Lattice-Theoretic Progress Measures and Coalgebraic Model Checking

Ichiro Hasuo
University of Tokyo (JP)

Shunsuke Shimizu

Corina Cirstea
University of Southampton (UK)
Contributions

* Lattice-theoretic progress measure

* Coalgebraic model checking as application
Invariant vs. Ranking Function

- **Gp** (everywhere \( p \)) is a gfp
  - the greatest solution of \( u = p \land Xu \)

- **Fp** (eventually \( p \)) is an lfp
  - the least solution of \( u = p \lor Xu \)

A linear Kripke structure:
\[
\text{succ}: X \to X, \quad [p] \subseteq X
\]
Invariant vs. Ranking Function

A linear Kripke structure:
\[ \text{succ}: X \rightarrow X, \quad [p] \subseteq X \]
Invariant vs. Ranking Function

A linear Kripke structure:
\[ \text{succ}: X \rightarrow X, \quad [p] \subseteq X \]

**Lem.** (witnessing \( Gp = \nu u. (p \land X u) \))

\[
\begin{align*}
I \subseteq [p] \quad x \in I & \Rightarrow \text{succ}(x) \in I \\
I \subseteq [Gp] &
\end{align*}
\]
Invariant vs. Ranking Function

A linear Kripke structure:
\( \text{succ}: X \rightarrow X, \quad [p] \subseteq X \)

**Lem.** (witnessing \( Gp = \nu u. (p \land X u) \))

\[
\begin{align*}
I \subseteq [p] & \quad x \in I \Rightarrow \text{succ}(x) \in I \\
I \subseteq [Gp] & \quad \text{invariant}
\end{align*}
\]
**Invariant vs. Ranking Function**

A linear Kripke structure:

\[ \text{succ: } X \rightarrow X, \quad [p] \subseteq X \]

**Lemma.** (witnessing \( G \ p = \nu u. (p \land X u) \))

\[
\begin{align*}
I \subseteq [p] \\
x \in I \Rightarrow \text{succ}(x) \in I \\
I \subseteq [G \ p]
\end{align*}
\]

**Lemma.** (witnessing \( F \ p = \mu u. (p \lor X u) \))

Let \( \text{rk}: X \rightarrow \omega \sqcup \{\spadesuit\} \) be such that

\[
\begin{align*}
\text{rk}(x) = n \land x \not\in [p] \\
\Rightarrow \text{rk}(\text{succ}(x)) \leq n - 1 .
\end{align*}
\]

Then \( \text{rk}(x) \neq \spadesuit \) implies \( x \in [F \ p] \).
Invariant vs. Ranking Function

A linear Kripke structure:
succ: $X \rightarrow X$, $\llbracket p \rrbracket \subseteq X$

**Lemma.** (witnessing $Gp = \nu u. (p \land X u)$)

$I \subseteq \llbracket p \rrbracket \quad x \in I \Rightarrow \text{succ}(x) \in I$

$I \subseteq \llbracket Gp \rrbracket$

**Lemma.** (witnessing $Fp = \mu u. (p \lor X u)$)

Let $rk: X \rightarrow \omega \uplus \{ \spadesuit \}$ be such that

$rk(x) = n \land x \not\in \llbracket p \rrbracket$

$\Rightarrow \quad rk(\text{succ}(x)) \leq n - 1$.

Then $rk(x) \neq \spadesuit$ implies $x \in \llbracket Fp \rrbracket$. 
**Lem.** (witnessing $\mathbf{G} p = \nu u. (p \land \mathbf{X} u)$)

$$I \subseteq [p] \quad x \in I \Rightarrow \text{succ}(x) \in I$$

$$I \subseteq [\mathbf{G} p]$$

**Lem.** (witnessing $\mathbf{F} p = \mu u. (p \lor \mathbf{X} u)$)

Let $\text{rk}: X \rightarrow \omega \sqcup \{♣\}$ be such that

$$\text{rk}(x) = n \land x \not\in [p]$$

$$\Rightarrow \quad \text{rk}(\text{succ}(x)) \leq n - 1.$$  

Then $\text{rk}(x) \neq ♣$ implies $x \in [\mathbf{F} p]$.

