Relating paths in transition systems: the fall of the modal μ-calculus

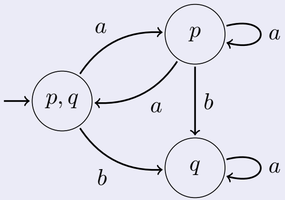
Cătălin Dima, Bastien Maubert and Sophie Pinchinat

Università degli Studi di Napoli Federico II

Journées ALGA, April 11-12, 2016

Logical approach to program verification

Programs:

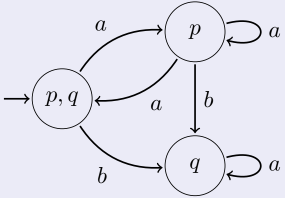


Properties:

- LTL, CTL, CTL*, L_{μ}...
- ATL, ATL*...

Logical approach to program verification

Programs:



Properties:

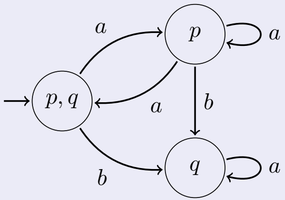
- LTL, CTL, CTL*, L_μ...
- ATL, ATL*...

What is a good logic?

- Complexity
- Expressivity

Logical approach to program verification

Programs:



Properties:

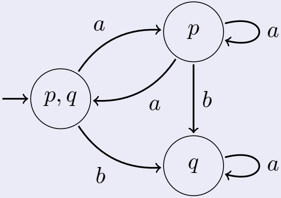
- LTL, CTL, CTL*, L$_\mu$. . .
- ATL, ATL*. . .

What is a good logic?

- Complexity
- Expressivity: compare to a "yardstick" logic.

Logical approach to program verification

Programs:



Properties:

- LTL, CTL, CTL*, L_μ...
- ATL, ATL*...

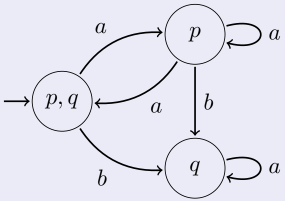
most $\not\leq$ FO

What is a good logic?

- Complexity
- Expressivity: compare to a "yardstick" logic.

Logical approach to program verification

Programs:



Properties:

- LTL, CTL, CTL*, L_μ...
- ATL, ATL*...

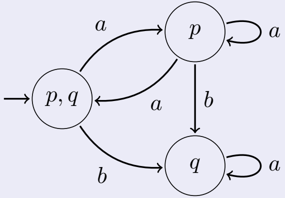
$\prec$ MSO

What is a good logic?

- Complexity
- Expressivity: compare to a "yardstick" logic.

Logical approach to program verification

Programs:



Properties:

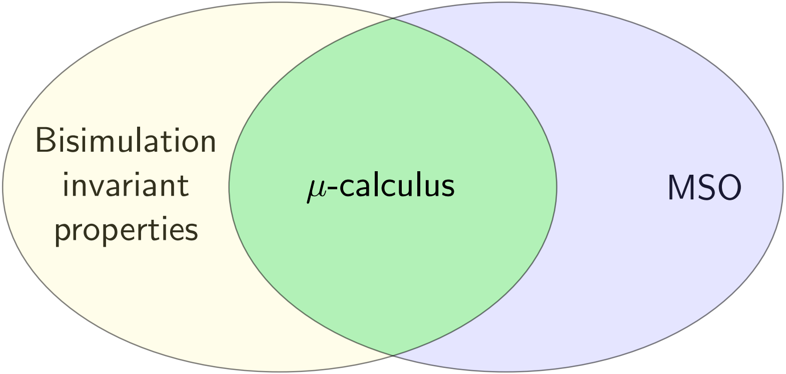
- LTL, CTL, CTL*, L$_\mu$...
- ATL, ATL*...

$\prec$ MSO, bisimulation invariant.

What is a good logic?

- Complexity
- Expressivity: compare to a "yardstick" logic.

Janin and Walukiewicz, 1996



Adding uncertainty

- Temporal epistemic logics: LTLK, CTLK, $\mathsf{L}_\mu\mathsf{K}$...
- Strategic logics with imperfect information: $\mathsf{ATL_i}$, ESL...

Common feature:

Indistinguishability relation on finite paths:

- Temporal epistemic logics: semantics of K
- Imperfect-information games: strategies must be *uniform*

In most works, this relation is fixed.

- memoryless, bounded memory, perfect recall
- synchronous, asynchronous...

Unlike the perfect information case, no unifying logic for now.
For instance: $\mathsf{ATL_i} \prec \mathsf{L}_\mu\mathsf{K}$?

