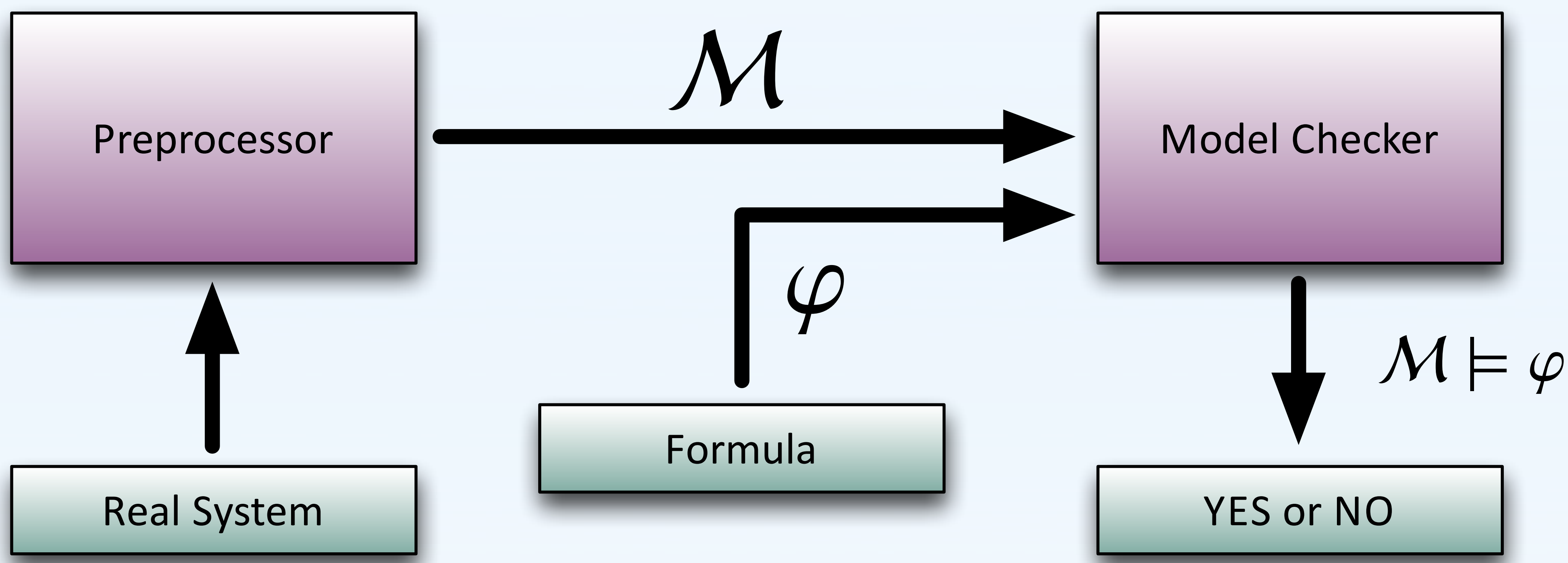
Simulation Relations for Rich Acceptance Conditions

César Sánchez[1,2] *and* ***Julian Samborski-Forlese***[1]

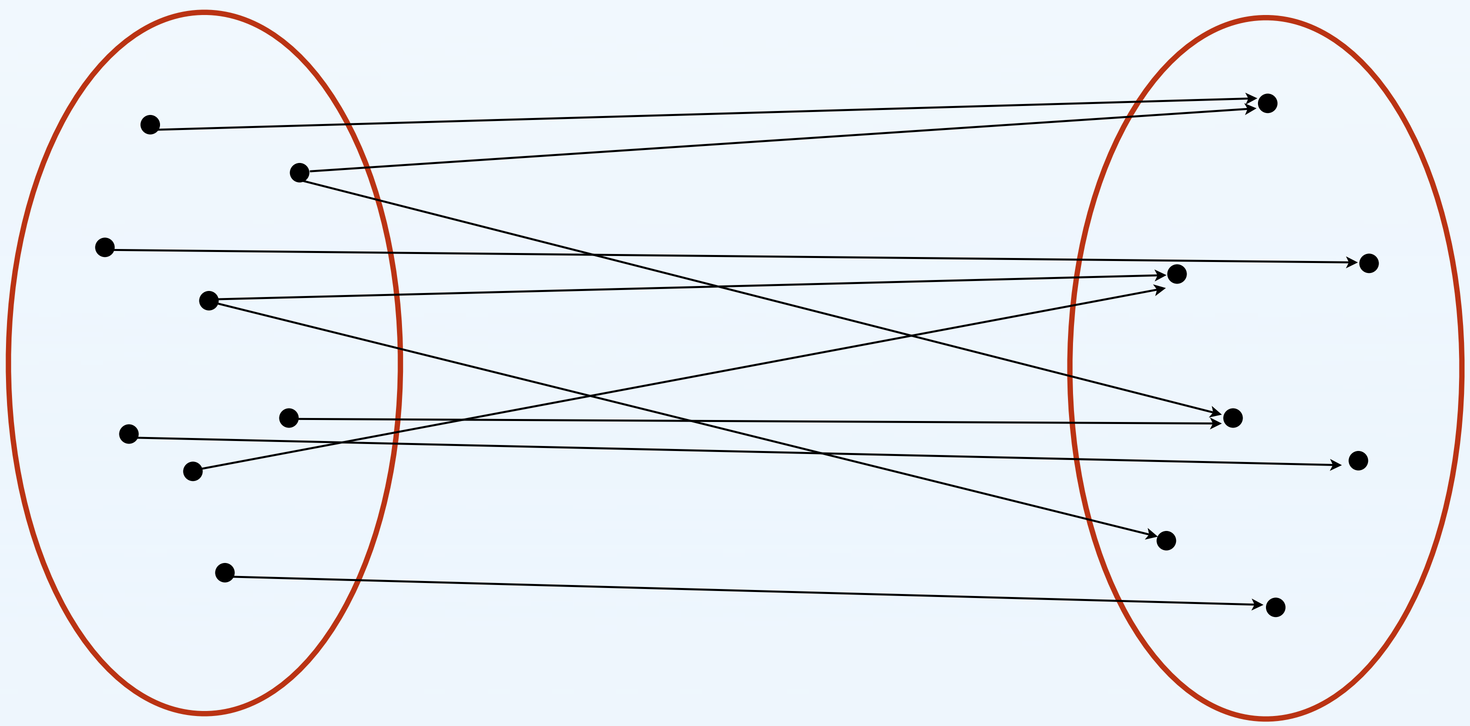
[1]IMDEA Software Institute, Madrid, Spain
[2]Institute for Information Security, CSIC, Spain

