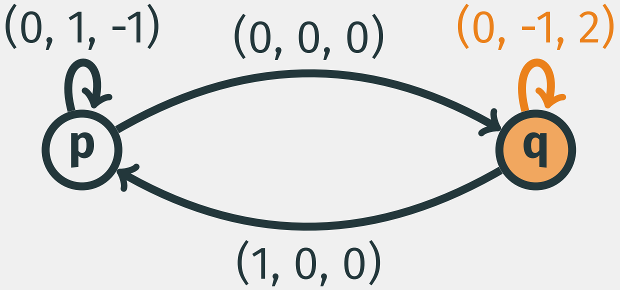
p(0, 1, 0)

Petri nets / Vector addition systems with states (VASS)



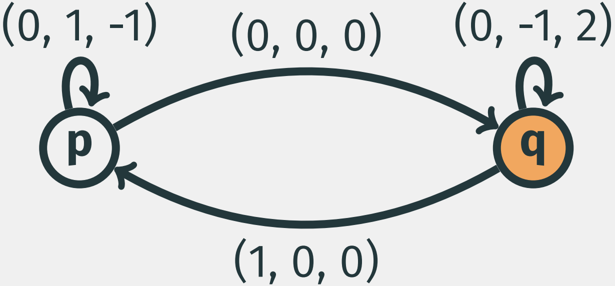
q(0, 1, 0)

Petri nets / Vector addition systems with states (VASS)



q(0, 1, 0)

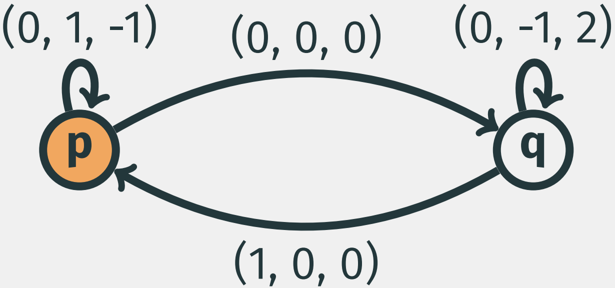
Petri nets / Vector addition systems with states (VASS)



q(0, 0, 2)

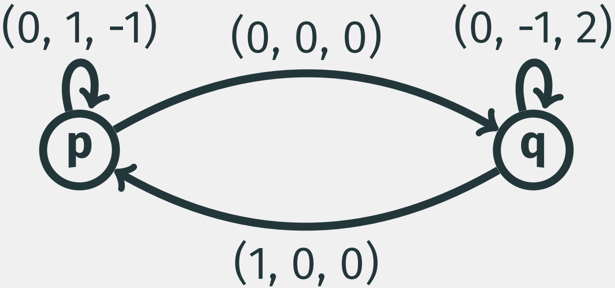
q(0, 0, 2)

Petri nets / Vector addition systems with states (VASS)

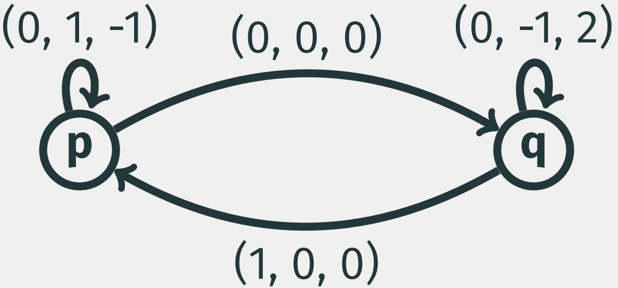


p(1, 0, 2)

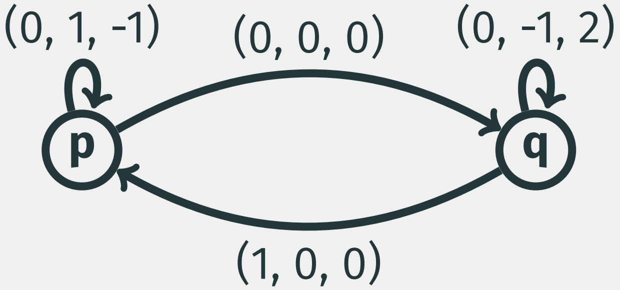
Petri nets / Vector addition systems with states (VASS)



$$p(0, 0, 1) \xrightarrow{*}_{\mathbb{N}} p(1, 0, 2)$$



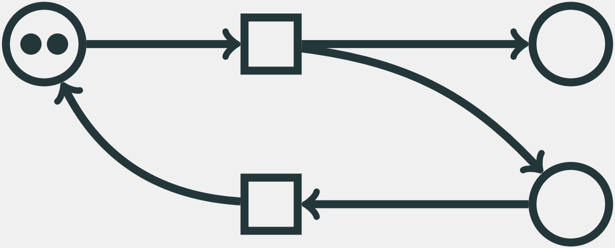
$$p(0,0,1) \xrightarrow{*}_{\mathbb{N}} p(x,y,z) \iff 0 < y + z \leq 2^x$$



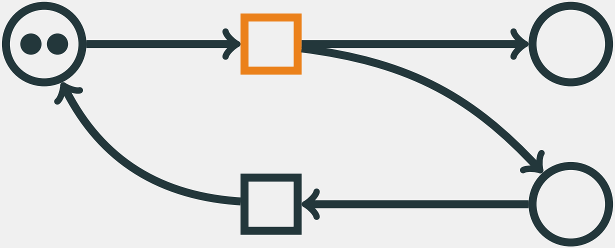
Reachability: $p(\boldsymbol{u}) \xrightarrow{*}_{\mathbb{N}} q(\boldsymbol{v})$?

