Lattice-Theoretic Progress Measures and Coalgebraic Model Checking

Ichiro Hasuo Shunsuke Shimizu
University of Tokyo (JP)

Corina Cirstea
University of Southampton (UK)

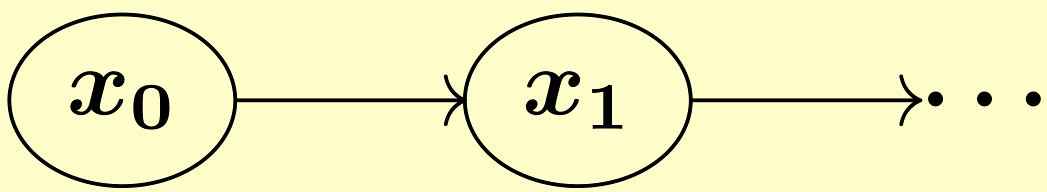
東京大学
THE UNIVERSITY OF TOKYO

UNIVERSITY OF Southampton

Contributions

* **Lattice-theoretic progress measure**
* **Coalgebraic model checking** as application

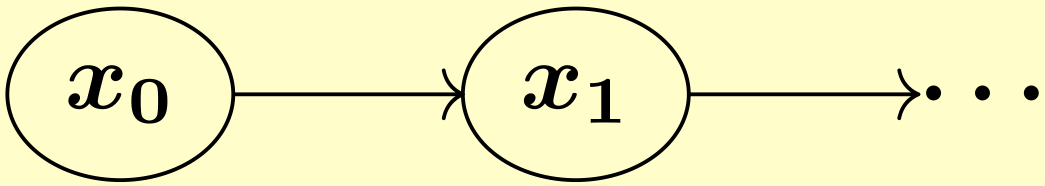
Invariant vs. Ranking Function



A linear Kripke structure:
$\mathsf{succ}\colon X \to X, \quad [\![p]\!] \subseteq X$

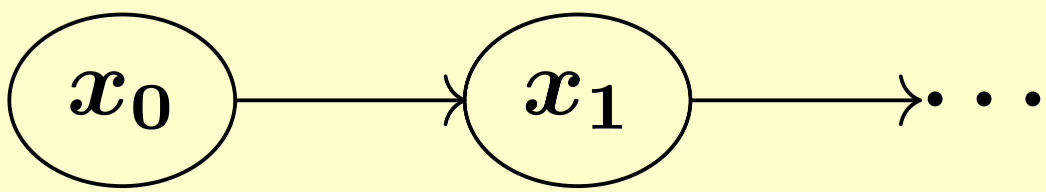
- **G**p (everywhere p) is a gfp $\quad \nu u.\, p \wedge \mathbf{X} u$
  - the greatest solution of $u = p \wedge \mathbf{X}\, u$
- **F**p (eventually p) is an lfp $\quad \mu u.\, p \vee \mathbf{X} u$
  - the least solution of $u = p \vee \mathbf{X}\, u$

Invariant vs. Ranking Function



A linear Kripke structure:
$\mathsf{succ} \colon X \to X, \quad [\![p]\!] \subseteq X$

Invariant vs. Ranking Function

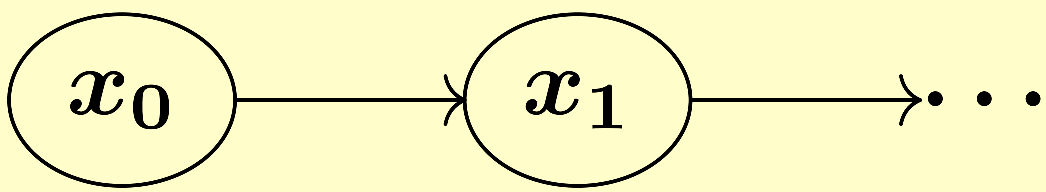


A linear Kripke structure:
$\mathsf{succ}\colon X \to X, \quad [\![p]\!] \subseteq X$

<u>Lem.</u> (witnessing $\mathbf{G}\,p = \nu u.\,(p \wedge \mathbf{X}\,u)$)

$$\frac{I \subseteq [\![p]\!] \qquad x \in I \;\Rightarrow\; \mathsf{succ}(x) \in I}{I \subseteq [\![\mathbf{G}\,p]\!]}$$

Invariant vs. Ranking Function



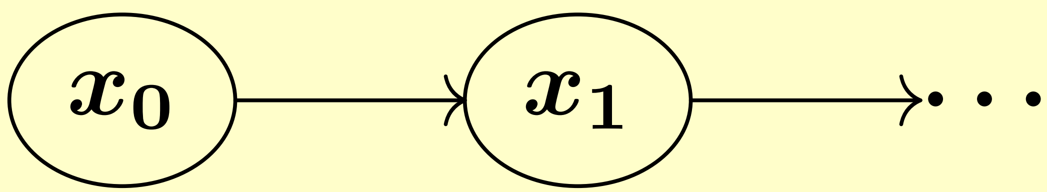
A linear Kripke structure:
$\mathsf{succ}\colon X \to X, \quad [\![p]\!] \subseteq X$

<u>Lem.</u> (witnessing $\mathsf{G}\,p = \nu u.\,(p \wedge \mathsf{X}\,u)$)

$$\frac{I \subseteq [\![p]\!] \qquad x \in I \;\Rightarrow\; \mathsf{succ}(x) \in I}{I \subseteq [\![\mathsf{G}\,p]\!]}$$

invariant

Invariant vs. Ranking Function



A linear Kripke structure:
$\mathsf{succ}\colon X \to X, \quad [\![p]\!] \subseteq X$

Lem. (witnessing $\mathsf{G}\,p = \nu u.\,(p \wedge \mathsf{X}\,u)$)

$$\frac{I \subseteq [\![p]\!] \qquad x \in I \;\Rightarrow\; \mathsf{succ}(x) \in I}{I \subseteq [\![\mathsf{G}\,p]\!]}$$

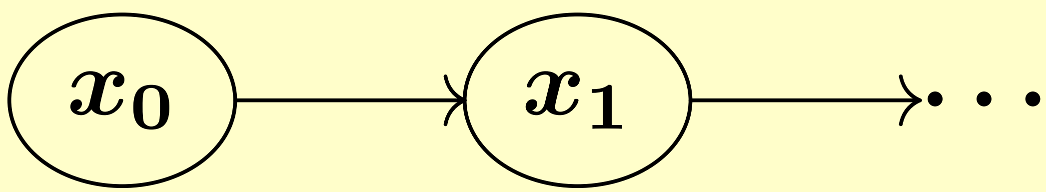
invariant

Lem. (witnessing $\mathsf{F}\,p = \mu u.\,(p \vee \mathsf{X}\,u)$)
Let $\mathbf{rk}\colon X \to \omega \amalg \{\spadesuit\}$ be such that

$$\mathbf{rk}(x) = n \;\wedge\; x \notin [\![p]\!] \implies \mathbf{rk}(\mathsf{succ}(x)) \leq n - 1\;.$$

Then $\mathbf{rk}(x) \neq \spadesuit$ implies $x \in [\![\mathsf{F}\,p]\!]$.

Invariant vs. Ranking Function



A linear Kripke structure:
$\mathsf{succ}\colon X \to X, \quad [\![p]\!] \subseteq X$

Lem. (witnessing $\mathbf{G}\,p = \nu u.\,(p \land \mathbf{X}\,u)$)

$$\frac{I \subseteq [\![p]\!] \qquad x \in I \;\Rightarrow\; \mathsf{succ}(x) \in I}{I \subseteq [\![\mathbf{G}\,p]\!]}$$

invariant

Lem. (witnessing $\mathbf{F}\,p = \mu u.\,(p \lor \mathbf{X}\,u)$)
Let $\mathbf{rk}\colon X \to \omega \amalg \{\spadesuit\}$ be such that

$$\mathbf{rk}(x) = n \;\land\; x \notin [\![p]\!] \implies \mathbf{rk}(\mathsf{succ}(x)) \leq n - 1\;.$$

Then $\mathbf{rk}(x) \neq \spadesuit$ implies $x \in [\![\mathbf{F}\,p]\!]$.

ranking func.

Lem. (witnessing $\mathsf{G}\,p = \nu u.\,(p \wedge \mathsf{X}\,u)$)

$$\frac{I \subseteq [\![p]\!] \qquad x \in I \;\Rightarrow\; \mathsf{succ}(x) \in I}{I \subseteq [\![\mathsf{G}\,p]\!]}$$

Lem. (witnessing $\mathsf{F}\,p = \mu u.\,(p \vee \mathsf{X}\,u)$)
Let $\mathbf{rk}\colon X \to \omega \amalg \{\spadesuit\}$ be such that

$$\mathbf{rk}(x) = n \;\wedge\; x \notin [\![p]\!] \implies \mathbf{rk}(\mathsf{succ}(x)) \leq n-1 \;.$$

Then $\mathbf{rk}(x) \neq \spadesuit$ implies $x \in [\![\mathsf{F}\,p]\!]$.

- How come the difference?
  ➜ Let us take a **foundational** view...