Rich Model Toolkit COST Action Meeting. Malta 2013. June 16th, 2013.

Quick Model Checking Intro

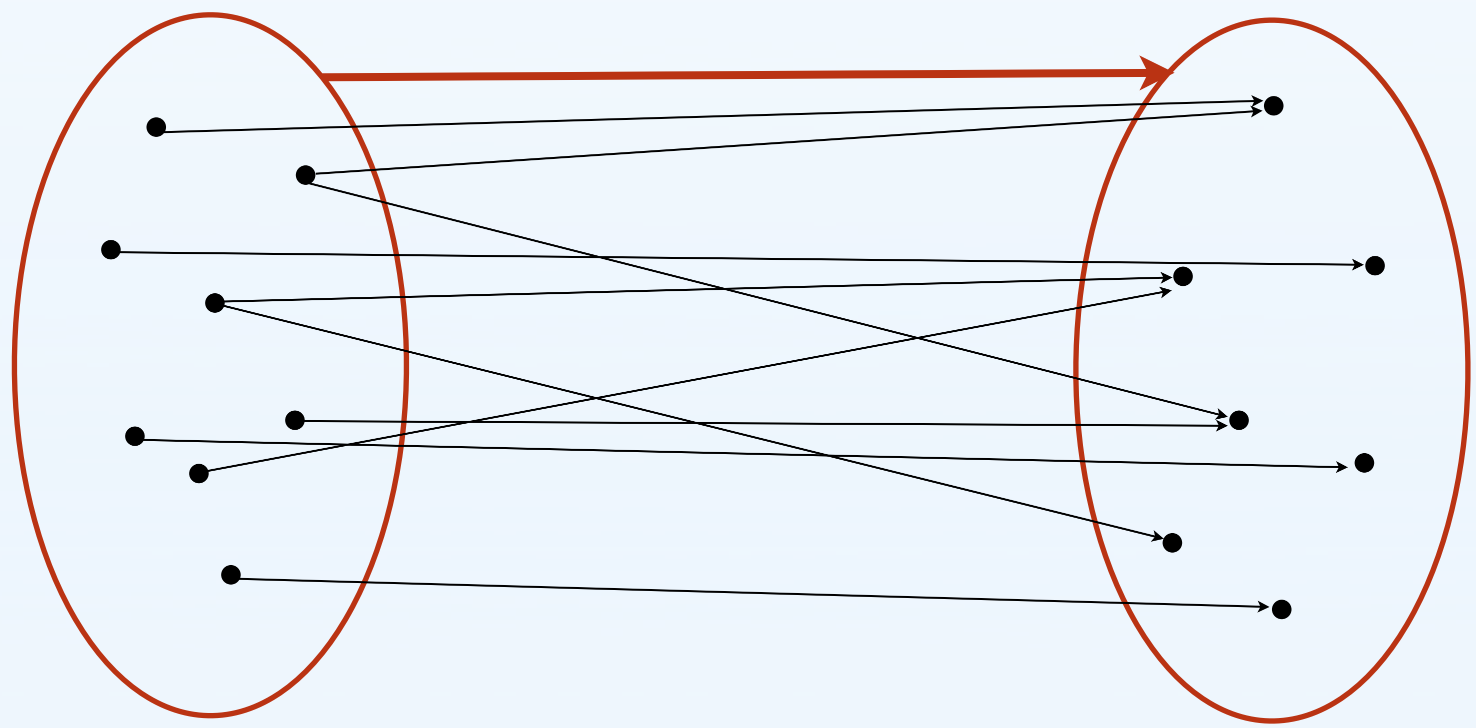


Antichain-based Model Checking [Raskin06]