* How come the difference?
  → Let us take a foundational view...
**Lattice-Theoretic Foundation**

$L$: complete lattice, $f : L \rightarrow L$ 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 $\mu f$

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^\omega(\top) \sqsupseteq \cdots$ stabilizes, and converges to $\nu f$
Lattice-Theoretic Foundation

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

**Thm.** (Knaster-Tarski)

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

**Thm.** (Cousot-Cousot)

\( \perp \subseteq f(\perp) \subseteq \cdots \subseteq f^\omega(\perp) \subseteq \cdots \)
stabilizes, and converges to \( \mu f \)

\( \top \supseteq f(\top) \supseteq \cdots \supseteq f^\omega(\top) \supseteq \cdots \)
stabilizes, and converges to \( \nu f \)
Lattice-Theoretic Foundation

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

**Thm.** (Knaster-Tarski)

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

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

**Thm.** (Cousot-Cousot)

\[ \bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^\omega (\bot) \sqsubseteq \cdots \]

stabilizes, and converges to $\mu f$

\[ \implies f^\alpha (\bot) \sqsubseteq \mu f \quad (\forall \alpha \in \text{Ord}) \]

\[ \top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^\omega (\top) \sqsupseteq \cdots \]

stabilizes, and converges to $\nu f$

\[ \implies \nu f \sqsupseteq f^\alpha (\top) \quad (\forall \alpha \in \text{Ord}) \]
Lattice-Theoretic Foundation

\( L: \) complete lattice, \( f: L \to L \) monotone

**Thm.** (Knaster-Tarski)

- \( \mu f = \min\{l \in L \mid f(l) \sqsubseteq l\} \)
  \[ \implies \frac{f(l) \sqsubseteq l}{\mu f \sqsubseteq l} \]
- \( \nu f = \max\{l \in L \mid l \sqsubseteq f(l)\} \)
  \[ \implies \frac{l \sqsubseteq f(l)}{l \sqsubseteq \nu f} \]

**Thm.** (Cousot-Cousot)

\( \perp \sqsubseteq f(\perp) \sqsubseteq \cdots \sqsubseteq f^\omega(\perp) \sqsubseteq \cdots \) stabilizes, and converges to \( \mu f \)

\[ \implies f^\alpha(\perp) \sqsubseteq \mu f \quad (\forall \alpha \in \text{Ord}) \]

\( \top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^\omega(\top) \sqsupseteq \cdots \) stabilizes, and converges to \( \nu f \)

\[ \implies \nu f \sqsubseteq f^\alpha(\top) \quad (\forall \alpha \in \text{Ord}) \]
Lattice-Theoretic Foundation

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

**Thm.** (Knaster-Tarski)

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

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

**Thm.** (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^\omega(\bot) \sqsubseteq \cdots$ stabilizes, and converges to $\mu f$

\[\implies f^\alpha(\bot) \sqsubseteq \mu f \quad (\forall \alpha \in \text{Ord})\]

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^\omega(\top) \sqsupseteq \cdots$ stabilizes, and converges to $\nu f$

\[\implies \nu f \sqsubseteq f^\alpha(\top) \quad (\forall \alpha \in \text{Ord})\]

Sound approx. from below
### The Table

<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
</tbody>
</table>
## The Table

<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating</td>
<td></td>
</tr>
<tr>
<td>gfp’s &amp; lfp’s</td>
<td></td>
</tr>
<tr>
<td>properties</td>
<td>witnessed by...</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating</td>
<td>winning strategies</td>
</tr>
<tr>
<td>gfp’s &amp; lfp’s</td>
<td>for a parity game</td>
</tr>
<tr>
<td></td>
<td>(if finitary)</td>
</tr>
</tbody>
</table>
The Parity-Game Workflow