Lattice-Theoretic Foundation

L: complete lattice, $\quad f : L \to L$ monotone

Thm. (Knaster-Tarski)

- $\mu f = \min\{l \in L \mid f(l) \sqsubseteq l\}$
- $\nu f = \max\{l \in L \mid l \sqsubseteq f(l)\}$

Thm. (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^{\omega}(\bot) \sqsubseteq \cdots$
stabilizes, and converges to μf

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^{\omega}(\top) \sqsupseteq \cdots$
stabilizes, and converges to νf

Lattice-Theoretic Foundation

L: complete lattice, $\quad f : L \to L$ monotone

Thm. (Knaster-Tarski)

- $\mu f = \min\{l \in L \mid f(l) \sqsubseteq l\}$

$$\Longrightarrow \quad \frac{f(l) \sqsubseteq l}{\mu f \sqsubseteq l}$$

- $\nu f = \max\{l \in L \mid l \sqsubseteq f(l)\}$

$$\Longrightarrow \quad \frac{l \sqsubseteq f(l)}{l \sqsubseteq \nu f}$$

Thm. (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^{\omega}(\bot) \sqsubseteq \cdots$
stabilizes, and converges to μf

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^{\omega}(\top) \sqsupseteq \cdots$
stabilizes, and converges to νf

Lattice-Theoretic Foundation

L: complete lattice, $f : L \to L$ monotone

Thm. (Knaster-Tarski)

- $\mu f = \min\{l \in L \mid f(l) \sqsubseteq l\}$

$$\Longrightarrow \quad \frac{f(l) \sqsubseteq l}{\mu f \sqsubseteq l}$$

- $\nu f = \max\{l \in L \mid l \sqsubseteq f(l)\}$

$$\Longrightarrow \quad \frac{l \sqsubseteq f(l)}{l \sqsubseteq \nu f}$$

Thm. (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^{\omega}(\bot) \sqsubseteq \cdots$
stabilizes, and converges to μf

$$\Longrightarrow \quad f^{\alpha}(\bot) \sqsubseteq \mu f \quad (\forall \alpha \in \mathbf{Ord})$$

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^{\omega}(\top) \sqsupseteq \cdots$
stabilizes, and converges to νf

$$\Longrightarrow \quad \nu f \sqsubseteq f^{\alpha}(\top) \quad (\forall \alpha \in \mathbf{Ord})$$

Lattice-Theoretic Foundation

L: complete lattice, $f : L \to L$ monotone

Thm. (Knaster-Tarski)

- $\mu f = \min\{l \in L \mid f(l) \sqsubseteq l\}$

$$\Longrightarrow \quad \frac{f(l) \sqsubseteq l}{\mu f \sqsubseteq l}$$

- $\nu f = \max\{l \in L \mid l \sqsubseteq f(l)\}$

$$\Longrightarrow \quad \frac{l \sqsubseteq f(l)}{l \sqsubseteq \nu f}$$

Thm. (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^{\omega}(\bot) \sqsubseteq \cdots$
stabilizes, and converges to μf

$$\Longrightarrow \quad f^{\alpha}(\bot) \sqsubseteq \mu f \quad (\forall \alpha \in \mathbf{Ord})$$

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^{\omega}(\top) \sqsupseteq \cdots$
stabilizes, and converges to νf

$$\Longrightarrow \quad \nu f \sqsubseteq f^{\alpha}(\top) \quad (\forall \alpha \in \mathbf{Ord})$$

Lattice-Theoretic Foundation

L: complete lattice, $f : L \to L$ monotone

Thm. (Knaster-Tarski)

- $\mu f = \min\{l \in L \mid f(l) \sqsubseteq l\}$

$$\Longrightarrow \quad \frac{f(l) \sqsubseteq l}{\mu f \sqsubseteq l}$$

- $\nu f = \max\{l \in L \mid l \sqsubseteq f(l)\}$

$$\Longrightarrow \quad \frac{l \sqsubseteq f(l)}{l \sqsubseteq \nu f}$$

Thm. (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^{\omega}(\bot) \sqsubseteq \cdots$
stabilizes, and converges to μf

$$\Longrightarrow \quad f^{\alpha}(\bot) \sqsubseteq \mu f \quad (\forall \alpha \in \mathbf{Ord})$$

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^{\omega}(\top) \sqsupseteq \cdots$
stabilizes, and converges to νf

$$\Longrightarrow \quad \nu f \sqsubseteq f^{\alpha}(\top) \quad (\forall \alpha \in \mathbf{Ord})$$

Sound approx. from below

The Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions

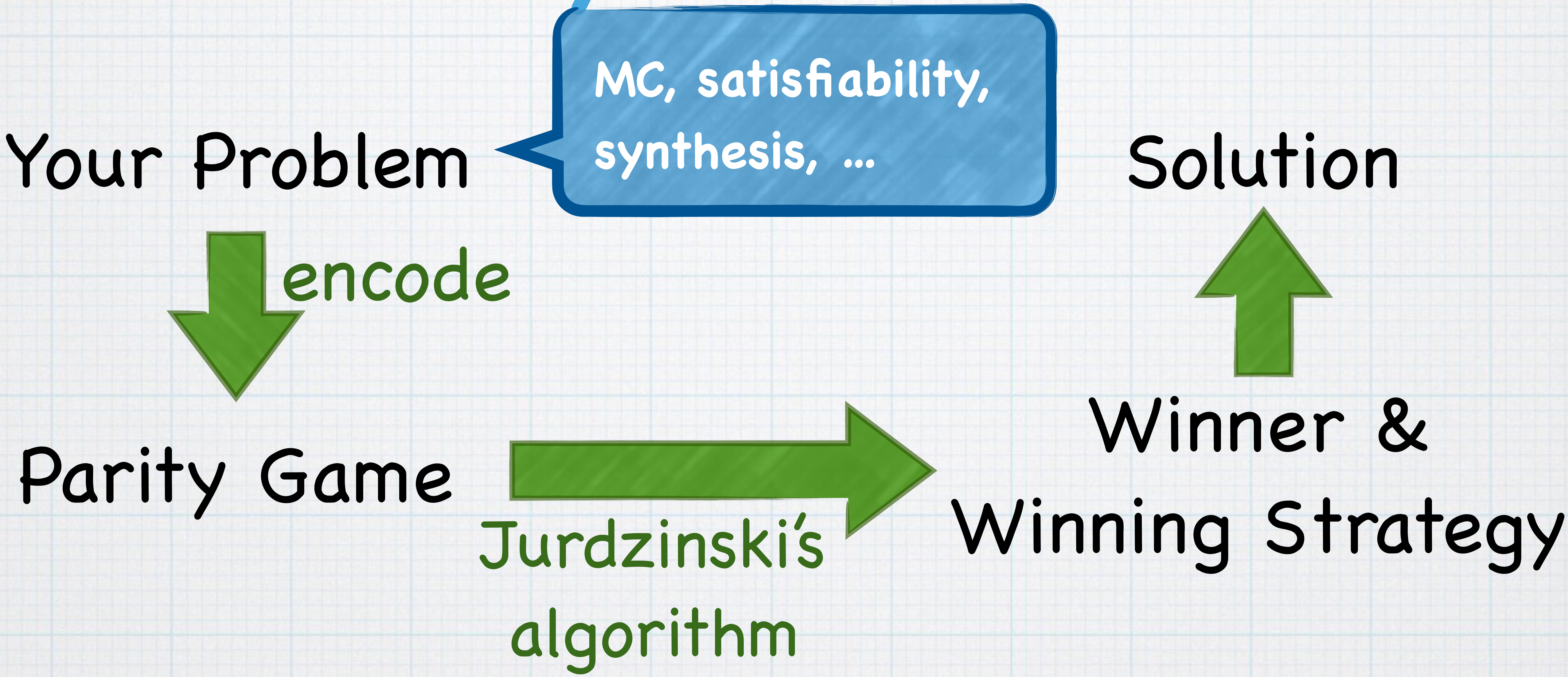
The Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	

The Table

properties	witnessed by…
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**winning strategies for a parity game** (if finitary)

The Parity-Game Workflow



The Parity-Game Workflow

Your Problem

MC, satisfiability, synthesis, …

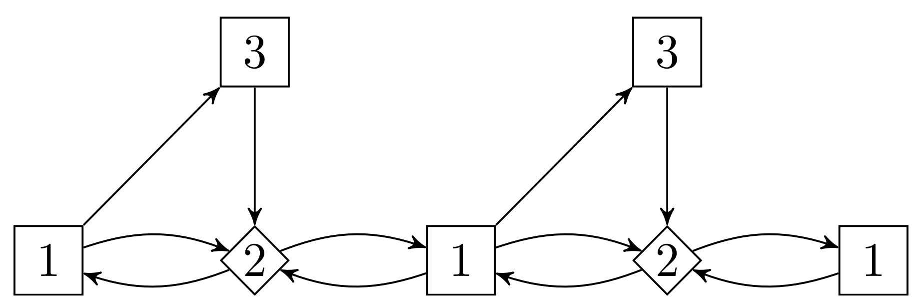
encode

Parity Game

Jurdzinski's algorithm

Winner & Winning Strategy

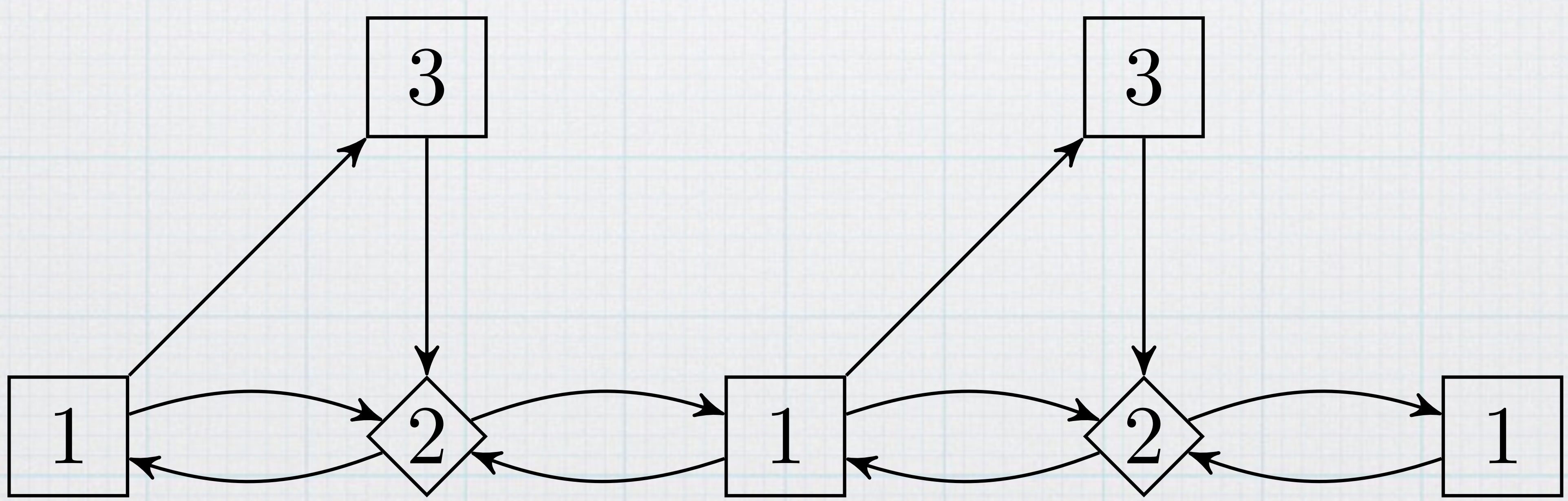
Solution



- In parity games:
  - alt. branching ($\forall$ vs $\exists$, $\wedge$ vs $\vee$)
  - parity acceptance cond.
    ➜ alt. betw. μ and ν