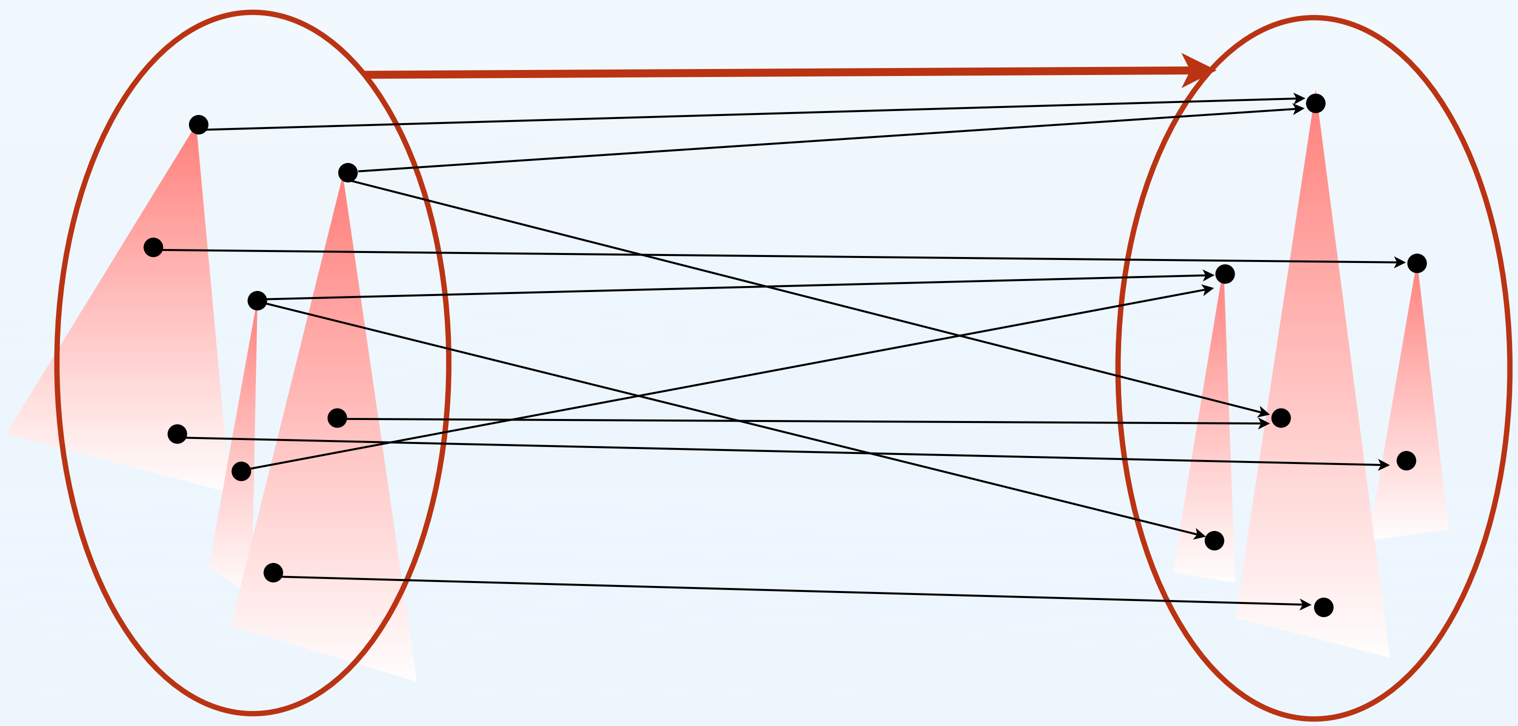
LTL ⟶ **ABW** $\xrightarrow{\text{MH}}$ **NBW**

Antichain-based Model Checking [Raskin06]



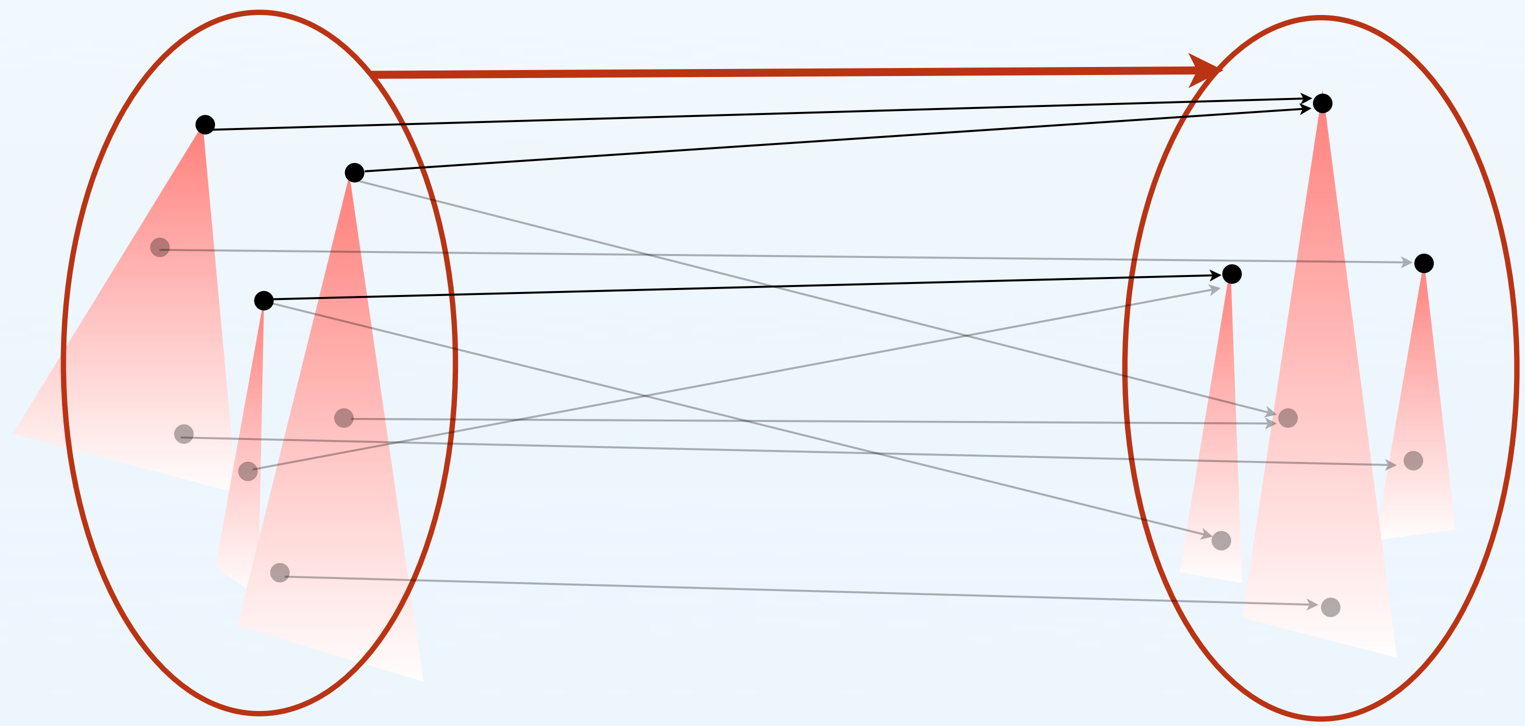
LTL $\longrightarrow$ **ABW** $\xrightarrow{\text{MH}}$ **NBW**