Reachability is...

- equivalent for Petri nets and VASS
- not expressible in FO($\mathbb{N}$, +, <)
- EXPSPACE-hard (Lipton '76)
- solvable in cubic-Ackermannian time
(Leroux and Schmitz LICS'15)



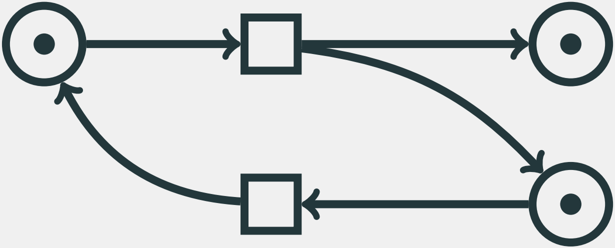
Can fire transitions fractionally



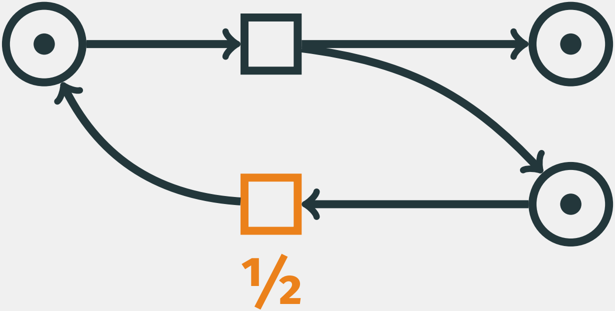
Can fire transitions fractionally

Continuous Petri nets

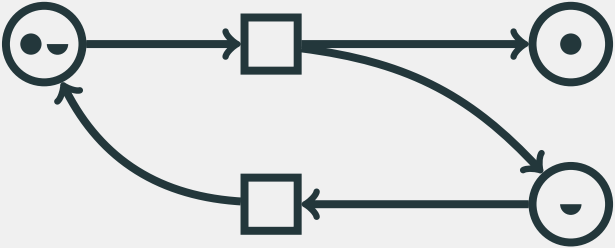
David & Alla '87



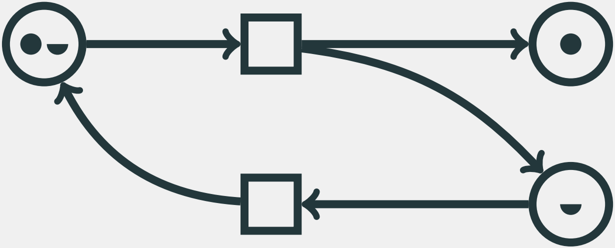
Can fire transitions
fractionally



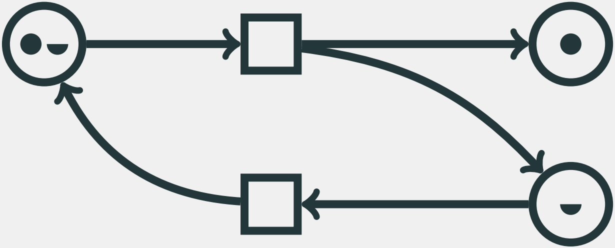
Can fire transitions fractionally



Can fire transitions fractionally



$$(2, 0, 0) \xrightarrow{*}_{\mathbb{Q}_+} (1\tfrac{1}{2}, 1, \tfrac{1}{2})$$



Continuous reachability: $\boldsymbol{u} \xrightarrow{*}_{\mathbb{Q}_+} \boldsymbol{v}$?

Continuous reachability is...

- an over-approximation:

$$\neg(\boldsymbol{u} \xrightarrow{*}_{\mathbb{Q}_+} \boldsymbol{v}) \text{ implies } \neg(\boldsymbol{u} \xrightarrow{*}_{\mathbb{N}} \boldsymbol{v})$$

- PTIME-complete (Fraca and Haddad PN'13)

- expressible in $\exists$ FO($\mathbb{Q}_+$, +, <)

(B., Finkel, Haase and Haddad TACAS'16)

Continuous Petri nets

David & Alla '87

Continuous reachability is...

- an over-approximation

fast with SMT solver
...but NP-complete

- PTIME-complete
- expressible in $\exists$ FO($\mathbb{Q}_+$, +, <)

Continuous Petri nets

David & Alla '87

Continuous reachability is...

- an over-approximation

often good

...but no control-states

- PTIME-complete
- expressible in $\exists\,\mathrm{FO}(\mathbb{Q}_+, +, <)$

new fragment of $\exists$ FO($\mathbb{Q}_+$, +, <)

- PTIME-complete
- equivalent to Petri net continuous reachability

new model: continuous VASS

- with control-states
- with reachability equivalent to $\exists$ FO($\mathbb{Q}$, +, <)

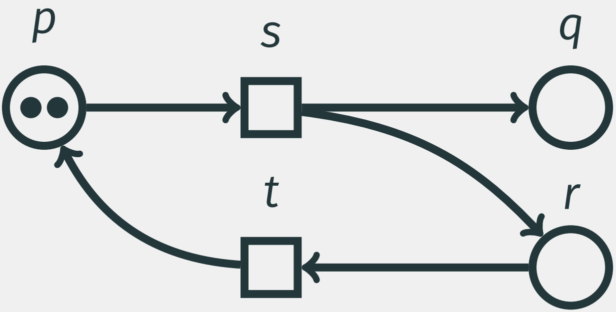
new fragment of $\exists$ FO($\mathbb{Q}_+$, +, <)