Jurdzinski's Progress Measure for Parity Games: Intuitions

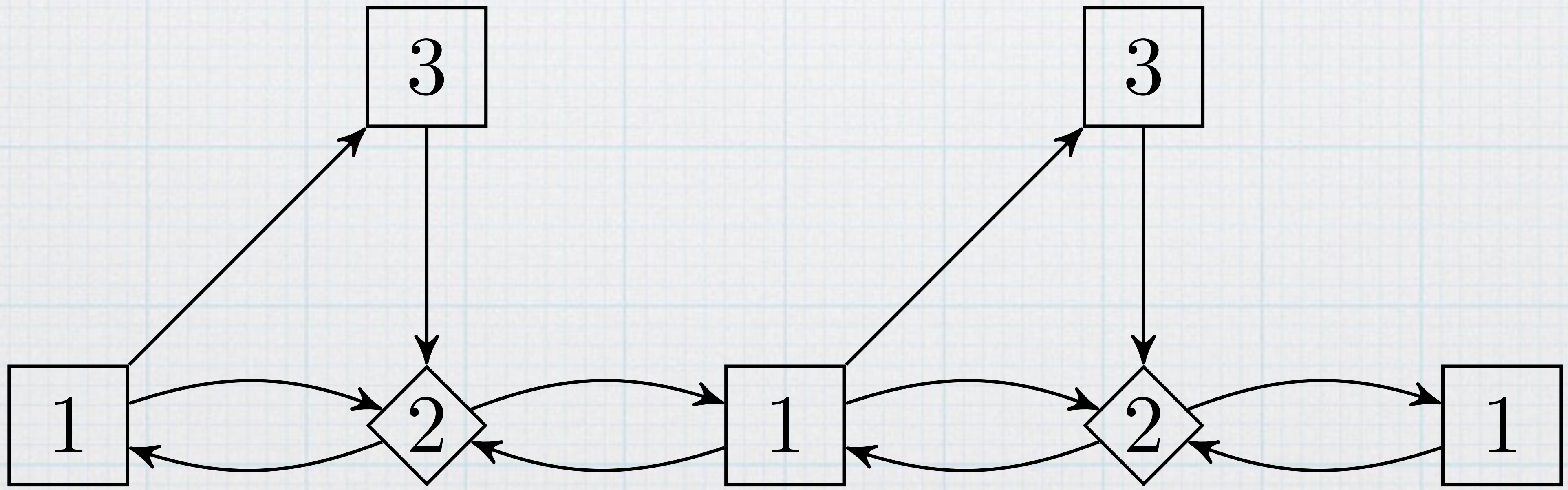
◇: your position
□: opponent's
goal: "visit bigger even"



Jurdzinski's Progress Measure for Parity Games: Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"

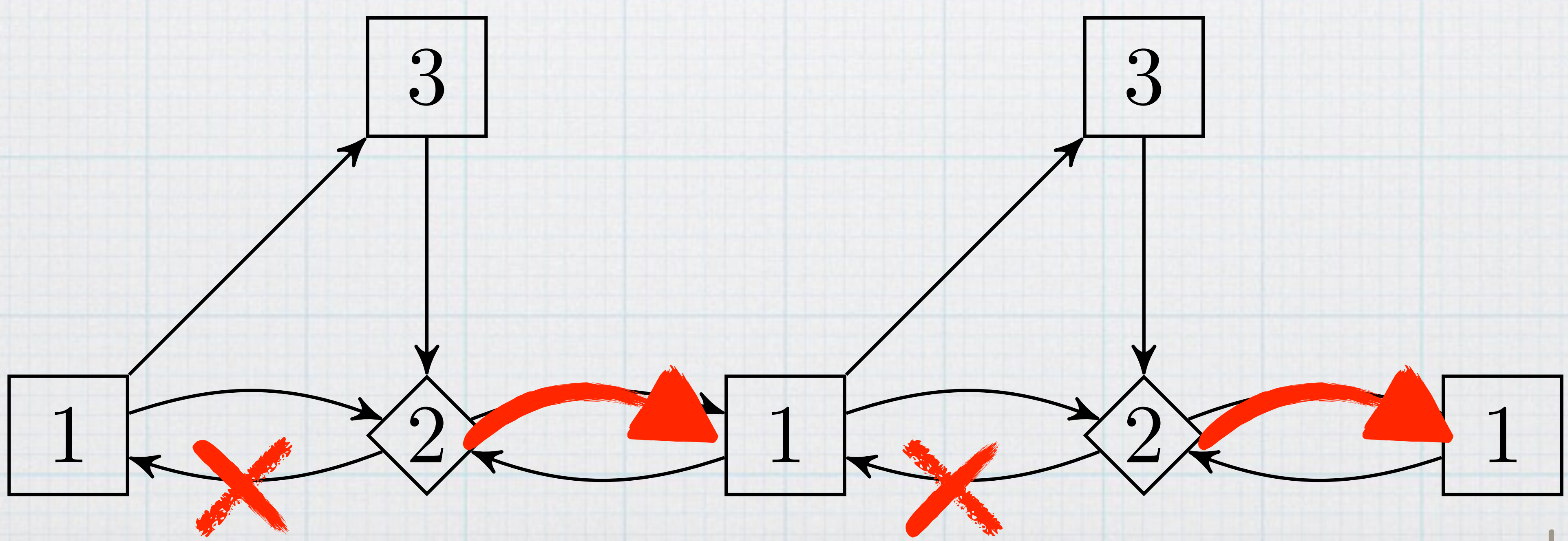
YOU WIN!



Jurdzinski's Progress Measure for Parity Games: Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"

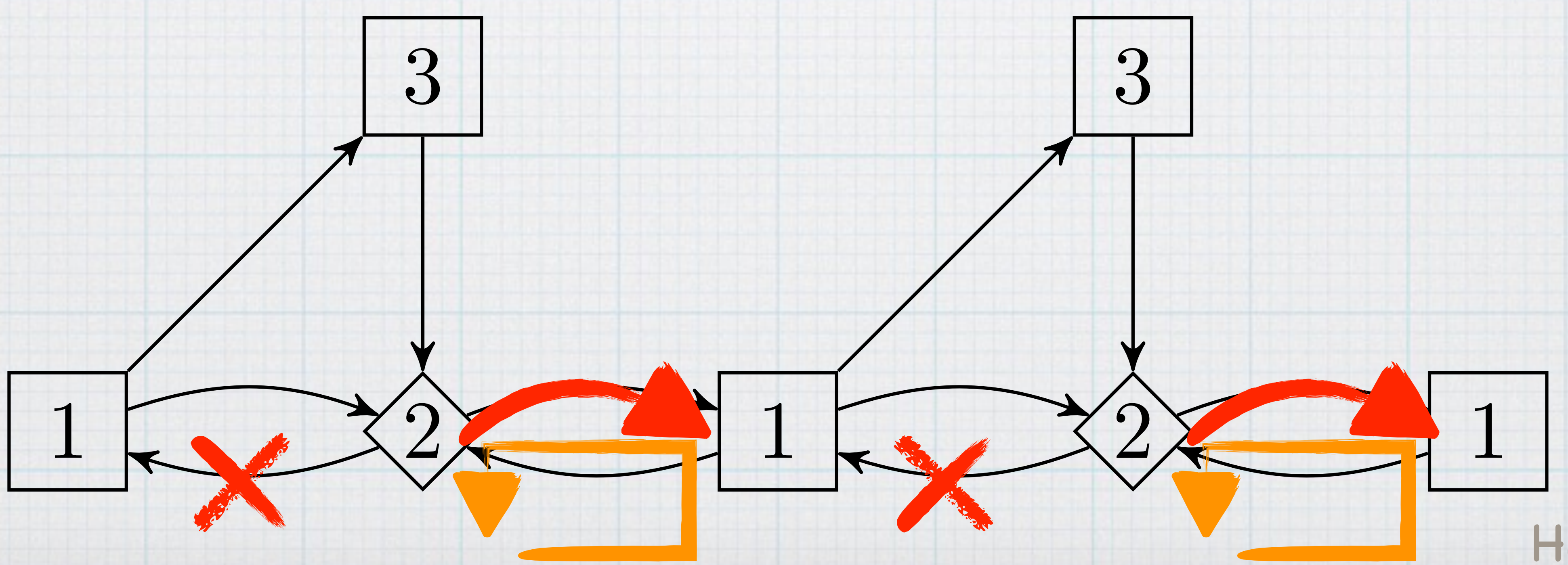
YOU WIN!