Your Problem -> encode

Parity Game

Jurdzinski’s algorithm

Winner & Winning Strategy

Solution

MC, satisfiability, synthesis, …
The Parity-Game Workflow

Your Problem

Parity Game

encode

Jurdzinski's algorithm

Solution

Winner & Winning Strategy

* In parity games:
  * alt. branching ($\forall$ vs $\exists$, $\land$ vs $\lor$)
  * parity acceptance cond.
    $\Rightarrow$ alt. betw. $\mu$ and $\nu$

Hasuo (Tokyo)
Jurdzinski’s Progress Measure for Parity Games: Intuitions

- ⧸: your position
- □: opponent’s
- goal: “visit bigger even”
Jurdzinski’s Progress Measure for Parity Games: Intuitions

YOU WIN!

◇: your position
☐: opponent’s
goal: “visit bigger even”
YOU WIN!

Jurdzinski’s Progress Measure for Parity Games: Intuitions

 namespaces: your position
☐: opponent’s goal: “visit bigger even”

Hasuo (Tokyo)
Jurdzinski’s Progress Measure for Parity Games: Intuitions

YOU WIN!

◇: your position
☐: opponent’s
goal: “visit bigger even”
Jurdzinski’s Progress Measure

Intuitions

◇: your position
☐: opponent’s
goal: “visit bigger even”
Jurdzinski’s Progress Measure Intuitions

- $n_3$: how many 3’s will be visited
- $n_1$: how many 1’s will be visited (before visiting 2, a bigger even)

◇: your position
☐: opponent’s goal: “visit bigger even”
Jurdzinski’s Progress Measure

Intuitions

- $\Diamond$: your position
- $\Box$: opponent’s

Goal: “visit bigger even”

- How many 3’s will be visited
- How many 1’s will be visited (before visiting 2, a bigger even)
Jurdzinski’s Progress Measure Intuitions

-how many 3’s will be visited

-how many 1’s will be visited

(before visiting 2, a bigger even)
Jurdzinski’s Progress Measure

Intuitions

$n_1 \quad +\quad +$

$n_3 \quad +\quad +$

how many 3’s will be visited

how many 1’s will be visited

(before visiting 2, a bigger even)
Jurdzinski’s Progress Measure

Intuitions

$n_3$ how many 3’s will be visited
$n_1$ how many 1’s will be visited (before visiting 2, a bigger even)

лежа: your position
☐: opponent’s
goal: “visit bigger even”

Hasuo (Tokyo)
Jurdzinski's Progress Measure

Intuitions

$n_1 := 0$

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)

◇: your position
☐: opponent's

goal: "visit bigger even"
Jurdzinski’s Progress Measure

Definition

* A prioritized ordinal is \( \alpha_1 \), \( \alpha_3 \), and \( \alpha_5 \) (each \( \alpha_j \) is an ordinal)

(Assuming priorities are 0, 1, ..., 6)
Jurdzinski’s Progress Measure

Definition

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

* A prioritized ordinal is $\alpha_5 \leq \alpha_3 \leq \alpha_1$ (each $\alpha_j$ is an ordinal)

* for each $i = 0, 1, ..., 6$,

the $i$-th truncated lexicographic order is defined by

- the lexicographic order
- after truncating $\alpha_j, \beta_j$ for all $j < i$

examples:

```
7  8  2  0
142 0 142 0
63 0 63 0
```
Jurdzinski’s Progress Measure

Definition

* A progress measure is an assignment like

such that

(Assuming priorities are 0, 1, ..., 6)
Jurdzinski’s Progress Measure

Definition

* A progress measure is an assignment like

such that

\[ i \rightarrow \exists \bullet \]

\[ i \rightarrow \forall \bullet \]