- PTIME-complete
- equivalent to Petri net continuous reachability

new model: continuous VASS

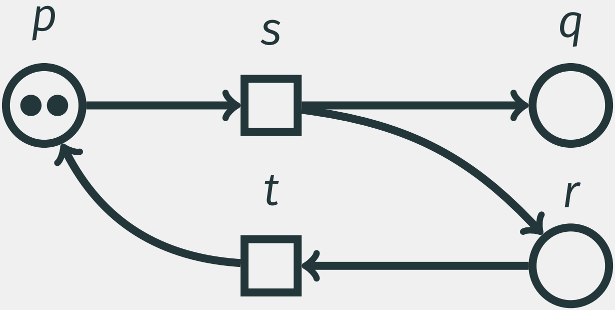
- with control-states
- with reachability equivalent to $\exists$ FO($\mathbb{Q}$, +, <)

Expressing continuous reachability



$\boldsymbol{y}$ reachable $\iff$ $\exists$ Parikh vector π s.t.

Expressing continuous reachability

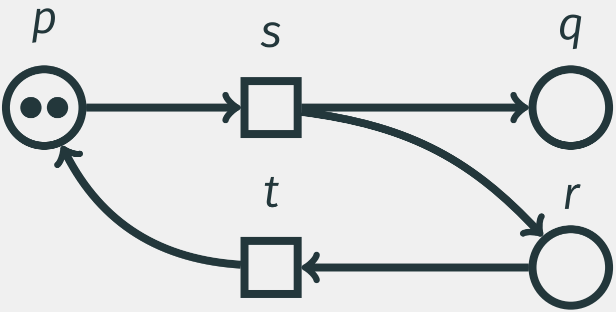


$\boldsymbol{y}$ reachable $\iff$ $\exists$ Parikh vector π s.t.

a) $\boldsymbol{y}(p) = 2 - \pi(s) + \pi(t)$ $\quad \boldsymbol{y}(q) = \pi(s)$

$\boldsymbol{y}(r) = \pi(s) + \pi(t)$

Expressing continuous reachability

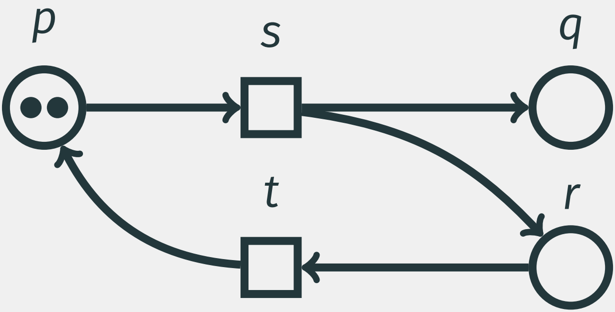


$\boldsymbol{y}$ reachable $\iff \exists$ Parikh vector π s.t.

b) $\{u : \pi(u) > 0\}$ firable from (2, 0, 0)

c) $\{u : \pi(u) > 0\}$ firable to $\boldsymbol{y}$

Expressing continuous reachability

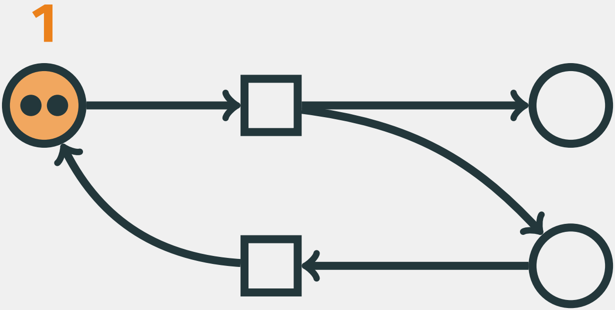


linear size $\exists FO(\mathbb{Q}_+, +, <)$ formula

b) $\{u : \pi(u) > 0\}$ firable from $(2, 0, 0)$

c) $\{u : \pi(u) > 0\}$ firable to $\boldsymbol{y}$

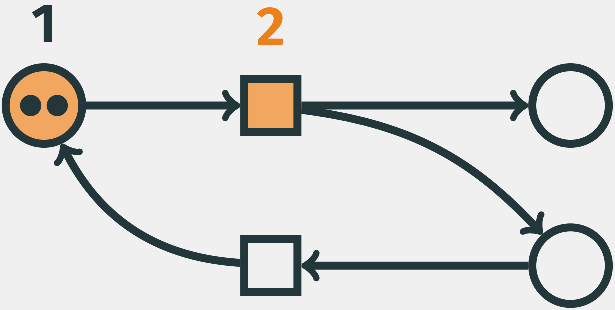
Expressing continuous reachability



linear size $\exists FO(\mathbb{Q}_+, +, <)$ formula

b) $\{u : \pi(u) > 0\}$ firable from (2, 0, 0)