Our contribution

Question

Is the μ-calculus still as central when uncertainty is considered?

Our contribution

Question

Is the μ-calculus still as central when uncertainty is considered?

Answer

It depends on the nature of the relation between paths. . .

Relating paths

Transition systems over $\mathcal{AP}$ and $\mathcal{A}ct$

$$\mathcal{S} = (S, s_\iota, \{a^{\mathcal{S}}\}_{a \in \mathcal{A}ct}, \{p^{\mathcal{S}}\}_{p \in \mathcal{AP}})$$

Relating paths

Transition systems over $\mathcal{AP}$ and $\mathcal{A}ct$

$\mathcal{S} = (S, s_\iota, \{a^{\mathcal{S}}\}_{a \in \mathcal{A}ct}, \{p^{\mathcal{S}}\}_{p \in \mathcal{AP}})$

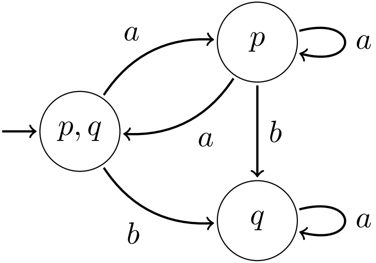
Fix a binary relation $\looparrowleft$ over $(\mathcal{A}ct \times 2^{\mathcal{AP}})^*$: *path relation*.

Relating paths

Transition systems over $\mathcal{AP}$ and $\mathcal{A}ct$

$\mathcal{S} = (S, s_\iota, \{a^{\mathcal{S}}\}_{a \in \mathcal{A}ct}, \{p^{\mathcal{S}}\}_{p \in \mathcal{AP}})$

Fix a binary relation $\leadsto$ over $(\mathcal{A}ct \times 2^{\mathcal{AP}})^*$: *path relation*.

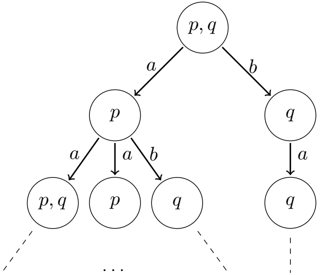


Relating paths

Transition systems over $\mathcal{AP}$ and $\mathcal{A}ct$

$$\mathcal{S} = (S, s_\iota, \{a^\mathcal{S}\}_{a\in\mathcal{A}ct}, \{p^\mathcal{S}\}_{p\in\mathcal{AP}})$$

Fix a binary relation $\rightharpoonup$ over $(\mathcal{A}ct \times 2^{\mathcal{AP}})^*$: *path relation*.

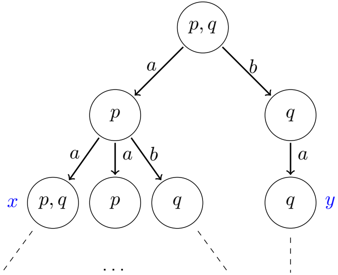


Relating paths

Transition systems over $\mathcal{AP}$ and $\mathcal{A}ct$

$$\mathcal{S} = (S, s_\iota, \{a^{\mathcal{S}}\}_{a \in \mathcal{A}ct}, \{p^{\mathcal{S}}\}_{p \in \mathcal{AP}})$$

Fix a binary relation $\rightsquigarrow$ over $(\mathcal{A}ct \times 2^{\mathcal{AP}})^*$: *path relation.*



$x \rightsquigarrow y$ if $w(x) \rightsquigarrow w(y)$

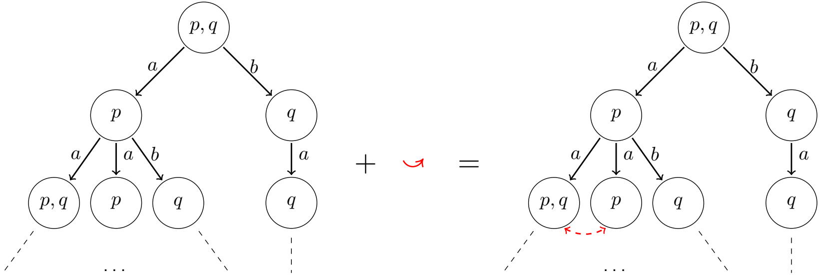
$$w(x) = \{p, q\}a\{p\}a\{p, q\}$$

Relating paths

Transition systems over $\mathcal{AP}$ and $\mathcal{A}ct$

$\mathcal{S} = (S, s_\iota, \{a^{\mathcal{S}}\}_{a \in \mathcal{A}ct}, \{p^{\mathcal{S}}\}_{p \in \mathcal{AP}})$

Fix a binary relation $\curvearrowright$ over $(\mathcal{A}ct \times 2^{\mathcal{AP}})^*$: *path relation*.