(Assuming priorities are 0, 1, ..., 6)
<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating gfp’s &amp; lfp’s</td>
<td>progress measure for a parity game [Jurdzinski]</td>
</tr>
<tr>
<td>properties</td>
<td>witnessed by...</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating</td>
<td>progress measure for a parity game</td>
</tr>
<tr>
<td>gfp's &amp; lfp's</td>
<td>[Jurdzinski]</td>
</tr>
<tr>
<td></td>
<td>lattice-theoretic progress measure</td>
</tr>
<tr>
<td></td>
<td>(Our first main contrib.)</td>
</tr>
</tbody>
</table>

Hasuo (Tokyo)
## The Table

<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating</td>
<td>progress measure for a parity game</td>
</tr>
<tr>
<td>gfps &amp; lfps</td>
<td>[Jurdzinski]</td>
</tr>
<tr>
<td></td>
<td>lattice-theoretic progress measure</td>
</tr>
<tr>
<td></td>
<td>(Our first main contrib.)</td>
</tr>
</tbody>
</table>

finite, algorithmic
<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating</td>
<td>progress measure for a parity game</td>
</tr>
<tr>
<td>gfp’s &amp; lfp’s</td>
<td>[Jurdzinski]</td>
</tr>
<tr>
<td></td>
<td>lattice-theoretic progress measure</td>
</tr>
<tr>
<td></td>
<td>(Our first main contrib.)</td>
</tr>
</tbody>
</table>

finite, algorithmic

infinite, symbolic, logical
## The Table

<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating gfp's &amp; lfp's</td>
<td>progress measure for a parity game [Jurdzinski]</td>
</tr>
</tbody>
</table>

- **Knaster-Tarski**
- **Cousot-Cousot**

**finite, algorithmic**

**infinite, symbolic, logical**

(Our first main contrib.)
Syntax: Equational Systems

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

**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

- $f_1, \ldots, f_m : L^m \rightarrow L$ are monotone, and

- $\eta_1, \ldots, \eta_m \in \{\mu, \nu\}$. 
**Syntax: Equational Systems**

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

\[
\begin{align*}
  u_1 &= \eta_1 f_1(u_1, \ldots, u_m), \\
  \vdots \\
  u_m &= \eta_m f_m(u_1, \ldots, u_m)
\end{align*}
\]

where

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

\[
\begin{align*}
  u_1 &= \mu f_1(u_1, u_2), \\
  u_2 &= \nu f_2(u_1, u_2) \\
  \nu u_2 \cdot f_2(\mu u_1 \cdot f_1(u_1, u_2), u_2)
\end{align*}
\]
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

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

The order matters!

\[ u_1 = \mu \ f_1(u_1, u_2), \]
\[ u_2 = \nu \ f_2(u_1, u_2) \]
\[ \nu u_2 \cdot f_2(\mu u_1 \cdot f_1(u_1, u_2), u_2) \]

solved first
Definition: Progress Measure for

\[ u_4 = v \cdot f_4(\bar{u}) \]
\[ u_3 = \mu \cdot f_3(\bar{u}) \]
\[ u_2 = \nu \cdot f_2(\bar{u}) \]
\[ u_1 = \mu \cdot f_1(\bar{u}) \]

over Hasuo (Tokyo)
Definition: 
Progress Measure for “Counters” $\alpha_1, \alpha_3$ for each $\mu$-var.

Subject to:
1. Monotonicity
2. $\mu$-var. cond.
3. $\nu$-var. cond.

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

$p$ = 
\[
\begin{pmatrix}
  p_1(\alpha_1, \alpha_3) \\
  p_2(\alpha_1, \alpha_3) \\
  p_3(\alpha_1, \alpha_3) \\
  p_4(\alpha_1, \alpha_3)
\end{pmatrix}
\]

with $p_i(\alpha_1, \alpha_3) \in L$, $\forall i \in [1, 4]$
Definition: Progress Measure for $L$

\[ p = \left( \begin{array}{c} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{array} \right) \quad \alpha_1, \alpha_3 \in \text{Ord} \]