c) $\{u : \pi(u) > 0\}$ firable to $\boldsymbol{y}$

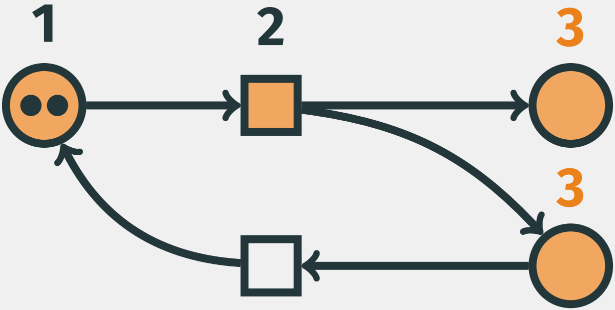


linear size $\exists FO(\mathbb{Q}_+, +, <)$ formula

b) $\{u : \pi(u) > 0\}$ firable from $(2, 0, 0)$

c) $\{u : \pi(u) > 0\}$ firable to $\boldsymbol{y}$

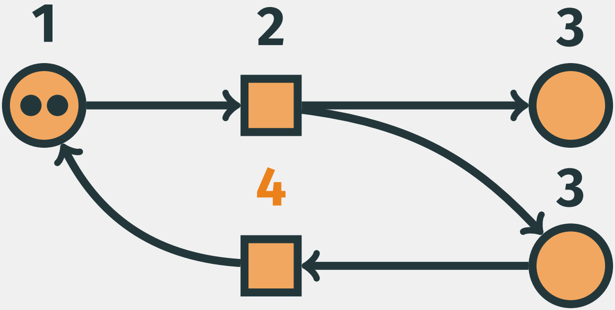
Expressing continuous reachability



linear size $\exists FO(\mathbb{Q}_+, +, <)$ formula

b) $\{u : \pi(u) > 0\}$ firable from (2, 0, 0)

c) $\{u : \pi(u) > 0\}$ firable to $\boldsymbol{y}$

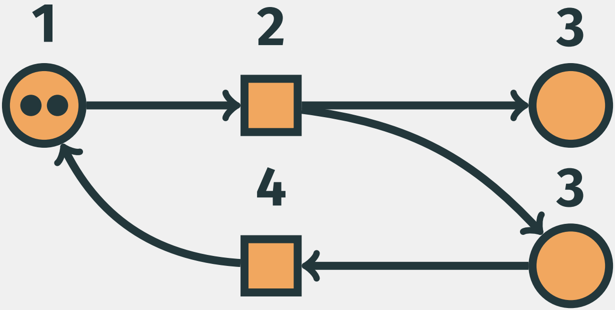


linear size $\exists FO(\mathbb{Q}_+, +, <)$ formula

b) $\{u : \pi(u) > 0\}$ firable from (2, 0, 0)

c) $\{u : \pi(u) > 0\}$ firable to $\boldsymbol{y}$

Expressing continuous reachability



linear size $\exists FO(\mathbb{Q}_+, +, <)$ formula

NP-complete

Conjunction of terms of the form

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n \sim c \vee \bigvee_{1 \leq i \leq m} \bigwedge_{j \in J_i} x_j > 0$$

Conjunction of terms of the form

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n \sim c \vee \bigvee_{1 \le i \le m} \bigwedge_{j \in J_i} x_j > 0$$

variables over $\mathbb{Q}_+$

Conjunction of terms of the form

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n \sim c \vee \bigvee_{1 \leq i \leq m} \bigwedge_{j \in J_i} x_j > 0$$

variables over $\mathbb{Q}_+$

coeff. in $\mathbb{Z}$

Conjunction of terms of the form

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n \sim c \vee \bigvee_{1 \leq i \leq m} \bigwedge_{j \in J_i} x_j > 0$$

variables over $\mathbb{Q}_+$

coeff. in $\mathbb{Z}$

$\sim$ is $\geq$ or $>$

Examples :

$$x = 0 \quad \equiv \quad -x \geq 0$$

Convex linear Horn constraints

Examples :

$$x = 0 \quad \equiv \quad -x \geq 0$$

$$x > 0 \rightarrow \bigvee_{y \in Y} y > 0 \quad \equiv \quad x = 0 \vee \bigvee_{y \in Y} y > 0$$

Examples :

$$x = 0 \quad \equiv \quad -x \geq 0$$

$$x > 0 \rightarrow \bigvee_{y \in Y} y > 0 \quad \equiv \quad x = 0 \vee \bigvee_{y \in Y} y > 0$$

$$x > 0 \leftarrow \bigvee_{y \in Y} y > 0 \quad \equiv \quad \bigwedge_{y \in Y} (y = 0 \vee x > 0)$$

Examples :

$$x = 0 \quad \equiv \quad -x \geq 0$$

$$x > 0 \rightarrow \bigvee_{y \in Y} y > 0 \quad \equiv \quad x = 0 \vee \bigvee_{y \in Y} y > 0$$

$$x > 0 \leftarrow \bigvee_{y \in Y} y > 0 \quad \equiv \quad \bigwedge_{y \in Y} (y = 0 \vee x > 0)$$

$$x > 0 \rightarrow \bigwedge_{y \in Y} y > 0 \quad \equiv \quad x = 0 \vee \bigwedge_{y \in Y} y > 0$$

Convex linear Horn constraints

Examples :

$$x = 0 \quad \equiv \quad -x \geq 0$$

$$x > 0 \rightarrow \bigvee_{y \in Y} y > 0 \quad \equiv \quad x = 0 \vee \bigvee_{y \in Y} y > 0$$

$$x > 0 \leftarrow \bigvee_{y \in Y} y > 0 \quad \equiv \quad \bigwedge_{y \in Y} (y = 0 \vee x > 0)$$

$$x > 0 \leftarrow \bigwedge_{y \in Y} y > 0 \quad \equiv \quad \text{not expressible}$$