Example: a synchronous perfect recall agent, who only observes p

Extending the framework

MSO

$$\psi ::= \quad p(X) \mid r(X) \mid a(X,Y) \mid X \subseteq Y \mid \neg\psi \mid \psi \vee \psi \mid \exists X.\psi(X)$$

where $p \in \mathcal{AP}$ and $a \in \mathcal{A}ct$.

L_μ

$$\varphi ::= X \mid p \mid \neg\varphi \mid \varphi \vee \varphi \mid \langle a \rangle\varphi \mid \mu X.\varphi(X)$$

where $p \in \mathcal{AP}$ and $a \in \mathcal{A}ct$.

Extending the framework

MSO$^{\curvearrowright}$: MSO with path relation

$$\psi ::= \quad p(X) \mid r(X) \mid a(X,Y) \mid X \subseteq Y \mid \neg\psi \mid \psi \vee \psi \mid \exists X.\psi(X) \mid \curvearrowright(X,Y)$$

where $p \in \mathcal{AP}$ and $a \in \mathcal{A}ct$.

$\mathrm{L}_{\mu}^{\curvearrowright}$: Jumping μ-calculus

$$\varphi ::= X \mid p \mid \neg\varphi \mid \varphi \vee \varphi \mid \langle a \rangle\varphi \mid \mu X.\varphi(X) \mid \langle \curvearrowright \rangle\varphi$$

where $p \in \mathcal{AP}$ and $a \in \mathcal{A}ct$.

Semantics

MSO$^{\curvearrowright}$

$t, V \models^{\curvearrowright} p(X)$ if for all $x \in V(X), p \in \ell(x)$

$t, V \models^{\curvearrowright} r(X)$ if $V(X) = \{\epsilon\}$

$t, V \models^{\curvearrowright} a(X, Y)$ if $V(X) = \{x\}, V(Y) = \{y\},$ and $x a^t y$

$t, V \models^{\curvearrowright} X \subseteq Y$ if $V(X) \subseteq V(Y)$

$t, V \models^{\curvearrowright} \neg\psi$ if $t, V \not\models^{\curvearrowright} \psi$

$t, V \models^{\curvearrowright} \psi \vee \psi'$ if $t, V \models^{\curvearrowright} \psi$ or $t, V \models^{\curvearrowright} \psi'$

$t, V \models^{\curvearrowright} \exists X.\psi(X)$ if there is $T \subseteq t$ s.t. $t, V[T/X] \models^{\curvearrowright} \psi(X)$

$t, V \models^{\curvearrowright} \curvearrowright(X, Y)$ if $V(X) = \{x\}, V(Y) = \{y\},$ and $x \curvearrowright y$

Semantics

$\mathsf{L}_{\mu}^{\curvearrowleft}$

$$[\![X]\!]^{t,V}_{\curvearrowleft} = V(X)$$
$$[\![p]\!]^{t,V}_{\curvearrowleft} = \{x \in t \mid p \in \ell^x\}$$
$$[\![\neg\varphi]\!]^{t,V}_{\curvearrowleft} = t \setminus [\![\varphi]\!]^{t,V}_{\curvearrowleft}$$
$$[\![\varphi \vee \varphi']\!]^{t,V}_{\curvearrowleft} = [\![\varphi]\!]^{t,V}_{\curvearrowleft} \cup [\![\varphi']\!]^{t,V}_{\curvearrowleft}$$
$$[\![\langle a \rangle\varphi]\!]^{t,V}_{\curvearrowleft} = \{x \in t \mid \text{ there exists } y \in [\![\varphi]\!]^{t,V}_{\curvearrowleft} \text{ such that } x a^t y\}$$
$$[\![\mu X.\varphi(X)]\!]^{t,V}_{\curvearrowleft} = \bigcap\{T \subseteq t \mid [\![\varphi(X)]\!]^{t,V[T/X]}_{\curvearrowleft} \subseteq T\}$$
$$[\![\langle \curvearrowleft \rangle\varphi]\!]^{t,V}_{\curvearrowleft} = \{x \in t \mid \text{ there exists } y \in [\![\varphi]\!]^{t,V}_{\curvearrowleft} \text{ such that } x \curvearrowleft y\}$$

Precise question

Now:

Is $L_{\mu}^{\smile}$ the bisimulation invariant fragment of $MSO^{\smile}$?