Jurdzinski's Progress Measure for Parity Games: Intuitions

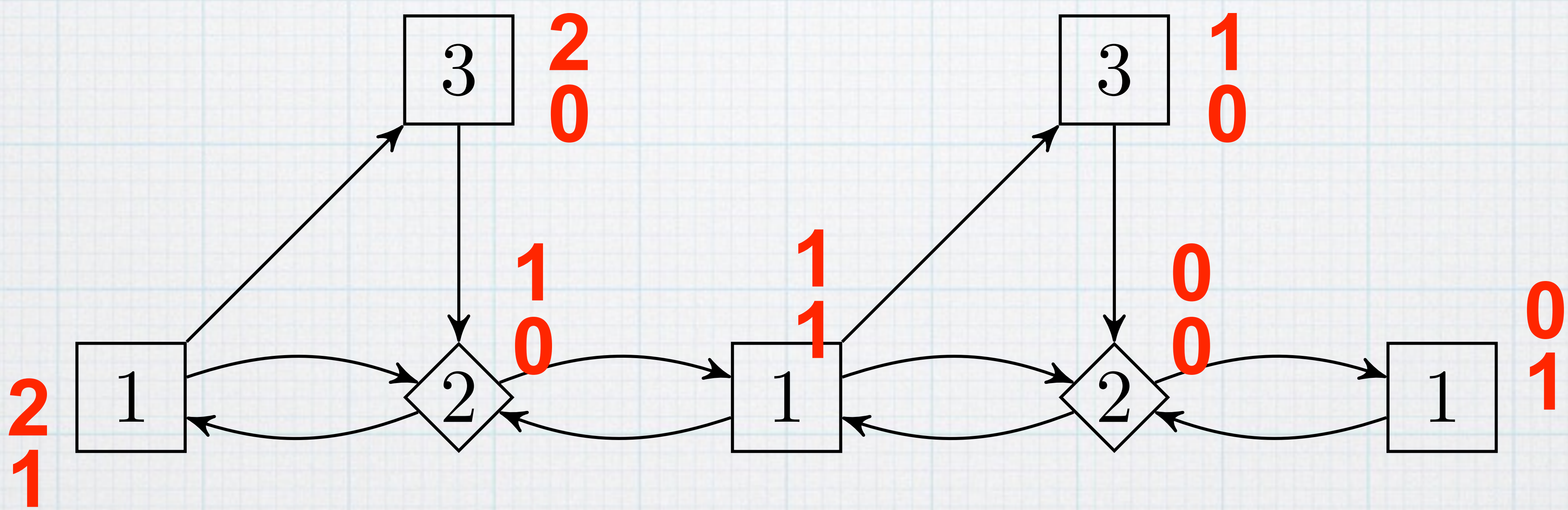
◇: your position
□: opponent's
goal: "visit bigger even"

YOU WIN!



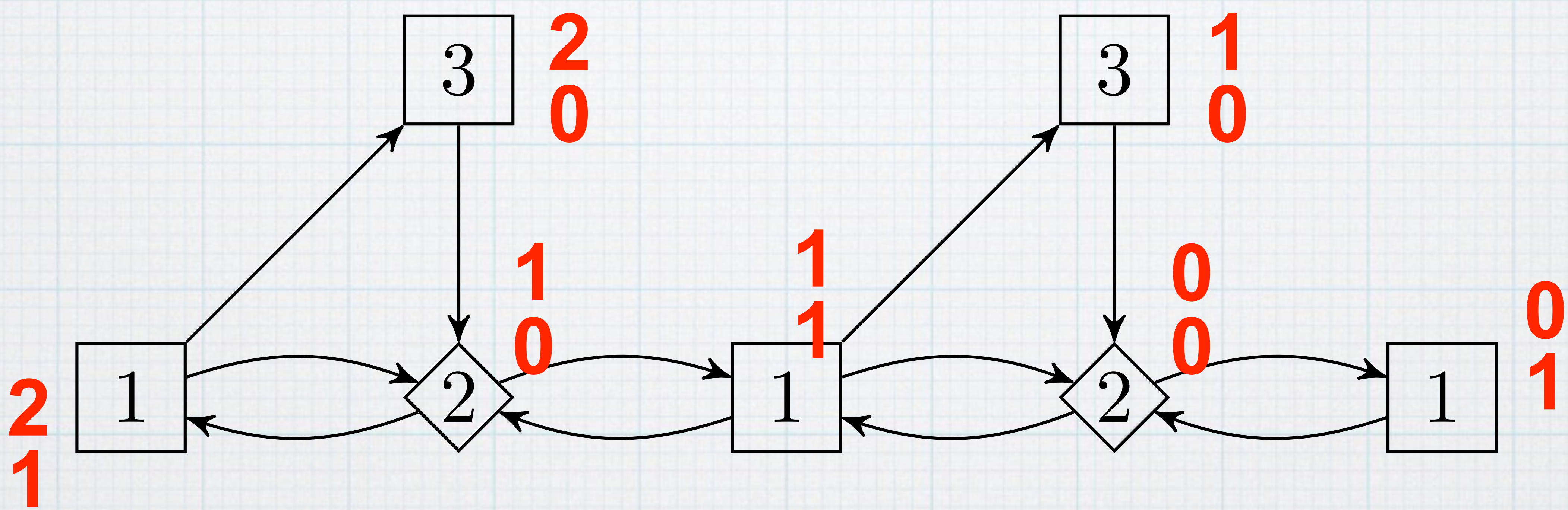
Jurdzinski's Progress Measure
Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"



Jurdzinski's Progress Measure Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"

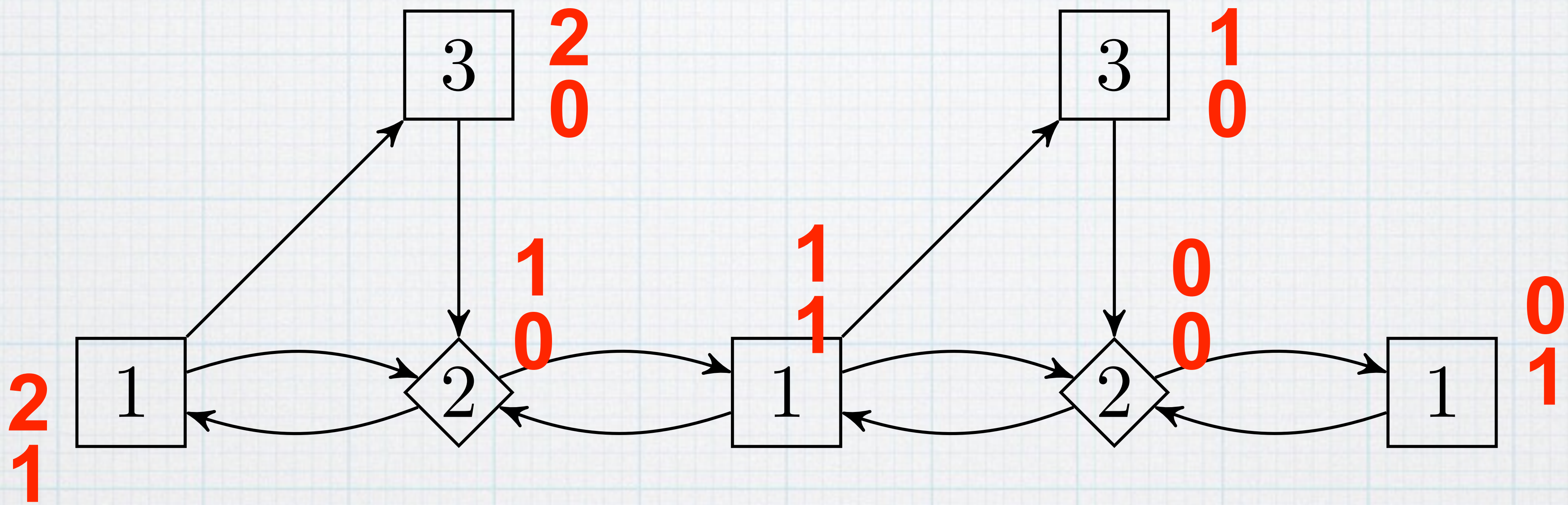


n_3 — how many 3's will be visited

n_1 — how many 1's will be visited (before visiting 2, a bigger even)

Jurdzinski's Progress Me
Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"

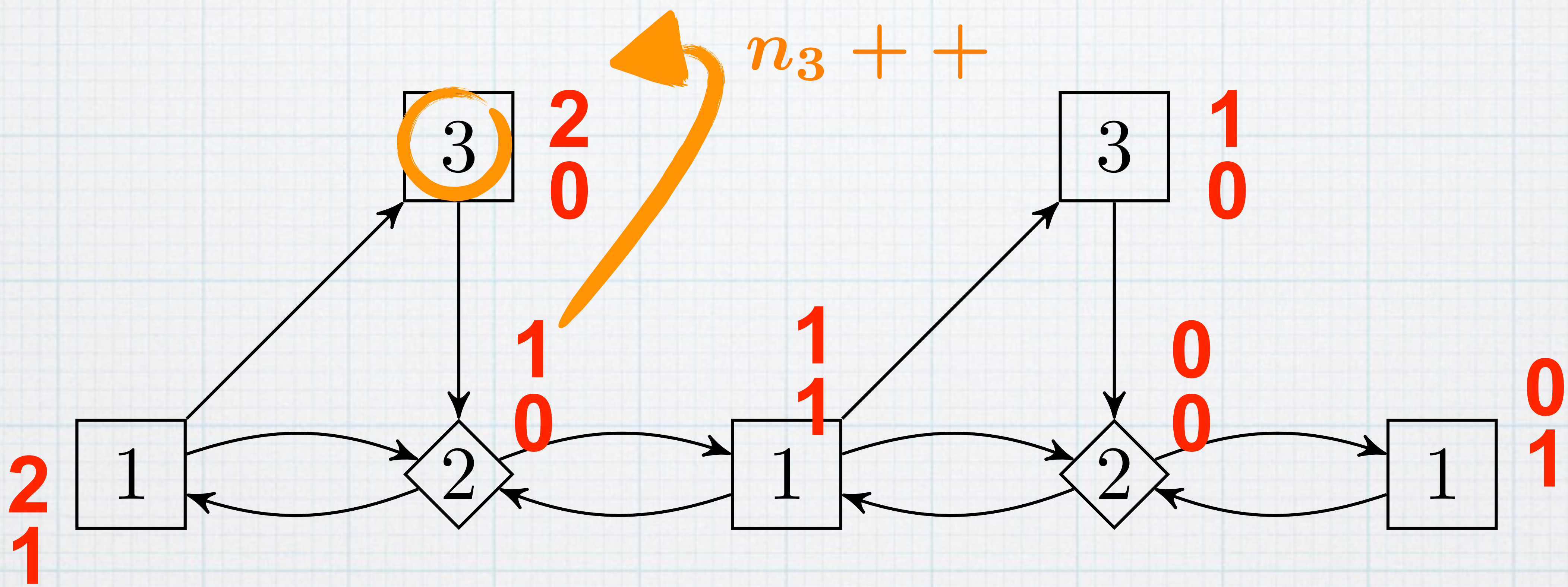


n_3 — how many 3's will be visited

n_1 — how many 1's will be visited
(before visiting 2, a bigger even)