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

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

\[ (\alpha_1, \alpha_3) \leq_i (\beta_1, \beta_3) \quad \Longrightarrow \quad p_i(\alpha_1, \alpha_3) \subseteq p_i(\beta_1, \beta_3) \]
Definition: Progress Measure for $L$

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

2. ($\mu$-var. cond.)
   - (base) $p_1(0, \alpha_3) = \bot$, $p_3(\alpha_1, 0) = \bot$
   - (step)
     
     $p_1(\alpha_1 + 1, \alpha_3) \subseteq f_1 \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \end{pmatrix}$
     
     $p_3(\alpha_1, \alpha_3 + 1) \subseteq f_3 \begin{pmatrix} p_1(\beta_1, \alpha_3) \\ p_3(\beta_1, \alpha_3) \end{pmatrix}$ ($\exists \beta_1$)

   - (limit)
     
     $p_1(\alpha_1, \alpha_3) \subseteq \bigsqcup_{\beta_1 < \alpha_1} p_1(\beta_1, \alpha_3)$ ($\alpha_1$: a limit ord.)

\[
\begin{align*}
  u_1 &= \mu f_1(\vec{u}) \\
  u_2 &= \nu f_2(\vec{u}) \\
  u_3 &= \mu f_3(\vec{u}) \\
  u_4 &= \nu f_4(\vec{u})
\end{align*}
\]
2. (μ-var. cond.)

• (base) \[ p_1(0, \alpha_3) = \bot, \quad p_3(\alpha_1, 0) = \bot \]

• (step) \[
\begin{align*}
  p_1(\alpha_1 + 1, \alpha_3) &\subseteq f_1 \left( \begin{pmatrix}
p_1(\alpha_1, \alpha_3) \\
p_3(\alpha_1, \alpha_3)
\end{pmatrix} \right) \\
  p_3(\alpha_1, \alpha_3 + 1) &\subseteq f_3 \left( \begin{pmatrix}
p_1(\beta_1, \alpha_3) \\
p_3(\beta_1, \alpha_3)
\end{pmatrix} \right) \quad (\exists \beta_1)
\end{align*}
\]

• (limit) \[
\begin{align*}
p_1(\alpha_1, \alpha_3) &\subseteq \bigsqcup_{\beta_1 < \alpha_1} p_1(\beta_1, \alpha_3) \quad (\alpha_1: \text{a limit ord.})
\end{align*}
\]
Definition: Progress Measure for $L$

$$p = \left( \begin{array}{c} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{array} \right)_{\alpha_1, \alpha_3 \in \text{Ord}}$$

with

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

3. (ν-var. cond.)

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

$$p_4(\alpha_1, \alpha_3) \sqsubseteq f_4(\overrightarrow{p}(\beta_1, \beta_3)) \quad (\exists \beta_1, \beta_3)$$
3. (ν-var. cond.)

\[ p_2(\alpha_1, \alpha_3) \subseteq f_2(\overrightarrow{p}(\beta_1, \alpha_3)) \quad (\exists \beta_1) \]

\[ p_4(\alpha_1, \alpha_3) \subseteq f_4(\overrightarrow{p}(\beta_1, \beta_3)) \quad (\exists \beta_1, \beta_3) \]
Definition: Progress Measure for $L$

$p = \left(\begin{array}{c} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{array}\right)$ with \(p_i(\alpha_1, \alpha_3) \in L, \quad \forall i \in [1, 4]\)

1. Monotonicity

2. $\mu$-var. cond.
   (base, step, limit)

3. $\nu$-var. cond.

\[
\begin{align*}
\mathbf{u}_1 &= \mu f_1(\mathbf{u}) \\
\mathbf{u}_2 &= \nu f_2(\mathbf{u}) \\
\mathbf{u}_3 &= \mu f_3(\mathbf{u}) \\
\mathbf{u}_4 &= \nu f_4(\mathbf{u})
\end{align*}
\]
Definition: Progress Measure for $L$