Antichain-based Model Checking [Raskin06]



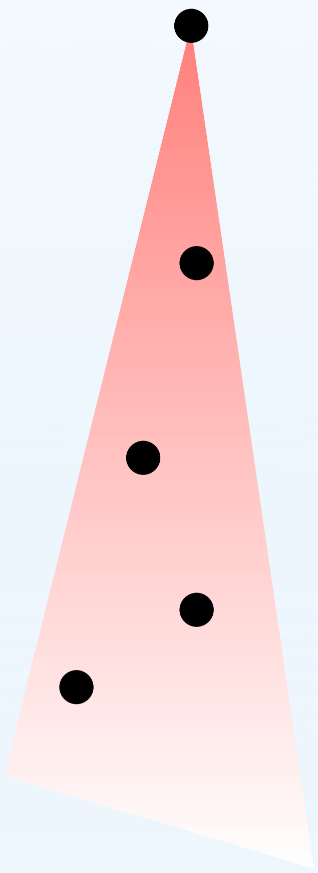
$$\mathbf{LTL} \longrightarrow \mathbf{ABW} \xrightarrow{\text{MH}} \mathbf{NBW}$$

Antichain-based Model Checking [Raskin06]



LTL $\longrightarrow$ **ABW** $\xrightarrow{\text{MH}}$ **NBW**

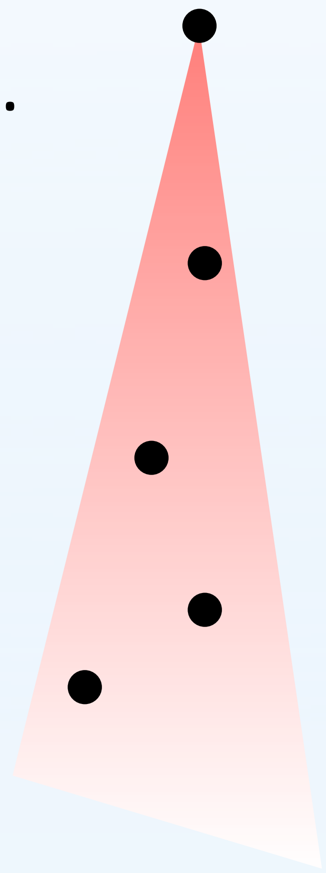
Antichain-based Model Checking [Raskin06]



LTL $\longrightarrow$ **ABW** $\xrightarrow{\text{MH}}$ **NBW**

Antichain-based Model Checking [Raskin06]

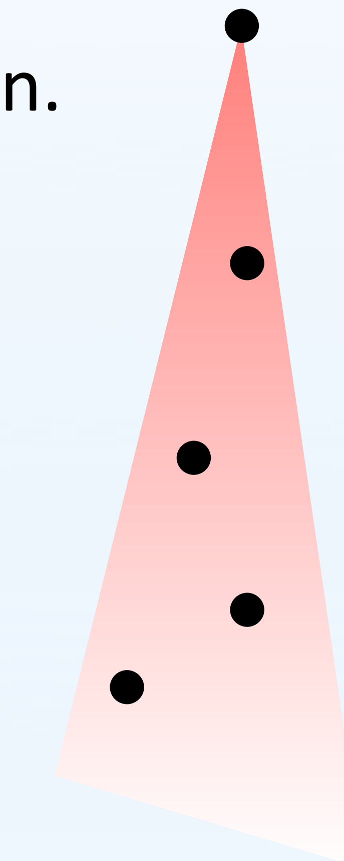
- Exploits simulation preorders that exist by-construction.



$$\textbf{LTL} \longrightarrow \textbf{ABW} \xrightarrow{\text{MH}} \textbf{NBW}$$

Antichain-based Model Checking [Raskin06]