Jurdzinski's Progress Me[asure]
Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"

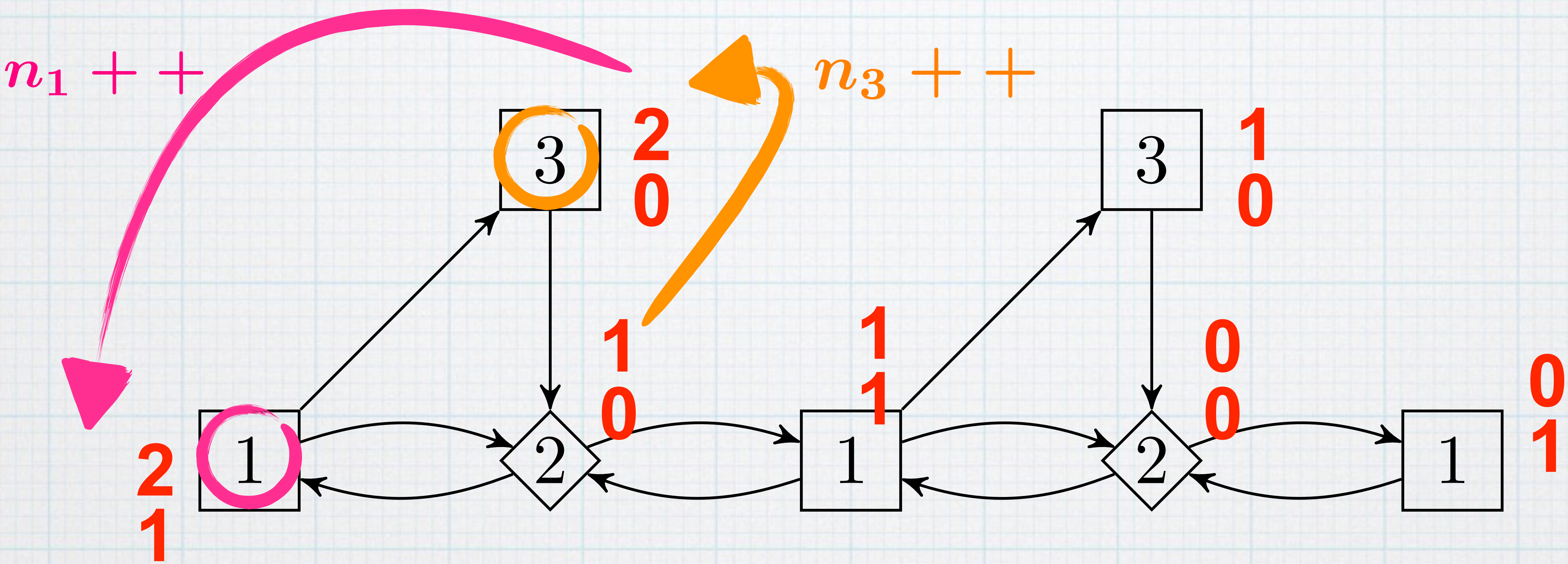


n_3 — how many 3's will be visited

n_1 — how many 1's will be visited (before visiting 2, a bigger even)

Jurdzinski's Progress Me[asure]
Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"



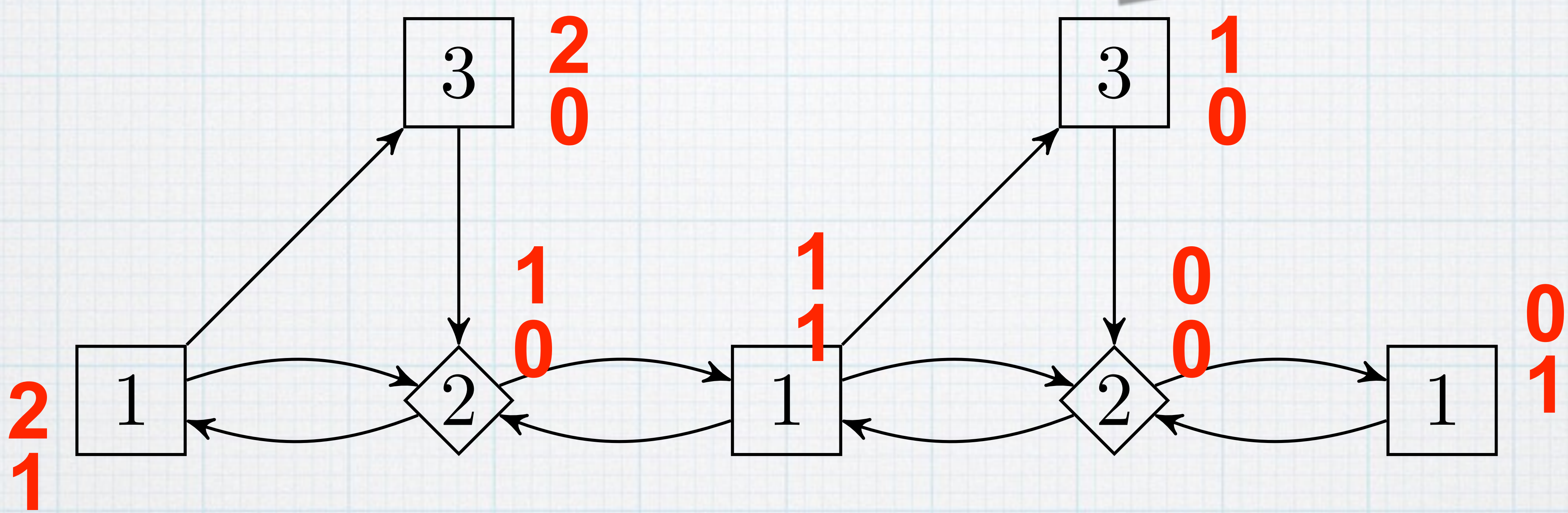
n_3 — how many 3's will be visited

n_1 — how many 1's will be visited (before visiting 2, a bigger even)

Jurdzinski's Progress Me

Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"

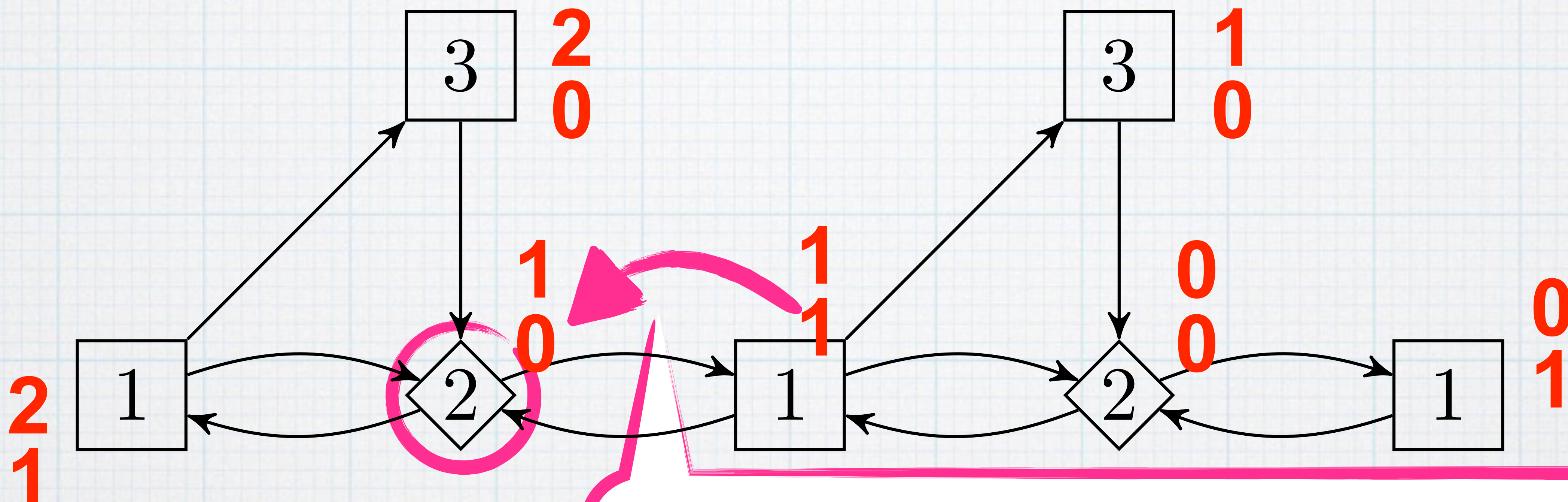


n_3 — how many 3's will be visited

n_1 — how many 1's will be visited (before visiting 2, a bigger even)

Jurdzinski's Progress Me
Intuitions

◇: your position
□: opponent's
goal: "visit bigger even"



$n_1 := 0$

because visiting 2 **cancels out** visiting 1

n_3 — how many 3's will be visited

n_1 — how many 1's will be visited (before visiting 2, a bigger even)