Examples :

- graph reachability
- strong connectivity (from a node)

in subgraph $G[u : \boldsymbol{x}_u > 0]$

Convex linear Horn constraints

Theorem

Continuous Petri net reachability is expressible by a quadratic size formula

Proof idea

$$\boldsymbol{x} + \boldsymbol{C} \cdot \pi = \boldsymbol{y} \ \wedge \ \text{firability constraints}$$

Convex linear Horn constraints

Theorem

Satisfiability is PTIME-complete

Proof idea

- $\in$ PTIME: algorithm exploiting convexity
- Hardness: from linear prog. feasability

Related work:

CSP of linear Horn constraints
(Jonsson and Backström '98
Koubarakis '01)

Convex linear Horn constraints

incomparable

Related work:

CSP of linear Horn constraints

(Jonsson and Backström '98

Koubarakis '01)

Solutions as reachability sets

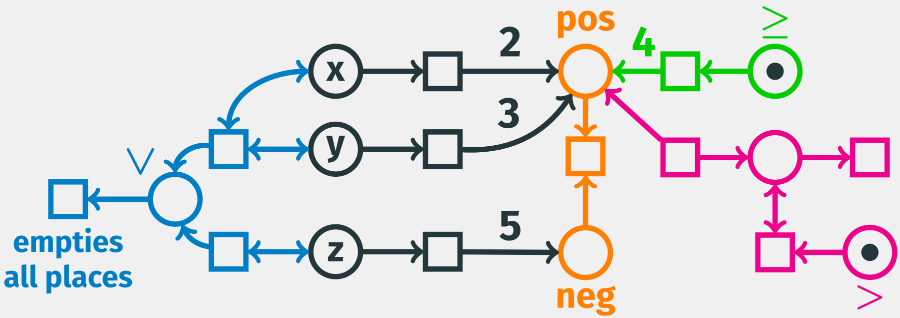
Theorem

Convex linear Horn constraints solutions
are expressible as
reachability sets of continuous Petri nets

$$2x + 3y - 5z > -4 \lor (x > 0 \land y > 0) \lor z > 0$$

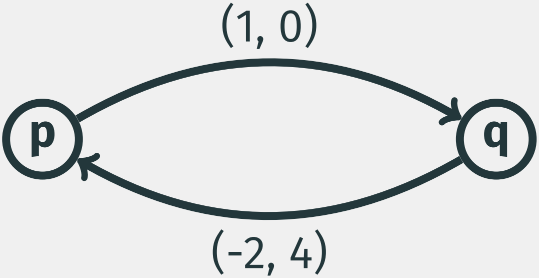
$$\iff$$

all places can be emptied



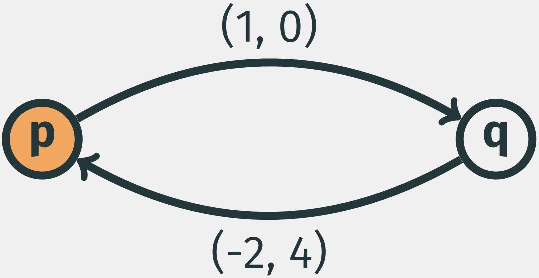
Continuous VASS:

- Hybrid model
- subsume continuous Petri nets



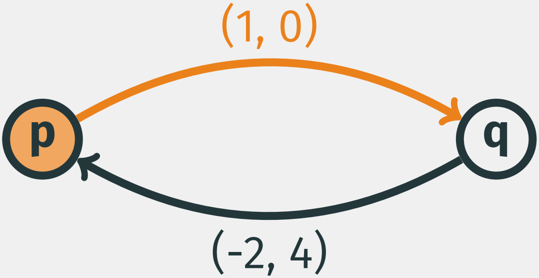
Transitions can be scaled by $0 < x \leq 1$

Continuous VASS



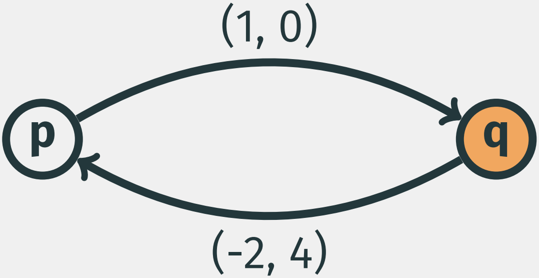
p(0, 0)

Continuous VASS



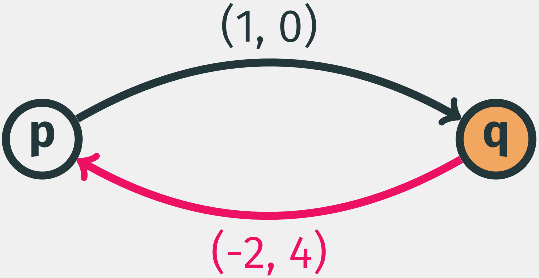
p(0, 0)

Continuous VASS



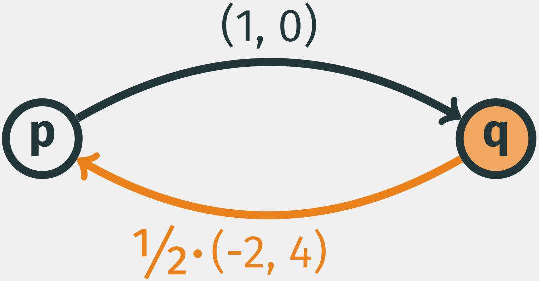
q(1, 0)