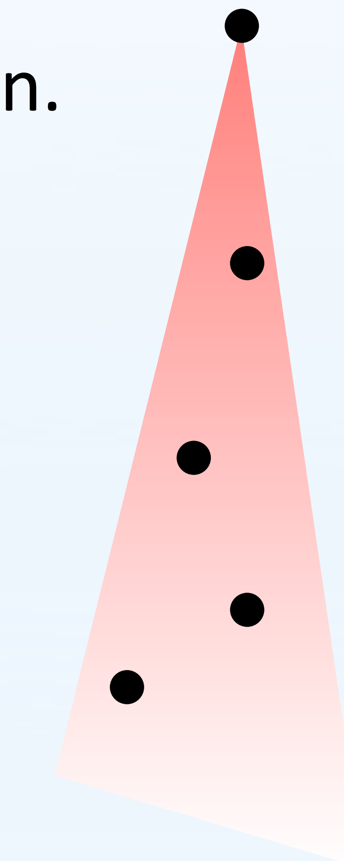
- Exploits simulation preorders that exist by-construction.
- For the Miyano-Hayashi construction the simulation relation is easy: [⊆,⊆].



LTL $\longrightarrow$ **ABW** $\xrightarrow{\text{MH}}$ **NBW**

Antichain-based Model Checking [Raskin06]

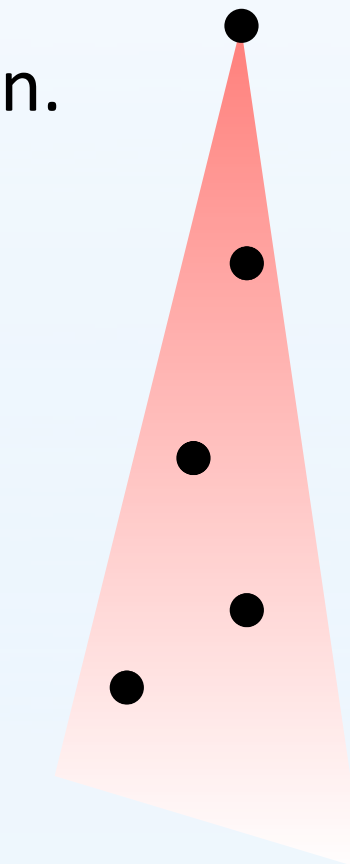
- Exploits simulation preorders that exist by-construction.
- For the Miyano-Hayashi construction the simulation relation is easy: [⊆,⊆].
- But, MH does not work for more complex logics.



$$\textbf{LTL} \longrightarrow \textbf{ABW} \xrightarrow{\text{MH}} \textbf{NBW}$$

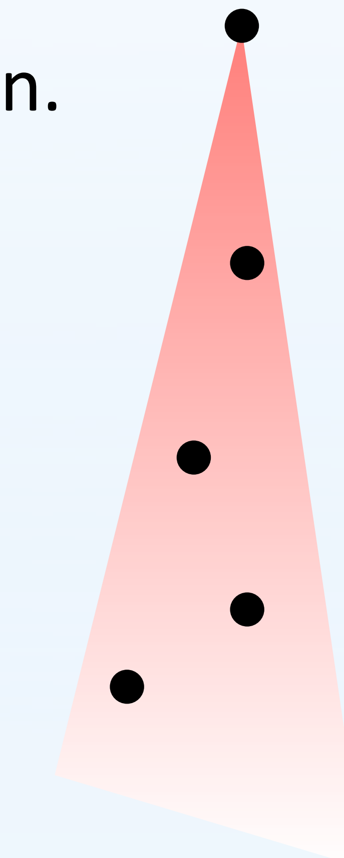
Antichain-based Model Checking [Raskin06]

- Exploits simulation preorders that exist by-construction.
- For the Miyano-Hayashi construction the simulation relation is easy: [⊆,⊆].
- But, MH does not work for more complex logics.



$$\textbf{RLTL} \longrightarrow \textbf{ABW} \xrightarrow{\text{MH}} \textbf{NBW}$$

Antichain-based Model Checking [Raskin06]

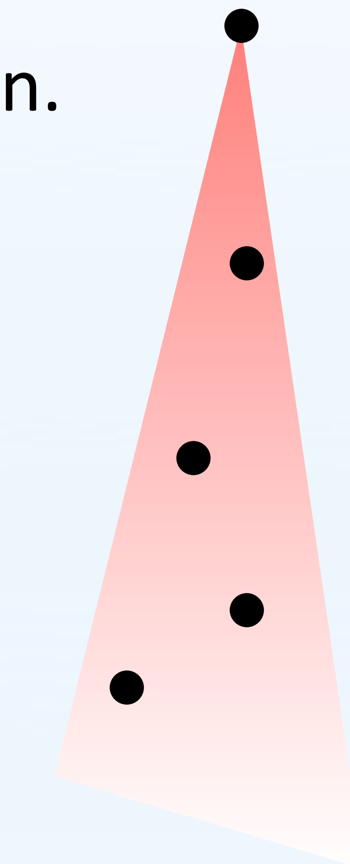


- Exploits simulation preorders that exist by-construction.
- For the Miyano-Hayashi construction the simulation relation is easy: [⊆,⊆].
- But, MH does not work for more complex logics.

$$\text{RLTL} \longrightarrow \cancel{\text{ABW}} \xrightarrow{\text{MH}} \text{NBW}$$