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

with

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

1. Monotonicity
2. $\mu$-var. cond. (base, step, limit)
3. $\nu$-var. cond.

$$ u_1 = \mu f_1(\vec{u}) $$
$$ u_2 = \nu f_2(\vec{u}) $$
$$ u_3 = \mu f_3(\vec{u}) $$
$$ u_4 = \nu f_4(\vec{u}) $$
Definition:
Progress Measure for

\[
p = \begin{pmatrix}
p_1(\alpha_1, \alpha_3) \\
p_2(\alpha_1, \alpha_3) \\
p_3(\alpha_1, \alpha_3) \\
p_4(\alpha_1, \alpha_3)
\end{pmatrix}
\]

\[\alpha_1, \alpha_3 \in \text{Ord}\]

1. Monotonicity
2. \(\mu\)-var. cond.  
   (base, step, limit)
3. \(\nu\)-var. cond.

\[
\begin{align*}
 u_1 &= \mu f_1(\vec{u}) \\
 u_2 &= \nu f_2(\vec{u}) \\
 u_3 &= \mu f_3(\vec{u}) \\
 u_4 &= \nu f_4(\vec{u})
\end{align*}
\]

over \(L\)

with

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

\[
\begin{pmatrix}
2 \\
142 \\
63 \\
2
\end{pmatrix} \preceq_4 \begin{pmatrix}
2 \\
0 \\
0
\end{pmatrix}
\]

\[
\begin{align*}
p_1(\alpha_1 + 1, \alpha_3) &\sqsubseteq f_1\left(\begin{pmatrix}
p_1(\alpha_1, \alpha_3) \\
p_3(\alpha_1, \alpha_3)
\end{pmatrix}\right) \\
p_3(\alpha_1, \alpha_3 + 1) &\sqsubseteq f_3\left(\begin{pmatrix}
p_1(\alpha_1, \alpha_3) \\
p_3(\alpha_1, \alpha_3)
\end{pmatrix}\right) (\exists \beta_1)
\end{align*}
\]

\[
\begin{align*}
p_2(\alpha_1, \alpha_3) &\sqsubseteq f_2\left(\begin{pmatrix}
\beta_1 \\
\alpha_3
\end{pmatrix}\right) (\exists \beta_1) \\
p_4(\alpha_1, \alpha_3) &\sqsubseteq f_4\left(\begin{pmatrix}
\beta_1 \\
\beta_3
\end{pmatrix}\right) (\exists \beta_1, \beta_3)
\end{align*}
\]
Correctness

* (soundness)

Let $p = \begin{pmatrix} p_1(\alpha_1, \alpha_3) \\ p_2(\alpha_1, \alpha_3) \\ p_3(\alpha_1, \alpha_3) \\ p_4(\alpha_1, \alpha_3) \end{pmatrix}_{\alpha_1, \alpha_3 \in \text{Ord}}$ be a prog. meas. for

Then $p$ underapproximates the solution:

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

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

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

\[ u_1 = \mu f_1(\bar{u}) \]
\[ u_2 = \nu f_2(\bar{u}) \]
\[ u_3 = \mu f_3(\bar{u}) \]
\[ u_4 = \nu f_4(\bar{u}) \]
## The Table

<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating gfp’s &amp; lfp’s</td>
<td>progress measure for a parity game (if finitary);</td>
</tr>
<tr>
<td></td>
<td>(lattice-theoretic)</td>
</tr>
<tr>
<td></td>
<td>progress measure (in general)</td>
</tr>
</tbody>
</table>

---

Hasuo (Tokyo)
(Potential) applications:

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

| Table
| witnessed by... |
|-----------------|----------------|
| invariants      | ranking functions |
| **progress measure for a parity game** | (if finitary); |
| (lattice-theoretic) progress measure | (in general) |

**gfp's & lfp's**
Lattice-Theoretic Progress Measures in Coalgebraic Model Checking (in 2 min.)
Coalgebra

* Categorical abstraction of state-based dynamics

\[ F(X) \]
\[ c \uparrow \]
\[ X \]

\[ F = 2 \times \text{operation} \]
\[ F = (\mathcal{P} \text{operation})^\Sigma \]
\[ F = \mathcal{D} \]
\[ F = \mathcal{P}\mathcal{P} \]
other \( F \)'s