Continuous VASS



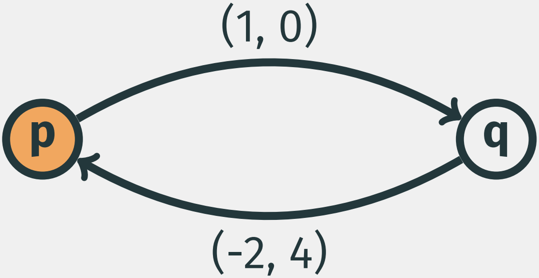
q(1, 0)

Continuous VASS



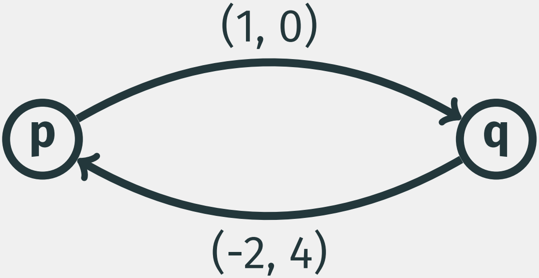
q(1, 0)

Continuous VASS

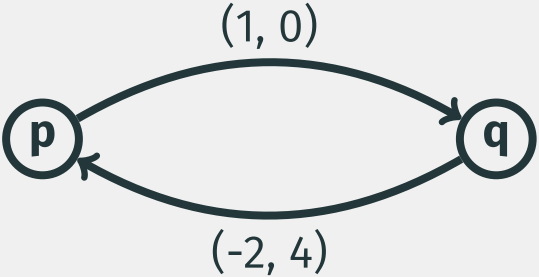


p(0, 2)

Continuous VASS



$$p(0,0) \xrightarrow{*}_{\mathbb{Q}_+} q(0,2)$$



Reachability: $p(\boldsymbol{u}) \xrightarrow{*}_{\mathbb{Q}_+} q(\boldsymbol{v})$?

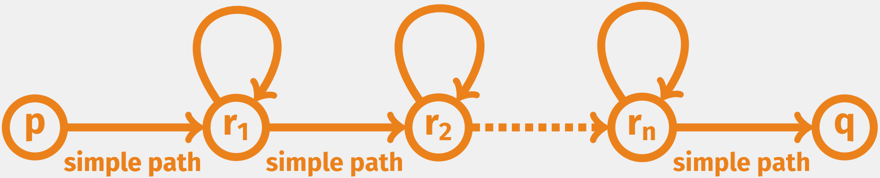
Continuous VASS: logical characterization

Theorem

$$p(\boldsymbol{u}) \xrightarrow{*}_{\mathbb{Q}_+} q(\boldsymbol{v})$$

is expressible in $\exists\,\mathrm{FO}(\mathbb{Q}, +, <)$

Continuous VASS: logical characterization

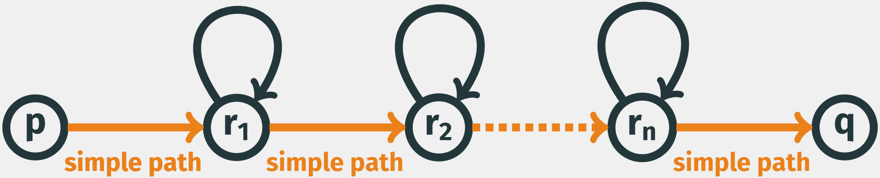


Theorem

$$p(\boldsymbol{u}) \xrightarrow{*}_{\mathbb{Q}_+} q(\boldsymbol{v})$$

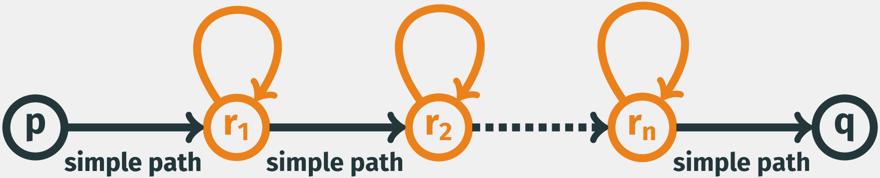
is expressible in $\exists\,\mathrm{FO}(\mathbb{Q}, +, <)$

Continuous VASS: logical characterization



Fixed length runs are easy to express in $\exists FO(\mathbb{Q}, +, <)$

Continuous VASS: logical characterization



$$r(\boldsymbol{x}) \xrightarrow{*}_{\mathbb{Q}_+} r(\boldsymbol{y})$$

$$r(\boldsymbol{x}) \xrightarrow{*}_{\mathbb{Q}_+} r(\boldsymbol{y})$$

Equivalent $\updownarrow$

$$r(\boldsymbol{x}) \xrightarrow{*}_{\mathbb{Q}} r(\boldsymbol{y})$$
$$\wedge\ r(\boldsymbol{x}) \xrightarrow{*}_{\mathbb{Q}_+} r(\_)$$
$$\wedge\ r(\_) \xrightarrow{*}_{\mathbb{Q}_+} r(\boldsymbol{y})$$