Jurdzinski's Progress Measure
Definition

(Assuming priorities are 0, 1, ..., 6)

* A **prioritized ordinal** is α_5 α_3 α_1 (each α_j is an ordinal)

Jurdzinski's Progress Measure

Definition

(Assuming priorities are 0, 1, ..., 6)

* A **prioritized ordinal** is $\begin{matrix}\alpha_5\\\alpha_3\\\alpha_1\end{matrix}$ (each α_j is an ordinal)

* for each $i = 0, 1, \ldots, 6,$ the **i-th truncated lexicographic order**

$$\begin{matrix}\alpha_5\\\alpha_3\\\alpha_1\end{matrix} \preceq_i \begin{matrix}\beta_5\\\beta_3\\\beta_1\end{matrix}$$

is defined by

* the lexicographic order
* after truncating α_j, β_j for all $j < i$

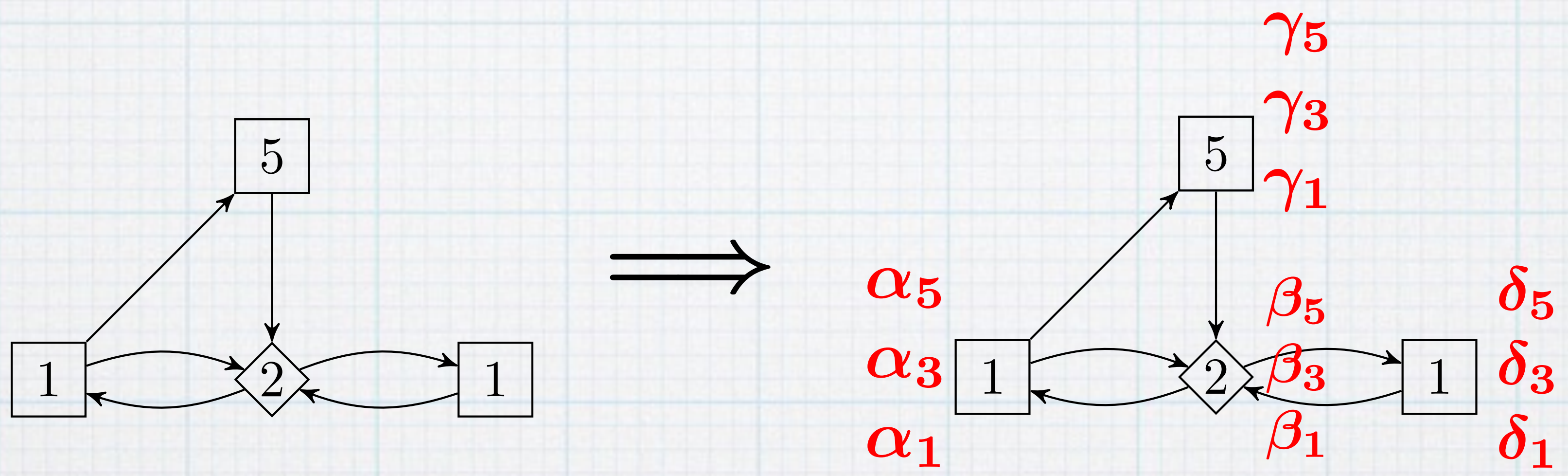
* examples: $\begin{matrix}7\\142\\63\end{matrix} \preceq_1 \begin{matrix}8\\0\\0\end{matrix}$ $\quad \begin{matrix}2\\142\\63\end{matrix} \preceq_4 \begin{matrix}2\\0\\0\end{matrix}$

truncated

Jurdzinski's Progress Measure Definition

(Assuming priorities are 0, 1, ..., 6)

* A **progress measure** is an assignment like

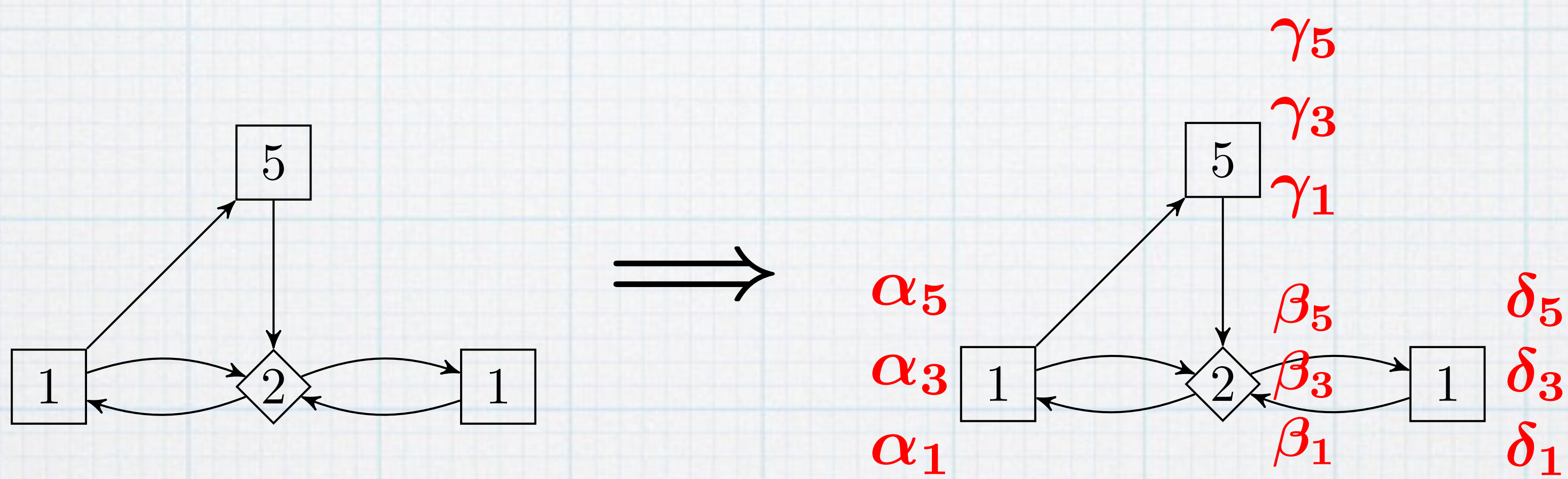


such that

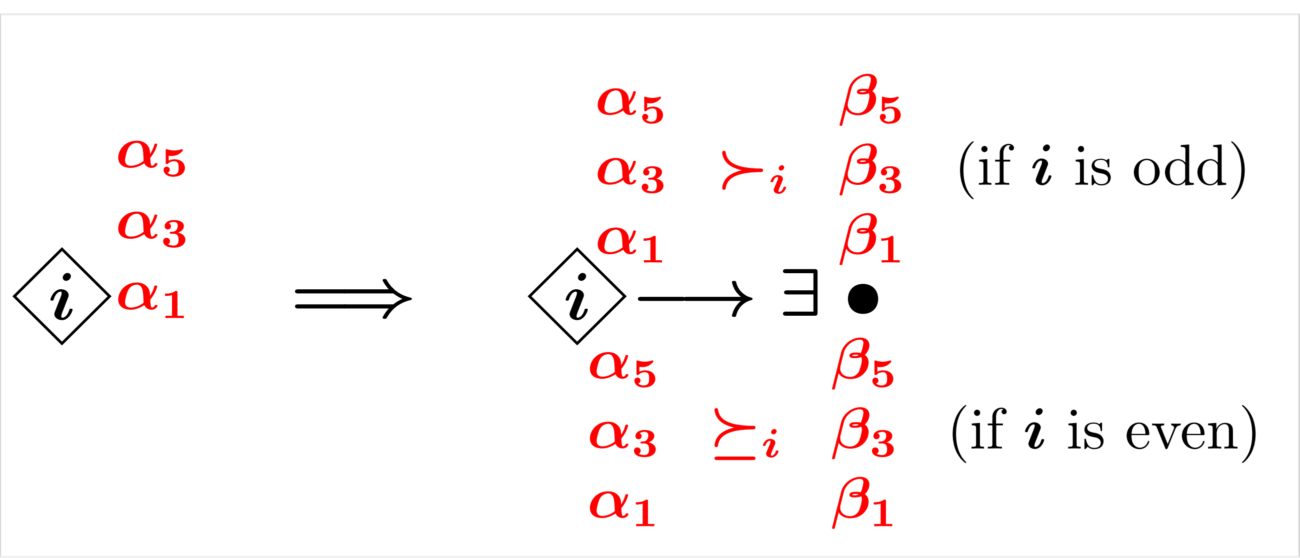
Jurdzinski's Progress Measure Definition

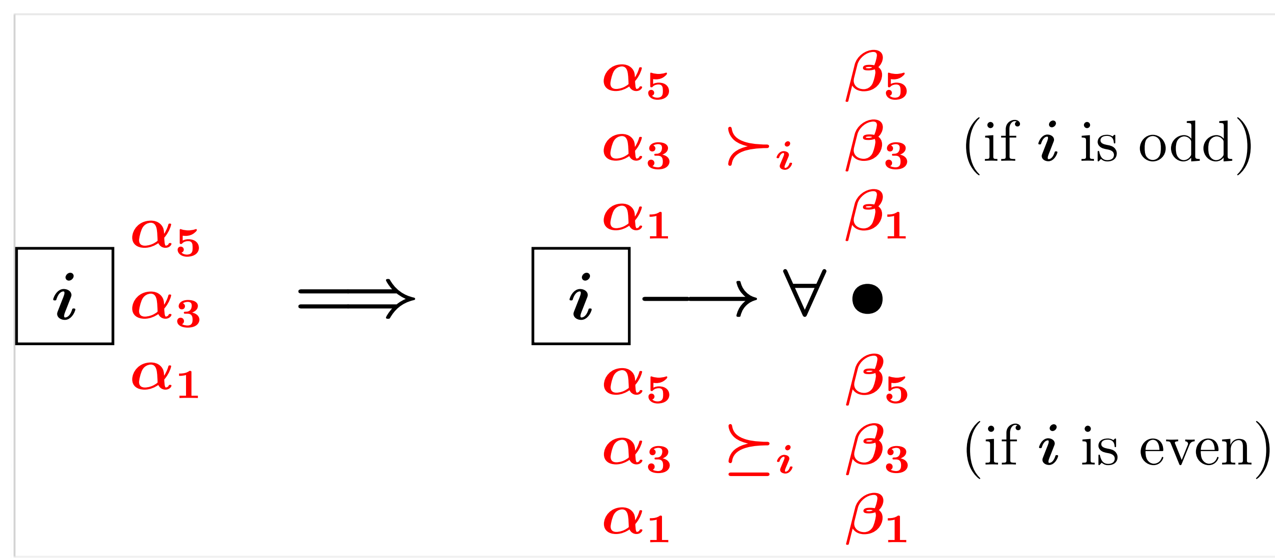
(Assuming priorities are 0, 1, …, 6)