Precise question

Now:

Is $\mathsf{L}_\mu^{\smile}$ the bisimulation invariant fragment of $\mathsf{MSO}^{\smile}$?

Proposition

$\mathsf{L}_\mu^{\smile} \prec \mathsf{MSO}^{\smile}$, and $\mathsf{L}_\mu^{\smile}$ is invariant under bisimulation.

Classes of relations

Regular relations

A relation is regular iff it is recognized by a synchronous transducer.

Recognizable relations

A relation is recognizable iff it is recognized by a word automaton:

$$\{u\#v \mid u \rightsquigarrow v\} \text{ is a regular language}$$

Recognizable $\subsetneq$ Regular

Answer

Theorem

For every recognizable relation $\curvearrowright$, $L_\mu^{\curvearrowright} \equiv \mathsf{MSO}^{\curvearrowright}_{\mathsf{bisim}}$.

Answer

Theorem

For every recognizable relation $\rightarrowtail$, $L_\mu^{\rightarrowtail} \equiv MSO^{\rightarrowtail}_{\text{bisim}}$.

Recognizable relations are MSO definable:

$\rightarrow MSO^{\rightarrowtail}$ collapses to MSO

$L_\mu^{\rightarrowtail} \subset MSO^{\rightarrowtail} = MSO$, and
$L_\mu^{\rightarrowtail}$ is invariant under bisimulation

$\rightarrow L_\mu^{\rightarrowtail}$ collapses to L_μ.

Answer

Theorem

For every recognizable relation $\curvearrowright$, $L_\mu^{\curvearrowright} \equiv MSO_{\text{bisim}}^{\curvearrowright}$.

Theorem

There are regular relations $\curvearrowright$ for which $L_\mu^{\curvearrowright} \not\equiv MSO_{\text{bisim}}^{\curvearrowright}$.

$\curvearrowright$: synchronous perfect recall / equal level.

Property: existence of a winning strategy in two-player reachability games with imperfect information.

- invariant under bisimulation
- expressible in $MSO^{\curvearrowright}$
- not expressible in $L_\mu^{\curvearrowright}$.

Answer

Theorem

For every recognizable relation $\smile$, $\mathrm{L}_\mu^{\smile} \equiv \mathrm{MSO}^{\smile}_{\mathrm{bisim}}$.

Theorem

There are regular relations $\smile$ for which $\mathrm{L}_\mu^{\smile} \not\equiv \mathrm{MSO}^{\smile}_{\mathrm{bisim}}$.

$\smile$: synchronous perfect recall / equal level.

Property: existence of a winning strategy in two-player reachability games with imperfect information.

- invariant under bisimulation ✓ [Berwanger, Kaiser, 2010]
- expressible in $\mathrm{MSO}^{\smile}$
- not expressible in $\mathrm{L}_\mu^{\smile}$.

Answer

Theorem

For every recognizable relation $\curvearrowright$, $L_\mu^{\curvearrowright} \equiv MSO^{\curvearrowright}_{\text{bisim}}$.

Theorem

There are regular relations $\curvearrowright$ for which $L_\mu^{\curvearrowright} \not\equiv MSO^{\curvearrowright}_{\text{bisim}}$.

$\curvearrowright$: synchronous perfect recall / equal level.

Property: existence of a winning strategy in two-player reachability games with imperfect information.

- invariant under bisimulation ✓ [Berwanger, Kaiser, 2010]
- expressible in $MSO^{\curvearrowright}$ ✓
- not expressible in $L_\mu^{\curvearrowright}$.

Answer

Theorem

For every recognizable relation $\looparrowright$, $\mathrm{L}_\mu^{\looparrowright} \equiv \mathrm{MSO}^{\looparrowright}_{\mathrm{bisim}}$.

Theorem

There are regular relations $\looparrowright$ for which $\mathrm{L}_\mu^{\looparrowright} \not\equiv \mathrm{MSO}^{\looparrowright}_{\mathrm{bisim}}$.

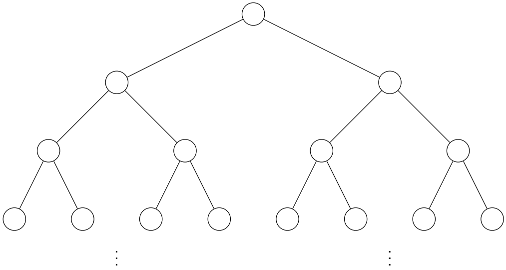
$\looparrowright$: synchronous perfect recall / equal level.

Property: existence of a winning strategy in two-player reachability games with imperfect information.