Continuous VASS: logical characterization

Characterization of admissible paths

$$r(\boldsymbol{x}) \xrightarrow{*}_{\mathbb{Q}} r(\boldsymbol{y})$$

$$\land\ r(\boldsymbol{x}) \xrightarrow{*}_{\mathbb{Q}_+} r(\_)$$

$$\land\ r(\_) \xrightarrow{*}_{\mathbb{Q}_+} r(\boldsymbol{y})$$

Continuous VASS: logical characterization

Next slide

$$r(\boldsymbol{x}) \xrightarrow{*}_{\mathbb{Q}} r(\boldsymbol{y})$$

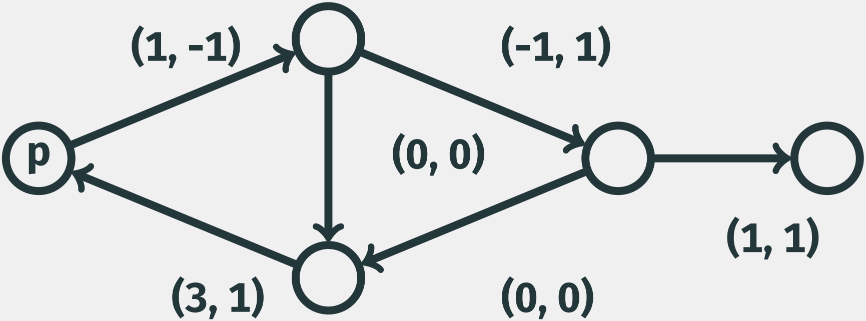
$$\wedge\ r(\boldsymbol{x}) \xrightarrow{*}_{\mathbb{Q}_+} r(\_)$$

$$\wedge\ r(\_) \xrightarrow{*}_{\mathbb{Q}_+} r(\boldsymbol{y})$$

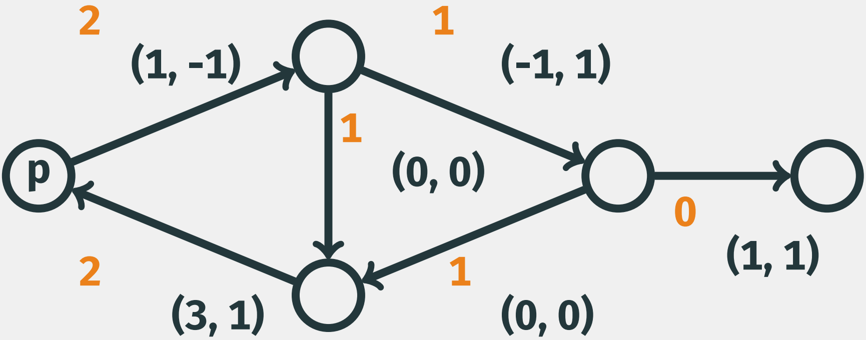
VASS cyclic $\mathbb{Q}$-reachability

$$p(\boldsymbol{u}) \xrightarrow{*}_{\mathbb{Q}} p(\boldsymbol{v})?$$

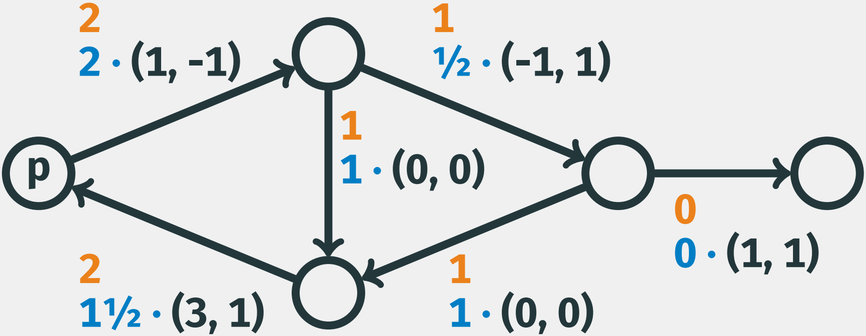
$$p(0,0) \xrightarrow{*}_{\mathbb{Q}} p(6,0)?$$