* A **progress measure** is an assignment like



such that





The Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**progress measure for a parity game** [Jurdzinski]

The Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**progress measure for a parity game** [Jurdzinski] **lattice-theoretic progress measure** **(Our first main contrib.)**

The Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**progress measure for a parity game** [Jurdzinski] **lattice-theoretic progress measure** **(Our first main contrib.)**

finite, algorithmic

The Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**progress measure for a parity game** [Jurdzinski] **lattice-theoretic progress measure** **(Our first main contrib.)**

finite, algorithmic

infinite, symbolic, logical

The Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**progress measure for a parity game** [Jurdzinski] **lattice-theoretic progress measure** **(Our first main contrib.)**

Knaster-Tarski

Cousot-Cousot

finite, algorithmic

infinite, symbolic, logical

Syntax: Equational Systems

[Arnold & Niwinski '01], [Cleaveland, Klein & Steffen, CAV'92], ...

<u>Def.</u> An *equational system* over a complete lattice L is

$$\begin{aligned} u_1 &=_{\eta_1} f_1(u_1, \dots, u_m), \\ &\vdots \\ u_m &=_{\eta_m} f_m(u_1, \dots, u_m) \end{aligned}$$

where

- $f_1, \dots, f_m \colon L^m \to L$ are monotone, and
- $\eta_1, \dots, \eta_m \in \{\mu, \nu\}$.

Syntax: Equational Systems

Def. An *equational system* over a complete lattice L is

$$u_1 =_{\eta_1} f_1(u_1, \ldots, u_m),$$
$$\vdots$$
$$u_m =_{\eta_m} f_m(u_1, \ldots, u_m)$$

where

- $f_1, \ldots, f_m \colon L^m \to L$ are monotone, and
- $\eta_1, \ldots, \eta_m \in \{\mu, \nu\}$.

$$u_1 =_\mu f_1(u_1, u_2),$$
$$u_2 =_\nu f_2(u_1, u_2)$$

//

$$\nu u_2.\, f_2(\, \mu u_1.\, f_1(u_1, u_2),\, u_2\,)$$

Syntax: Equational Systems

Def. An *equational system* over a complete lattice L is

$$u_1 =_{\eta_1} f_1(u_1, \dots, u_m),$$
$$\vdots$$
$$u_m =_{\eta_m} f_m(u_1, \dots, u_m)$$

where

- $f_1, \dots, f_m \colon L^m \to L$ are monotone, and
- $\eta_1, \dots, \eta_m \in \{\mu, \nu\}$.

solved first

$$u_1 =_\mu f_1(u_1, u_2),$$
$$u_2 =_\nu f_2(u_1, u_2)$$

$$\nu u_2.\, f_2(\,\mu u_1.\, f_1(u_1, u_2),\, u_2\,)$$

The order matters!

Definition: Progress Measure for

$$u_1 =_{\mu} f_1(\vec{u})$$
$$u_2 =_{\nu} f_2(\vec{u})$$
$$u_3 =_{\mu} f_3(\vec{u})$$
$$u_4 =_{\nu} f_4(\vec{u})$$

over L

Definition: Progress Measure for

$$u_1 =_\mu f_1(\vec{u})$$
$$u_2 =_\nu f_2(\vec{u})$$
$$u_3 =_\mu f_3(\vec{u})$$
$$u_4 =_\nu f_4(\vec{u})$$

over L

$$p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathbf{Ord}}$$

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [1, 4]$

* "Counters" α_1, α_3 for each μ-var.
* Subject to:
  1. Monotonicity
  2. μ-var. cond.
  3. ν-var. cond.

Definition: Progress Measure for

$$\begin{array}{l} u_1 =_\mu f_1(\vec{u}) \\ u_2 =_\nu f_2(\vec{u}) \\ u_3 =_\mu f_3(\vec{u}) \\ u_4 =_\nu f_4(\vec{u}) \end{array}$$

over L

$$p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathrm{Ord}}$$

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [1, 4]$

1. (Monotonicity) For $i \in [1,4]$,

$$(\alpha_1, \alpha_3) \preceq_i (\beta_1, \beta_3) \implies p_i(\alpha_1, \alpha_3) \sqsubseteq p_i(\beta_1, \beta_3)$$

Definition: Progress Measure for

$$
\begin{aligned}
u_1 &=_\mu f_1(\vec{u}) \\
u_2 &=_\nu f_2(\vec{u}) \\
u_3 &=_\mu f_3(\vec{u}) \\
u_4 &=_\nu f_4(\vec{u})
\end{aligned}
$$

over L

$$
p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathbf{Ord}}
$$

with $p_i(\alpha_1, \alpha_3) \in L, \quad \forall i \in [1, 4]$

2. (μ-var. cond.)

- (base) $p_1(0, \alpha_3) = \bot, \quad p_3(\alpha_1, 0) = \bot$
- (step)

$$
p_1(\alpha_1 + 1, \quad \alpha_3 \quad) \sqsubseteq f_1 \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \end{pmatrix}
$$

$$
p_3(\quad \alpha_1 \quad, \alpha_3 + 1) \sqsubseteq f_3 \begin{pmatrix} p_1(\beta_1, \alpha_3) \\ p_3(\beta_1, \alpha_3) \end{pmatrix} \qquad (\exists \beta_1)
$$

- (limit)

$$
p_1(\alpha_1, \alpha_3) \sqsubseteq \bigsqcup_{\beta_1 < \alpha_1} p_1(\beta_1, \alpha_3) \qquad (\alpha_1 \text{: a limit ord.})
$$

(same for α_3)

Defi...

Thm. (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^{\omega}(\bot) \sqsubseteq \cdots$

stabilizes, and converges to μf

for

$$\begin{aligned} u_1 &=_{\mu} f_1(\vec{u}) \\ u_2 &=_{\nu} f_2(\vec{u}) \\ u_3 &=_{\mu} f_3(\vec{u}) \\ u_4 &=_{\nu} f_4(\vec{u}) \end{aligned}$$

over L

$$p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathbf{Ord}}$$

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [1, 4]$

2. (μ-var. cond.)

- (base)

$$p_1(0, \alpha_3) = \bot, \quad p_3(\alpha_1, 0) = \bot$$

- (step)

$$p_1(\alpha_1 + 1, \alpha_3) \sqsubseteq f_1 \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \end{pmatrix}$$

$$p_3(\alpha_1, \alpha_3 + 1) \sqsubseteq f_3 \begin{pmatrix} p_1(\beta_1, \alpha_3) \\ p_3(\beta_1, \alpha_3) \end{pmatrix} \quad (\exists \beta_1)$$

- (limit)

$$p_1(\alpha_1, \alpha_3) \sqsubseteq \bigsqcup_{\beta_1 < \alpha_1} p_1(\beta_1, \alpha_3) \qquad (\alpha_1\text{: a limit ord.})$$

(same for α_3)

Definition: Progress Measure for

$$\begin{aligned} u_1 &=_{\mu} f_1(\vec{u}) \\ u_2 &=_{\nu} f_2(\vec{u}) \\ u_3 &=_{\mu} f_3(\vec{u}) \\ u_4 &=_{\nu} f_4(\vec{u}) \end{aligned}$$

over L

$$p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathbf{Ord}}$$

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [1, 4]$

3. (ν-var. cond.)

$$p_2(\alpha_1, \alpha_3) \sqsubseteq f_2\left(\overrightarrow{p}(\beta_1, \alpha_3)\right) \qquad (\exists \beta_1)$$

$$p_4(\alpha_1, \alpha_3) \sqsubseteq f_4\left(\overrightarrow{p}(\beta_1, \beta_3)\right) \qquad (\exists \beta_1, \beta_3)$$

Thm. (Knaster-Tarski)

- $\nu f = \max\{l \in L \mid l \sqsubseteq f(l)\}$

$$\Longrightarrow \quad \frac{l \sqsubseteq f(l)}{l \sqsubseteq \nu f}$$

for

$$\begin{aligned} u_1 &=_{\mu} f_1(\vec{u}) \\ u_2 &=_{\nu} f_2(\vec{u}) \\ u_3 &=_{\mu} f_3(\vec{u}) \\ u_4 &=_{\nu} f_4(\vec{u}) \end{aligned}$$

over L

$$\begin{pmatrix} \ldots \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathbf{Ord}}$$

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [1, 4]$

3. (ν-var. cond.)

$$p_2(\alpha_1, \alpha_3) \sqsubseteq f_2\left(\vec{p}(\beta_1, \alpha_3)\right) \quad (\exists \beta_1)$$

$$p_4(\alpha_1, \alpha_3) \sqsubseteq f_4\left(\vec{p}(\beta_1, \beta_3)\right) \quad (\exists \beta_1, \beta_3)$$