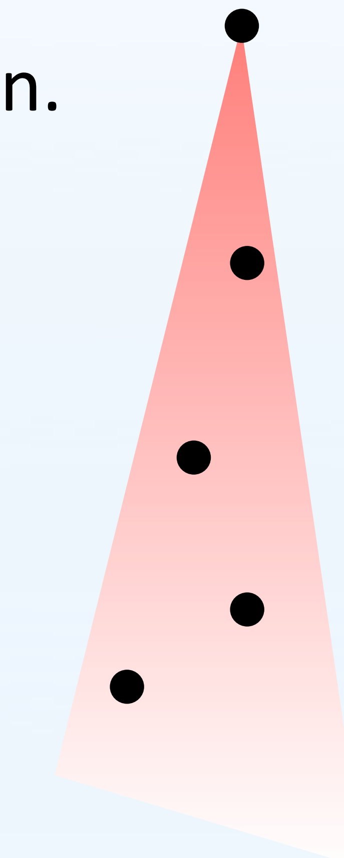
Antichain-based Model Checking [Raskin06]

- Exploits simulation preorders that exist by-construction.
- For the Miyano-Hayashi construction the simulation relation is easy: [⊆,⊆].
- But, MH does not work for more complex logics.



RLTL ⟶ **ASW** $\xrightarrow{\text{MH}}$ **NBW**

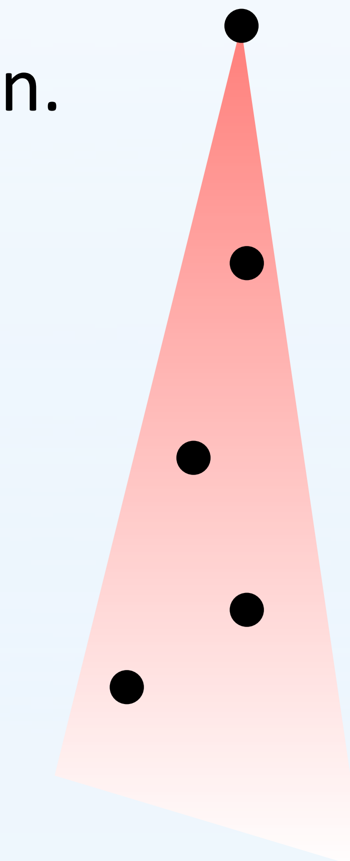
Antichain-based Model Checking [Raskin06]



- Exploits simulation preorders that exist by-construction.
- For the Miyano-Hayashi construction the simulation relation is easy: $[\subseteq,\subseteq]$.
- But, MH does not work for more complex logics.

$$\textbf{RLTL} \longrightarrow \textbf{ASW} \xrightarrow{\cancel{\text{MH}}} \textbf{NBW}$$

Antichain-based Model Checking [Raskin06]



- Exploits simulation preorders that exist by-construction.
- For the Miyano-Hayashi construction the simulation relation is easy: [⊆,⊆].
- But, MH does not work for more complex logics.
- **Original antichain-based algorithms cannot be applied to model checking extensions of LTL.**

$$\textbf{RLTL} \longrightarrow \textbf{ASW} \xrightarrow{\cancel{\text{MH}}} \textbf{NBW}$$

Our Goal

Develop antichain-based algorithms for extensions of LTL

Acceptance Conditions

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

- **Finite words**
  - $F \subseteq Q$ $\qquad$ $trace(\pi)$ ends in F

Acceptance Conditions

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

- **Finite words**
  - $F \subseteq Q$ $\quad$ $trace(\pi)$ ends in F
- **Infinite words**
  - Büchi $\quad F \subseteq Q \quad inf(\pi) \cap F \neq \emptyset$
  - coBüchi $\quad F \subseteq Q \quad inf(\pi) \cap F = \emptyset$
  - Parity $\quad Q \rightarrow \{0..k\} \quad max(F(inf(\pi)))$ is even
  - Street⟨1⟩ $\quad (B, G) \quad$ if $inf(\pi) \cap B \neq \emptyset$ then $inf(\pi) \cap G \neq \emptyset$
  - Rabin⟨1⟩ $\quad (B, G) \quad inf(\pi) \cap B \neq \emptyset$ and $inf(\pi) \cap G \neq \emptyset$

Acceptance Conditions

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

- **Finite words**
  - $F \subseteq Q$ $\qquad$ $trace(\pi)$ ends in F
- **Infinite words**
  - Büchi $\qquad$ $F \subseteq Q$ $\qquad$ $inf(\pi) \cap F \neq \emptyset$
  - coBüchi $\qquad$ $F \subseteq Q$ $\qquad$ $inf(\pi) \cap F = \emptyset$
  - Parity $\qquad$ $Q \to \{0..k\}$ $\qquad$ $max(F(inf(\pi)))$ is even
  - Street⟨1⟩ $\qquad$ (B, G) $\qquad$ if $inf(\pi) \cap B \neq \emptyset$ then $inf(\pi) \cap G \neq \emptyset$
  - Rabin⟨1⟩ $\qquad$ (B, G) $\qquad$ $inf(\pi) \cap B \neq \emptyset$ and $inf(\pi) \cap G \neq \emptyset$