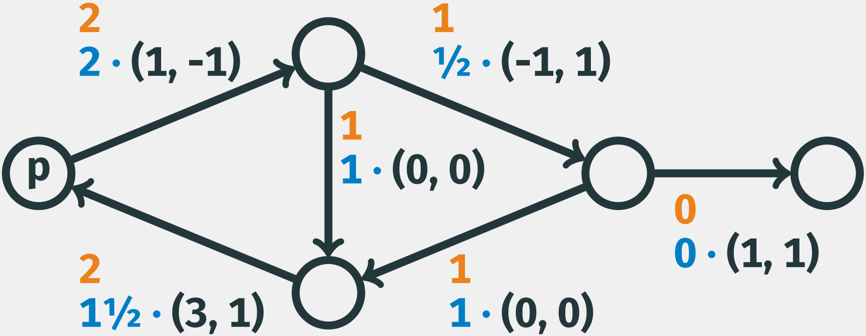
Guess transitions occurrences



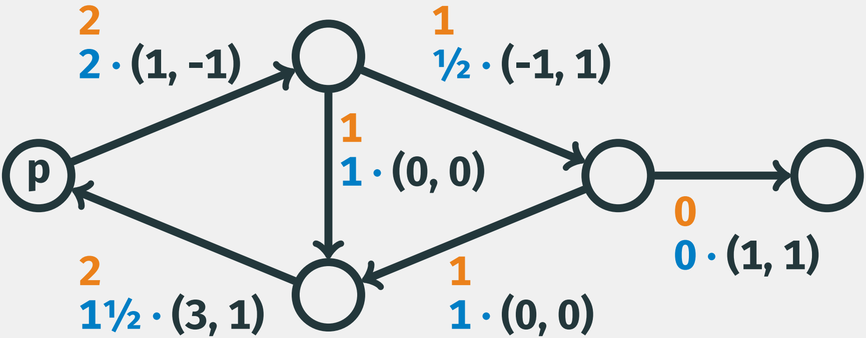
Guess scaling factors



occurrences ≥ scaling

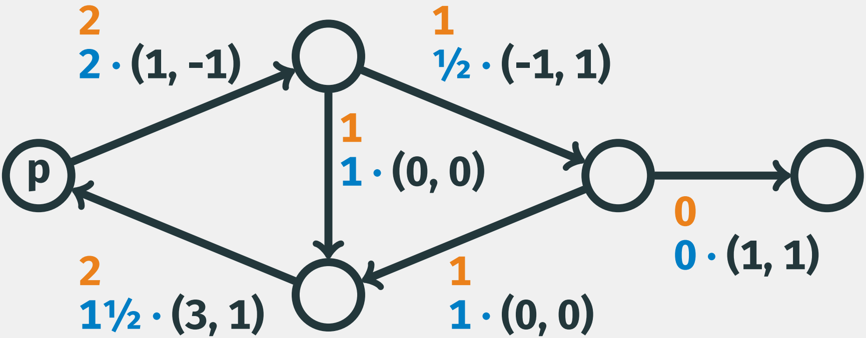


occurrences > 0 $\leftrightarrow$ scaling > 0

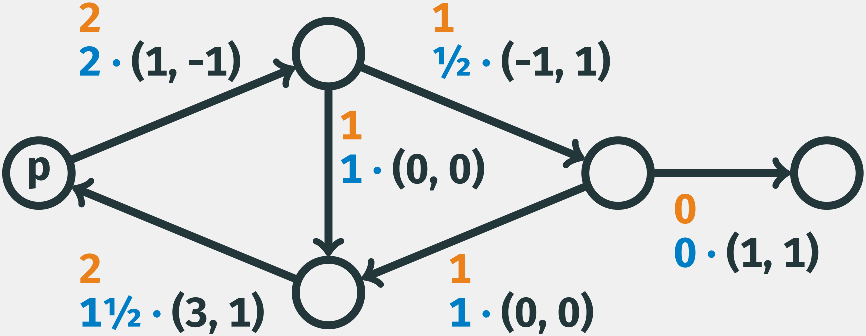


VASS cyclic $\mathbb{Q}$-reachability

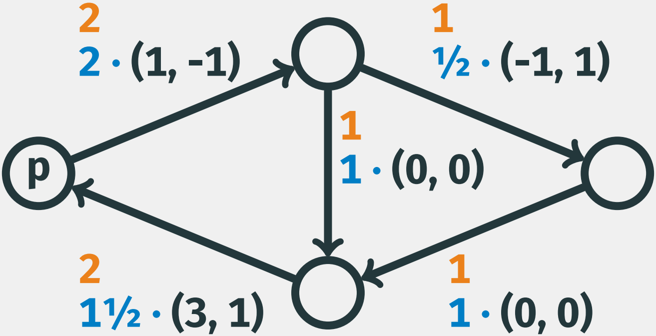
$$(0, 0) + \sum_{t \in T} \boldsymbol{f}_t \cdot \boldsymbol{z}_t = (6, 0)$$



G[$\boldsymbol{x}_t$ > 0] strongly connected

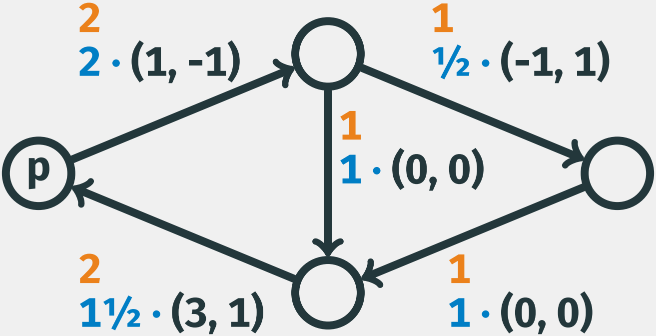


G[x_t > 0] strongly connected



VASS cyclic $\mathbb{Q}$-reachability

$$\sum_{t \in \text{in}(q)} x_t = \sum_{t \in \text{out}(q)} x_t$$



VASS cyclic $\mathbb{Q}$-reachability

Theorem

These conditions are expressible as convex linear Horn constraints

Corollary

VASS cyclic $\mathbb{Q}$-reachability is in PTIME

VASS cyclic $\mathbb{Q}$-reachability

Theorem

These conditions are expressible as convex linear Horn constraints

Corollary

VASS cyclic $\mathbb{Q}$-reachability is in PTIME

Conclusion: summary

- new PTIME fragment of $\exists\mathrm{FO}(\mathbb{Q}, +, <)$
- logical characterization of continuous Petri nets
- new hybrid model: continuous VASS
- characterization of $\exists\mathrm{FO}(\mathbb{Q}, +, <)$

Conclusion: future work

- optimization of continuous Petri nets
  w.r.t. to linear objective functions
  (e.g. constant-rate multi-mode systems of Alur *et al.* HSCC'12)

- games on continuous Petri nets
  (e.g. Minkowski games of Le Roux *et al.* STACS'17)

- more succinct encoding of
  continuous VASS reachability

Thank you !

Takk fyrir !