- invariant under bisimulation ✓ [Berwanger, Kaiser, 2010]
- expressible in $\mathrm{MSO}^{\looparrowright}$ ✓
- not expressible in $\mathrm{L}_\mu^{\looparrowright}$.

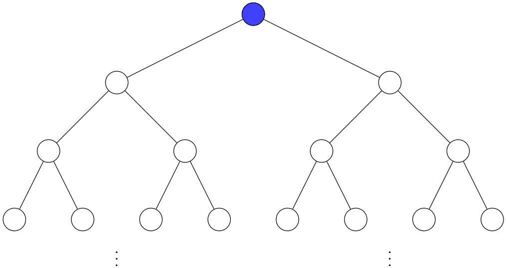
Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$



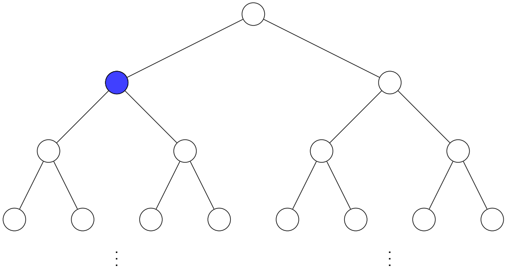
Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$



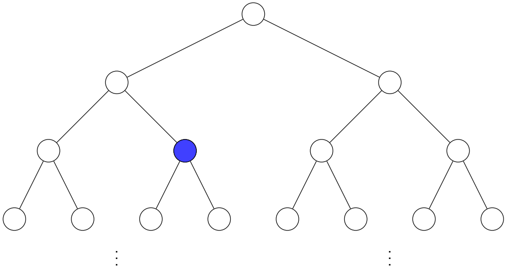
Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$



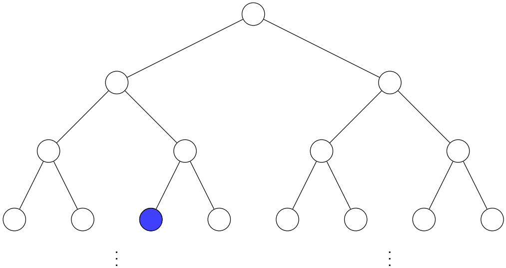
Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: ↓



Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: ↓

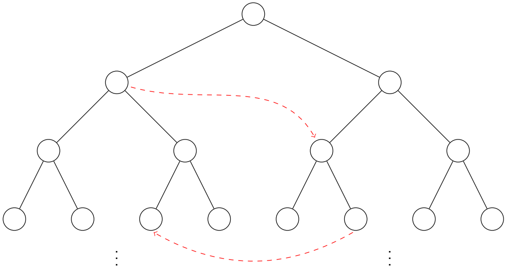


Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$

Path relation $\hookrightarrow$

Jumping tree automata: $\downarrow + \hookrightarrow$

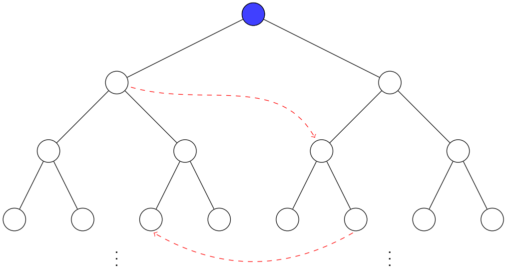


Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$

Path relation $\hookrightarrow$

Jumping tree automata: $\downarrow + \hookrightarrow$

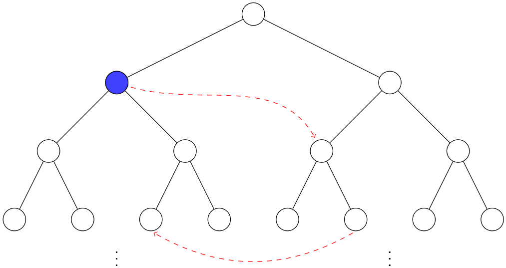


Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$

Path relation $\textcolor{red}{\hookrightarrow}$

Jumping tree automata: $\downarrow + \textcolor{red}{\hookrightarrow}$

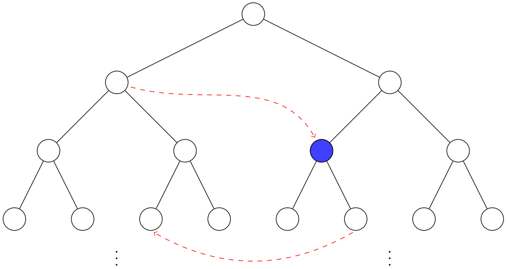


Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$

Path relation $\hookrightarrow$

Jumping tree automata: $\downarrow + \hookrightarrow$

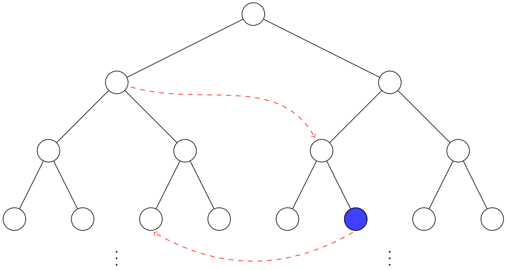


Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$

Path relation $\hookrightarrow$

Jumping tree automata: $\downarrow + \hookrightarrow$

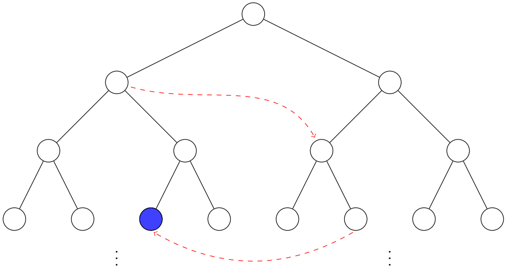


Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$

Path relation $\curvearrowright$

Jumping tree automata: $\downarrow + \curvearrowright$

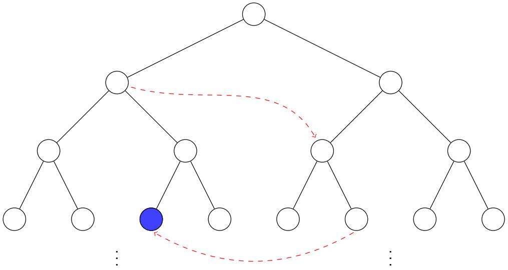


Jumping tree automata (JTA) [M., Pinchinat, 2013]

Alternating tree automata: $\downarrow$

Path relation $\curvearrowright$

Jumping tree automata: $\downarrow + \curvearrowright$

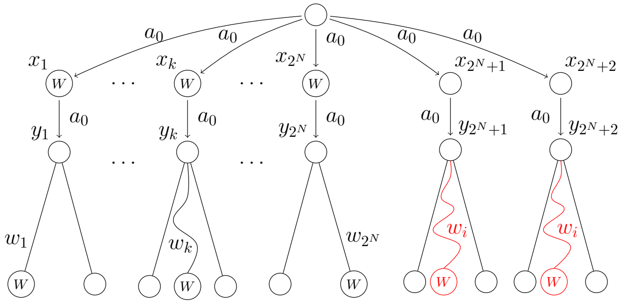


Proposition

$$\mathsf{JTA} \equiv \mathsf{L}_{\mu}^{\curvearrowright}$$

Outline of the proof (1/4)

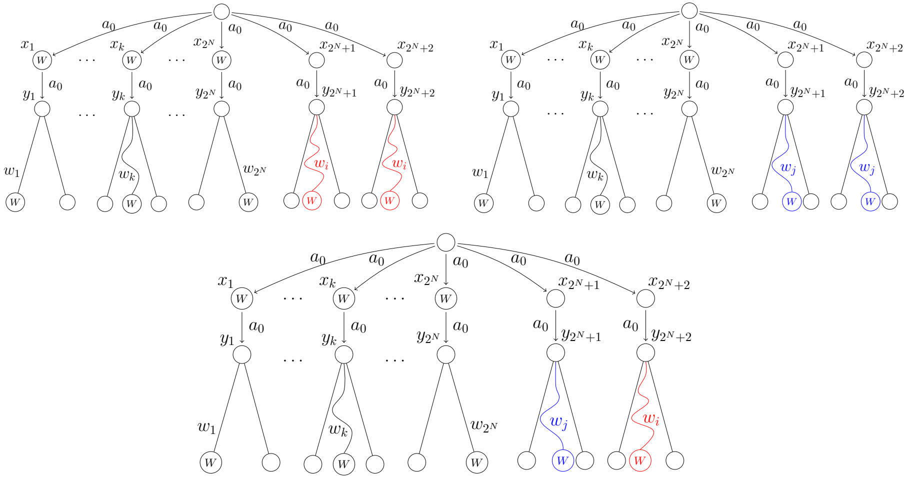
- Assume that $\varphi \in \mathsf{L}_\mu^{\circlearrowleft}$ expresses what we want.
- There is a JTA $\mathcal{A}_\varphi$ that accepts (unfoldings of) arenas where Eve wins. Let N be the number of states in $\mathcal{A}_\varphi$ plus one.
- We build 2^N arenas, $t_1, \ldots, t_{2^N}$, where Eve wins (and is blind). Winning strategy in t_i : $a_0 \cdot a_0 \cdot w_i$