Simulation Preorders on FSM

$\mathcal{N} = (\Sigma, Q, \delta, I, F)$

- **Forward Simulation** $\preceq_{\mathsf{f}} \subseteq Q \times Q$

Simulation Preorders on FSM

$\mathcal{N} = (\Sigma, Q, \delta, I, F)$

- **Forward Simulation** $\preceq_{\mathsf{f}} \subseteq Q \times Q$

q_1

$\preceq_{\mathsf{f}}$

q_2

Simulation Preorders on FSM

$\mathcal{N} = (\Sigma, Q, \delta, I, F)$

- **Forward Simulation** $\preceq_{\mathsf{f}} \subseteq Q \times Q$

$$\begin{array}{ccc} q_1 & \xrightarrow{\sigma} & q_3 \\ \rotatebox{90}{$\preceq_{\mathsf{f}}$} & & \\ q_2 & & \end{array}$$

Simulation Preorders on FSM

$\mathcal{N} = (\Sigma, Q, \delta, I, F)$

- **Forward Simulation** $\preceq_{\mathsf{f}} \subseteq Q \times Q$

$$
\begin{tikzcd}
q_1 \arrow[r, "\sigma"] \arrow[d, phantom, "\preceq_{\mathsf{f}}"] & q_3 \\
q_2 \arrow[r, "\sigma"] & q_4
\end{tikzcd}
$$

Simulation Preorders on FSM

$\mathcal{N} = (\Sigma, Q, \delta, I, F)$

- **Forward Simulation** $\preceq_{\mathsf{f}} \subseteq Q \times Q$

$$\begin{tikzcd} q_1 \arrow[r, "\sigma"] \arrow[d, phantom, "\rotatebox{90}{$\preceq_{\mathsf{f}}$}"] & q_3 \arrow[d, phantom, "\rotatebox{90}{$\preceq_{\mathsf{f}}$}"] \\ q_2 \arrow[r, "\sigma"] & q_4 \end{tikzcd}$$

Simulation Preorders on FSM

$\mathcal{N} = (\Sigma, Q, \delta, I, F)$

- **Forward Simulation** $\preceq_f \subseteq Q \times Q$

$$\begin{array}{ccc} q_1 & \xrightarrow{\quad\sigma\quad} & q_3 \\ \rotatebox{90}{$\preceq_f$} & & \rotatebox{90}{$\preceq_f$} \\ q_2 & \xrightarrow{\quad\sigma\quad} & q_4 \end{array}$$

q_2 forward simulates q_1

Emptiness and Model Checking $\mathcal{N} = (\Sigma, Q, \delta, I, F)$

Emptiness and Model Checking $\mathcal{N} = (\Sigma, Q, \delta, I, F)$

- **Backward Repeated Reachability**

$$\mathsf{BB}^*(M) = \mathsf{GFP}(\ \ X \cdot \mathsf{pre}^+(X) \cap F)$$

Language Emptiness

$$\mathcal{L}(\mathcal{N}) = \emptyset \text{ iff } \mathsf{BB}^* \cap I = \emptyset$$

Emptiness and Model Checking $\mathcal{N} = (\Sigma, Q, \delta, I, F)$

- **Backward Repeated Reachability**

$$\mathsf{BB}^*(M) = \mathsf{GFP}(\ X \cdot \mathsf{pre}^+(X) \cap F)$$

Language Emptiness

$$\mathcal{L}(\mathcal{N}) = \emptyset \text{ iff } \mathsf{BB}^* \cap I = \emptyset$$

- **Symbolic Backward Repeated Reachability**

$$\widehat{\mathsf{BB}}^*(M) = \mathsf{GFP}(\lambda X \cdot \lceil F \rceil \ \sqcap \ \widehat{\mathsf{pre}}^+(X)) \qquad (\preceq_{\mathsf{f}})$$

MH Construction

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

MH Construction

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

MH Construction

$\mathcal{A} = (\Sigma, Q, \delta, I, F)$

(S, O)

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

MH Construction

$\mathcal{A} = (\Sigma, Q, \delta, I, F)$

(S, O) $\qquad$ $(M, \emptyset)$

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

I. *M is a minimal model of $I_{\mathcal{N}}$*

MH Construction

$\mathcal{A} = (\Sigma, Q, \delta, I, F)$

(S, O)

$(M, \emptyset)$

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

$(S, \emptyset)$

MH Construction

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

$$\delta_{\mathcal{N}} : Q_{\mathcal{N}} \to 2^{Q_{\mathcal{N}}}$$

$$(S, O) \qquad (M, \emptyset)$$

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

$$(S, \emptyset)$$

$$\mathbf{D.}\ \delta_{\mathcal{N}} = \begin{array}{l} \left\{ \langle (\ {}_1\ \varnothing)\ \sigma\ (\ {}_2\ \ {}_2 \setminus\ \ )\rangle \;\middle|\; {}_1 \overset{\sigma}{\rightsquigarrow}\ {}_2 \right\} \cup \\ \left\{ \langle (\ {}_1\ \ {}_1 \neq \varnothing)\ \sigma\ (\ {}_2\ \ {}_2 \setminus\ \ )\rangle \;\middle|\; {}_1 \overset{\sigma}{\rightsquigarrow}\ {}_2\ \ {}_1 \overset{\sigma}{\rightsquigarrow}\ {}_2\ \ {}_2 \subseteq\ {}_2 \right\} \end{array}$$

Streett Construction

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

Streett Construction

$\mathcal{A} = (\Sigma, Q, \delta, I, F)$

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

Streett Construction

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

$$(S, O, f, ok)$$

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

Q1. *if q B then f(q) is e en.*

Q2. *if* $O \neq \emptyset$ *then* $ok = false$.