Definition: Progress Measure for

$$u_1 =_\mu f_1(\vec{u})$$
$$u_2 =_\nu f_2(\vec{u})$$
$$u_3 =_\mu f_3(\vec{u})$$
$$u_4 =_\nu f_4(\vec{u})$$

over L

$$p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathrm{Ord}}$$

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [1, 4]$

1. Monotonicity
2. μ-var. cond. (base, step, limit)
3. ν-var. cond.

Definition: Progress Measure for

$$\begin{aligned} u_1 &=_\mu f_1(\vec{u}) \\ u_2 &=_\nu f_2(\vec{u}) \\ u_3 &=_\mu f_3(\vec{u}) \\ u_4 &=_\nu f_4(\vec{u}) \end{aligned}$$

over L

$$p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathbf{Ord}}$$

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [1, 4]$

1. Monotonicity
2. μ-var. cond. (base, step, limit)

$$p_1(\alpha_1 + 1, \quad \alpha_3 \quad) \sqsubseteq f_1 \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \end{pmatrix}$$

$$p_3(\quad \alpha_1 \quad , \alpha_3 + 1) \sqsubseteq f_3 \begin{pmatrix} p_1(\beta_1, \alpha_3) \\ p_3(\beta_1, \alpha_3) \end{pmatrix} \qquad (\exists \beta_1)$$

3. ν-var. cond.

$$p_2(\alpha_1, \alpha_3) \sqsubseteq f_2(\vec{p}(\beta_1, \alpha_3)) \qquad (\exists \beta_1)$$

$$p_4(\alpha_1, \alpha_3) \sqsubseteq f_4(\vec{p}(\beta_1, \beta_3)) \qquad (\exists \beta_1, \beta_3)$$

Definition: Progress Measure for

$$\begin{aligned} u_1 &=_\mu f_1(\vec{u}) \\ u_2 &=_\nu f_2(\vec{u}) \\ u_3 &=_\mu f_3(\vec{u}) \\ u_4 &=_\nu f_4(\vec{u}) \end{aligned}$$

over L

$$p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathrm{Ord}}$$

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [\;\; 4]$

$$\begin{matrix} 2 \\ 142 \\ 63 \end{matrix} \preceq_4 \begin{matrix} 2 \\ 0 \\ 0 \end{matrix}$$

1. Monotonicity
2. μ-var. cond. (base, step, limit)

$$p_1(\alpha_1 + 1, \quad \alpha_3 \quad) \sqsubseteq f_1 \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \end{pmatrix}$$

$$p_3(\quad \alpha_1 \quad , \alpha_3 + 1) \sqsubseteq f_3 \begin{pmatrix} p_1(\beta_1, \alpha_3) \\ p_3(\beta_1, \alpha_3) \end{pmatrix} \qquad (\exists \beta_1)$$

3. ν-var. cond.

$$p_2(\alpha_1, \alpha_3) \sqsubseteq f_2\left(\vec{p}(\beta_1, \alpha_3)\right) \qquad (\exists \beta_1)$$

$$p_4(\alpha_1, \alpha_3) \sqsubseteq f_4\left(\vec{p}(\beta_1, \beta_3)\right) \qquad (\exists \beta_1, \beta_3)$$

Correctness

* (soundness)

  Let $p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \mathbf{Ord}}$ be a prog. meas. for $\begin{array}{l} u_1 =_\mu f_1(\vec{u}) \\ u_2 =_\nu f_2(\vec{u}) \\ u_3 =_\mu f_3(\vec{u}) \\ u_4 =_\nu f_4(\vec{u}) \end{array}$

  Then p underapproximates the solution:

$$p_i(\alpha_1, \alpha_3) \sqsubseteq (\text{the solution for } u_i),$$

$$\text{for each } \alpha_1, \alpha_3 \in \mathbf{Ord} \text{ and } i \in [1, 4]$$

* **(completeness)** There is a prog. meas. that achieves equalities

The Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**progress measure for a parity game** (if finitary); **(lattice-theoretic) progress measure** (in general)

(Potential) applications:

- **Theorem proving**, proof rules
- Program verification: "**synthesis of symbolic progress measures**"
- In metatheories
- Generic "coalgebraic" model checking

Table

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, **alternating** gfp's & lfp's	**progress measure for a parity game** (if finitary); **(lattice-theoretic) progress measure** (in general)

Lattice-Theoretic Progress Measures in Coalgebraic Model Checking

(in 2 min.)

See e.g. [Rutten, TCS'00] [Jacobs, book draft]

Coalgebra

* Categorical abstraction of **state-based dynamics**

$$\begin{array}{c} FX \\ c\uparrow \\ X \end{array}$$

$F = 2 \times (\_)^{\Sigma}$	DFA
$F = (\mathcal{P}\_)^{\Sigma}$	LTS
$F = \mathcal{D}$	Markov chain
$F = \mathcal{P}\mathcal{P}$	nbd. frames, games
other F's	graded sys., game frames, $\cdots$

Coalgebraic Modal Logic

[Moss, Pattinson, Kurz, Cirstea, Kupke, Venema, Schroeder,...]

$$\frac{\text{modal logic}}{\text{Kripke frame}} = \frac{\textbf{coalg. modal logic}}{\text{coalgebra}}$$

Coalgebraic Modal Logic

[Moss, Pattinson, Kurz, Cirstea, Kupke, Venema, Schroeder,...]

$$\frac{\text{modal logic}}{\text{Kripke frame}} = \frac{\text{coalg. modal logic}}{\text{coalgebra}}$$

- Modalities by **predicate liftings**

$$\lambda\colon \Omega^X \longrightarrow \Omega^{FX}, \quad \text{natural in } X$$

where $\Omega = \{\text{truth values}\}$ (e.g. $\{\mathbf{t}, \mathbf{f}\}$ or $[0,1]$)

- Hennessy-Milner logic, neighborhood logic, graded logic ("in more than k successors"), game logic ("a coalition C forces..."), Lukasiewicz logic [Mio, Simpson, ...], logics w/ future discounting [Almagor, Boker, Kupfermann, ...], ...

- Fixed points by eq. sys.

$$u_1 =_\mu (p \wedge u_2) \vee \mathsf{X} u_1$$
$$u_2 =_\nu u_2$$

Contributions I: Branching Time

* **Progress measure**, as a witness in model checking
  * X can be infinite
  * $\mathbf{\Omega}$ can be $[0,1]$
* **MC algorithm**, if finitary
  * X: finite, $\mathbf{\Omega} = \{\mathrm{t}, \mathrm{f}\}$
  * Generic algorithm, works for a variety of logics
  * Complexity exponential only in alternation depth

Def.

$$p = \begin{pmatrix} p_1(\alpha_1, \dots, \alpha_k) \\ \vdots \\ p_m(\alpha_1, \dots, \alpha_k) \end{pmatrix}_{\vec{\alpha} \in \mathbf{Ord}}$$

- with $p_i(\vec{\alpha}) \in \mathbf{\Omega}^X$,
- subject to
  1. monotonicity
  2. μ-var. cond.
  3. ν-var. cond.

Thm.

$$\begin{pmatrix} p_1(\alpha_1, \dots, \alpha_k) \\ \vdots \\ p_m(\alpha_1, \dots, \alpha_k) \end{pmatrix}_{\vec{\alpha} \in \mathbf{Ord}} \sqsubseteq \left[\!\left[\begin{matrix} u_1 =_{\eta_1} \varphi_1(\vec{u}) \\ \vdots \\ u_m =_{\eta_m} \varphi_m(\vec{u}) \end{matrix} \right]\!\right]_{\substack{FX \\ \uparrow \\ X}}$$

Contributions II: Linear Time

Contributions II: Linear Time

- Like **LTL** (as opp. to CTL)
- More challenging for coalgebra
  ➜
  in a **Kleisli** category
- We focus on **nondet.** branching

Contributions II: Linear Time

* **Progress measure**, for linear-time model checking
  * $\left(\begin{array}{c} \mathcal{P}FX \\ \uparrow \\ X \end{array}, x \right) \models \left(\begin{array}{ccc} u_1 & =_{\eta_1} & \varphi_1(\vec{u}) \\ & \vdots & \\ u_m & =_{\eta_m} & \varphi_m(\vec{u}) \end{array} \right)$

    is witnessed by
    * a **runtree** $\begin{array}{c} FY \\ \uparrow \\ Y \end{array}$, and
    * data like $\left(\begin{array}{c} p_1(\alpha_1, \dots, \alpha_k) \\ \vdots \\ p_m(\alpha_1, \dots, \alpha_k) \end{array} \right)_{\vec{\alpha} \in \mathbf{Ord}}$

      with $p_i(\vec{\alpha}) \in \Omega^Y$

* **Decision procedure**, if finitary
  * Exploits the **small runtree** theorem

- Like **LTL** (as opp. to CTL)
- More challenging for coalgebra ➜ in a **Kleisli** category
- We focus on **nondet.** branching

Conclusions

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**winning strategies for a parity game** (if finitary); **(lattice-theoretic) progress measure** (in general)

(Potential) applications:

- **[done]** Generic "coalgebraic" model checking
- **[Forthcoming]** Coalgebraic modeling of Buechi automata & simulations
- **Theorem proving**, proof rules
- Program verification: "**synthesis of symbolic progress measures**"
- In metatheories, e.g. for higher-order model checking [Ong, Kobayashi, Tsukada, ...]

Conclusions

Thank you for your attention!

Ichiro Hasuo (Dept. CS, U. Tokyo)
http://www-mmm.is.s.u-tokyo.ac.jp/~ichiro

properties	witnessed by...
safety, gfp	invariants
liveness, lfp	ranking functions
nested, alternating gfp's & lfp's	**winning strategies for a parity game** (if finitary); **(lattice-theoretic) progress measure** (in general)

(Potential) applications:

- **[done]** Generic "coalgebraic" model checking
- **[Forthcoming]** Coalgebraic modeling of Buechi automata & simulations
- **Theorem proving**, proof rules
- Program verification: "**synthesis of symbolic progress measures**"
- In metatheories, e.g. for higher-order model checking [Ong, Kobayashi, Tsukada, ...]