$w_i = i - 1$ in binary

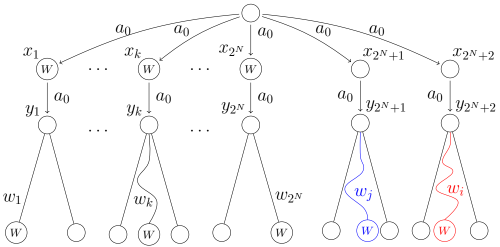
Outline of the proof (2/4)

Purpose : combine two arenas t_i and t_j into an arena t_0 where Eve does not win, but that is accepted by $\mathcal{A}_\varphi$.



Outline of the proof (3/4)

- $\mathcal{G}_i := \mathcal{G}(\mathcal{A}_\varphi, t_i)$: acceptance game of $\mathcal{A}_\varphi$ on t_i
  - perfect-information parity game between Verifier and Refuter
  - positions : $(x, q) \in t_i \times \mathcal{A}_\varphi$
- For each i, Verifier has a **positional** winning strategy σ_i in $\mathcal{G}_i$.
- $\text{visit}_{\sigma_i}(x) := \{q \in \mathcal{A}_\varphi \mid \exists \pi \in \text{Out}(\mathcal{G}_i, \sigma_i) \text{ s.t } \pi \text{ goes through } (x, q)\}$
- Pigeon hole: $\exists\, i \neq j$ s.t. $\text{visit}_{\sigma_i}(y_{2^N+1}) = \text{visit}_{\sigma_j}(y_{2^N+1})$.



Outline of the proof (4/4)

How does Verifier accept t_0?

At first : follow σ_i. When a position (y_k, q) is reached:

If $k \neq 2^N + 1$:

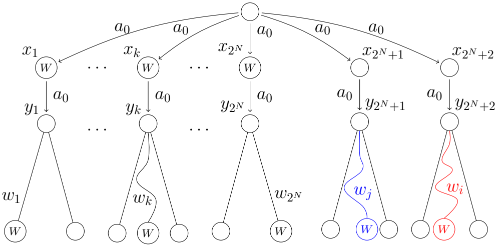
- $\mathcal{G}_i, (y_k, q)$ is winning for Verifier,
- $\mathcal{G}_i, (y_k, q) \Leftrightarrow \mathcal{G}_0, (y_k, q)$, so

$\mathcal{G}_0, (y_k, q)$ is winning for Verifier

If $k = 2^N + 1$:

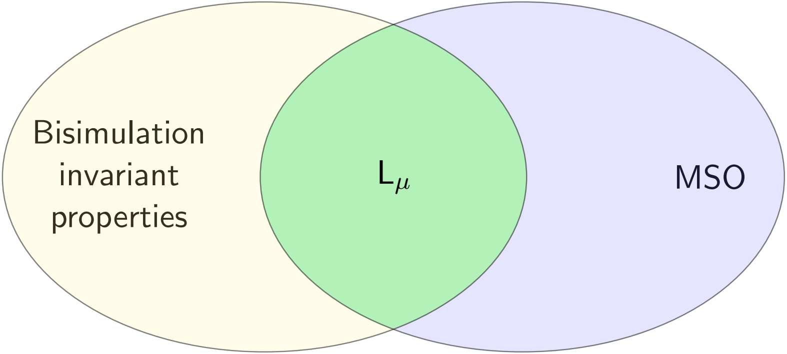
- $q \in \text{visit}_{\sigma_i}(y_{2^N+1}) = \text{visit}_{\sigma_j}(y_{2^N+1})$,
- $\mathcal{G}_j, (y_{2^N+1}, q)$ is winning for Verifier,
- $\mathcal{G}_j, (y_{2^N+1}, q) \Leftrightarrow \mathcal{G}_0, (y_{2^N+1}, q)$, so

$\mathcal{G}_0, (y_{2^N+1}, q)$ is winning for Verifier



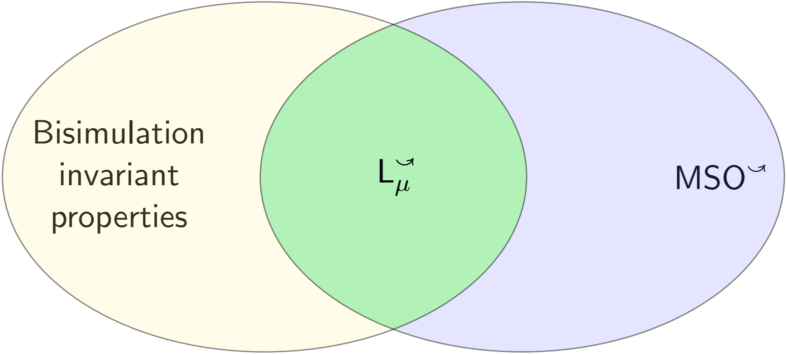
Conclusion

Janin and Walukiewcz:



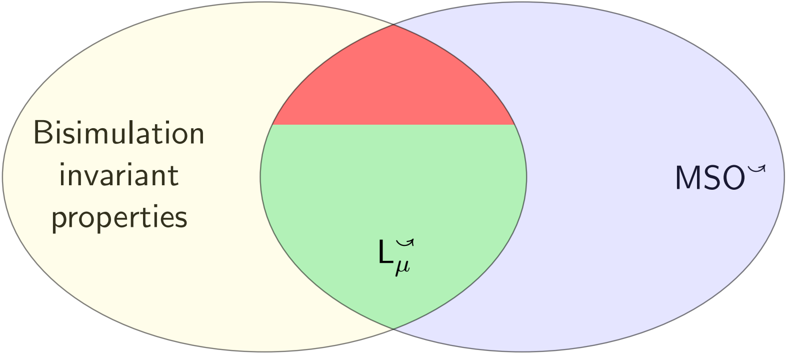
Conclusion

With recognizable relations over paths:



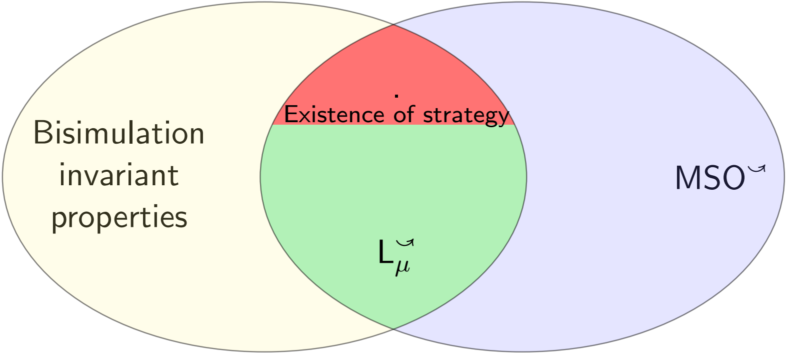
Conclusion

For some regular relations over paths:



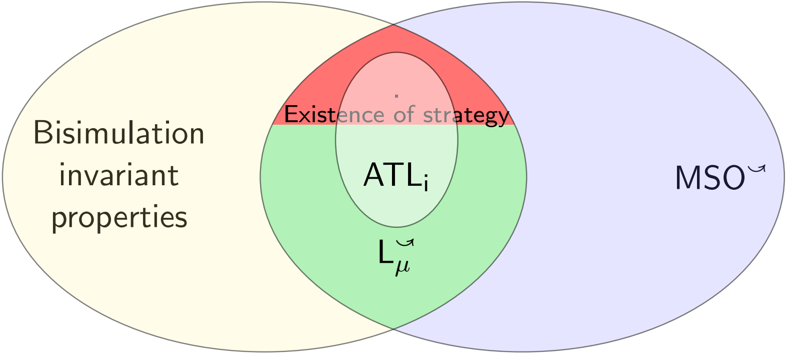
Conclusion

For some regular relations over paths:



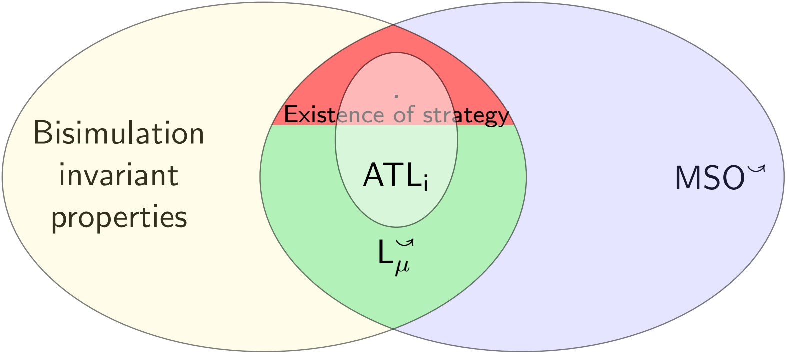
Conclusion

For some regular relations over paths:



Conclusion

For some regular relations over paths:



Thank you!