DFA
LTS
Markov chain
nbd. frames, games
graded sys., game frames, \cdots
Coalgebraic Modal Logic

\[
\begin{align*}
\text{modal logic} & \quad = \quad \text{coalg. modal logic} \\
\text{Kripke frame} & \quad \quad = \quad \text{coalgebra}
\end{align*}
\]
Coalgebraic Modal Logic

```
modal logic
Kripke frame = coalg. modal logic
coalgebra
```

* Modalities by **predicate liftings**

\[ \lambda : \Omega^X \rightarrow \Omega^{FX} , \text{ natural in } X \]

where \( \Omega = \{ \text{truth values} \} \) (e.g. \{t, 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.

\[
\begin{align*}
  u_1 &= \mu (p \land u_2) \lor Xu_1 \\
  u_2 &= \nu u_2
\end{align*}
\]
Contributions I: Branching Time

* **Progress measure**, as a witness in model checking
  * $X$ can be infinite
  * $\Omega$ can be $[0,1]$

* **MC algorithm**, if finitary
  * $X$: finite, $\Omega = \{t, f\}$
  * Generic algorithm, works for a variety of logics
  * Complexity exponential only in alternation depth

---

**Def.**

\[
p = \begin{pmatrix}
p_1(\alpha_1, \ldots, \alpha_k) \\
\vdots \\
p_m(\alpha_1, \ldots, \alpha_k)
\end{pmatrix}
\forall \vec{\alpha} \in \text{Ord}
\]

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

**Thm.**

\[
\begin{pmatrix}
p_1(\alpha_1, \ldots, \alpha_k) \\
\vdots \\
p_m(\alpha_1, \ldots, \alpha_k)
\end{pmatrix}
\forall \vec{\alpha} \in \text{Ord}
\]

$u_1 = \eta_1 \varphi_1(\vec{u})$

$u_m = \eta_m \varphi_m(\vec{u})$

$FX \uparrow X$
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

\[
\begin{pmatrix}
\mathcal{P} F X \\
\uparrow \\
X
\end{pmatrix}
\vDash
\begin{pmatrix}
u_1 = \eta_1 & \varphi_1(\overline{u}) \\
\vdots \\
u_m = \eta_m & \varphi_m(\overline{u})
\end{pmatrix}
\]

is witnessed by

* a runtree \[FY\]

* data like \[
\begin{pmatrix}
p_1(\alpha_1, \ldots, \alpha_k) \\
\vdots \\
p_m(\alpha_1, \ldots, \alpha_k)
\end{pmatrix}
\]

with \[p_i(\overline{\alpha}) \in \Omega^Y\]

* 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

Hasuo (Tokyo)
Conclusions

<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating</td>
<td>winning strategies for a parity game</td>
</tr>
<tr>
<td>gfp’s &amp; lfp’s</td>
<td>(if finitary);</td>
</tr>
<tr>
<td></td>
<td>(lattice-theoretic) progress measure</td>
</tr>
<tr>
<td></td>
<td>(in general)</td>
</tr>
</tbody>
</table>

(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

<table>
<thead>
<tr>
<th>properties</th>
<th>witnessed by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>safety, gfp</td>
<td>invariants</td>
</tr>
<tr>
<td>liveness, lfp</td>
<td>ranking functions</td>
</tr>
<tr>
<td>nested, alternating</td>
<td></td>
</tr>
<tr>
<td>gfp’s &amp; lfp’s</td>
<td>winning strategies for a parity game</td>
</tr>
<tr>
<td></td>
<td>(if finitary);</td>
</tr>
<tr>
<td></td>
<td>(lattice-theoretic) progress measure</td>
</tr>
<tr>
<td></td>
<td>(in general)</td>
</tr>
</tbody>
</table>

(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, ...]