Streett Construction

$\mathcal{A} = (\Sigma, Q, \delta, I, F)$

(S, O, f, ok) (M, O, f, ok)

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

I. M *is a minimal model of* $I_{\mathcal{N}}$
$O = \{q \in M \mid q \notin G \text{ and } f(q) \text{ is even}\}$ *and* $ok = \mathit{false}$.

Streett Construction

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

$$(S, O, f, ok)$$

$$(M, O, f, ok)$$

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

$$\{(S, O, f, ok) \mid ok = true\}$$

Streett Construction

$$\mathcal{A} = (\Sigma, Q, \delta, I, F)$$

$$\delta_{\mathcal{N}} : Q_{\mathcal{N}} \to 2^{Q_{\mathcal{N}}}$$

$$(S, O, f, ok)$$

$$(M, O, f, ok)$$

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

$$\{(S, O, f, ok) \mid ok = true\}$$

Streett Construction

$\mathcal{A} = (\Sigma, Q, \delta, I, F)$

$\delta_{\mathcal{N}} : Q_{\mathcal{N}} \rightarrow 2^{Q_{\mathcal{N}}}$

(S, O, f, ok)

(M, O, f, ok)

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

$\{(S, O, f, ok) \mid ok = true\}$

D1. $S' = \cup_{q \in S} M_q$,

Streett Construction

$\mathcal{A} = (\Sigma, Q, \delta, I, F)$

$$\delta_{\mathcal{N}} : Q_{\mathcal{N}} \rightarrow 2^{Q_{\mathcal{N}}}$$

(S, O, f, ok)

(M, O, f, ok)

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

$$\{(S, O, f, ok) \mid ok = true\}$$

D1. $S' = \cup_{q \in S} M_q$,

D2. $f'(p) \leq min\{f(q) \mid q \in pred(p) \setminus G\}$

Streett Construction

$\mathcal{A} = (\Sigma, Q, \delta, I, F)$

$\delta_{\mathcal{N}} : Q_{\mathcal{N}} \to 2^{Q_{\mathcal{N}}}$

(S, O, f, ok)

(M, O, f, ok)

$$\mathcal{N} = (\Sigma, Q_{\mathcal{N}}, \delta_{\mathcal{N}}, I_{\mathcal{N}}, F_{\mathcal{N}})$$

$\{(S, O, f, ok) \mid ok = true\}$

D1. $S' = \cup_{q \in S} M_q$,

D2. $f'(p) \leq min\{f(q) \mid q \in pred(p) \setminus G\}$

D3. O' *is given as follows. Let* $p \in S' \setminus G$, *we have*

- *If* $ok = true$ *then* $p \in O'$ *iff* $f'(p)$ *is even.*
- *If* $ok = false$ *then* $p \in O'$ *iff* $f'(p) = f(q)$ *for some* $q \in (pred(p) \cap O)$.

Our Contribution

Definition (Streett Simulation Relation) *The Streett simulation relation* $\preceq$ *on* $\mathsf{S}(\mathscr{A}) \subseteq Q_N \times Q_N$ *is defined as* $(S_2, O_2, f_2, ok_2) \preceq (S_1, O_1, f_1, ok_1)$ *whenever:*

- **S1**. *for all* $q_2 \in S_2 \cap G$ *there is a* $q_1 \in S_1$ *with* $q_2 \ll q_1$.
- **S2**. *for all* $q_2 \in S_2 \cap \overline{G}$ *there is a* $q_1 \in S_1$ *with* $q_2 \ll q_1$ *and* $f_1(q_1) \leq f_2(q_2)$.
- **S3**. *for all* $q_2 \in O_2$ *there is a* $q_1 \in O_1$ *with* $q_2 \ll q_1$ *and* $f_1(q_1) \leq f_2(q_2)$.
- **S4**. ok_2 *if and only if* ok_1.

Our Contribution

Definition (Streett Simulation Relation) *The Streett simulation relation* $\preceq$ *on* $\mathsf{S}(\mathscr{A}) \subseteq Q_N \times Q_N$ *is defined as* $(S_2, O_2, f_2, ok_2) \preceq (S_1, O_1, f_1, ok_1)$ *whenever:*

- **S1**. *for all* $q_2 \in S_2 \cap G$ *there is a* $q_1 \in S_1$ *with* $q_2 \ll q_1$.
- **S2**. *for all* $q_2 \in S_2 \cap \overline{G}$ *there is a* $q_1 \in S_1$ *with* $q_2 \ll q_1$ *and* $f_1(q_1) \leq f_2(q_2)$.
- **S3**. *for all* $q_2 \in O_2$ *there is a* $q_1 \in O_1$ *with* $q_2 \ll q_1$ *and* $f_1(q_1) \leq f_2(q_2)$.
- **S4**. ok_2 *if and only if* ok_1.

Lemma *The Streett simulation relation* $\preceq$ *is a forward simulation on* $\mathsf{S}(\mathscr{A})$ *compatible with final states.*

Summary

- Antichains is a very cleaver model checking technique.
- Applied successfully to LTL model checking, outperforming traditional approaches.
- Showed the existence of simulation preorders on our more complex Streett construction.
- Similar results for our Rabin construction.

- Future guidelines:
  - Similar results for other interesting acceptance conditions (like Hesitant).
  - Implement antichains for RLTL (and possibly for PSL) and integrate into NuSMV.