Focus-style proofs for the two-way alternation-free μ-calculus

(joint work with Yde Venema)

Jan Rooduijn

ILLC, University of Amsterdam

WoLLIC, 12 July 2023

Overview

- The (alternation-free) modal μ-calculus
    - Game semantics
    - Focus-style proofs for the alternation-free modal μ-calculus
    - Completeness
- The two-way alternation-free modal μ-calculus
    - Problems for completeness
    - The solution: trace atoms
- Our results
- Conclusion and future work

The modal μ-calculus

- A set P of propositional variables.
- A set D of actions.

$$\varphi ::= p \mid \overline{p} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \langle a \rangle \varphi \mid [a]\varphi \mid \mu x \varphi \mid \nu x \varphi$$

where $\overline{x}$ does not occur in φ.

Given a Kripke model $\mathbb{S} = (S, (R_a)_{a \in \mathrm{D}}, V)$ and a propositional variable x, a formula φ induces a function

$$\begin{aligned} [\![\varphi]\!]^{\mathbb{S}}_x &: \mathcal{P}(S) \to \mathcal{P}(S) \\ &: X \mapsto [\![\varphi]\!]^{\mathbb{S}[x \mapsto X]} \end{aligned}$$

$[\![\eta x \varphi]\!]^{\mathbb{S}}$ is the least/greatest fixed point of $[\![\varphi]\!]^{\mathbb{S}}_x$ ($\eta \in \{\mu, \nu\}$).

The alternation-free fragment

Roughly: a formula φ is *alternation free* if there is no entanglement between μ and ν operators.

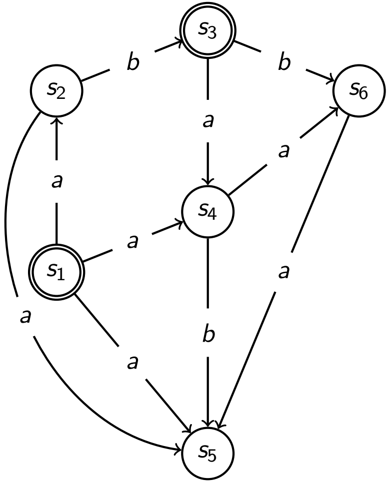
$$\mu x \mu y(\langle a\rangle(x \vee p) \wedge \langle b\rangle y) \qquad \mu x \nu y(\langle a\rangle(x \vee p) \wedge \langle b\rangle y)$$

$$\mu x(\langle a\rangle(x \vee p) \wedge \mu y\langle b\rangle y) \qquad \mu x(\langle a\rangle(x \vee p) \wedge \nu y\langle b\rangle y)$$

- The alternation-free variant is strictly less expressive than the full modal μ-calculus. Many of the proof-theoretical difficulties, however, already manifest themselves on the alternation-free level.
- The alternation-free modal μ-calculus subsumes PDL, CKL and many other extensions of modal logic by fixed point operators.

The evaluation game (example)

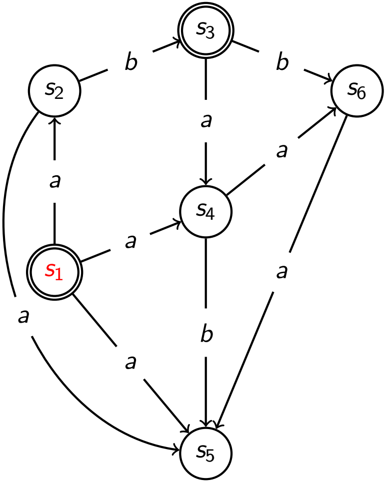
At position (φ, s), player $\exists$ wants to show that φ is true s, while player $\forall$ wishes to show that φ is false at s.



$V(p) = \{s_i : s_i \text{ has a double circle}\}$

The evaluation game (example)

At position (φ, s), player $\exists$ wants to show that φ is true s, while player $\forall$ wishes to show that φ is false at s.

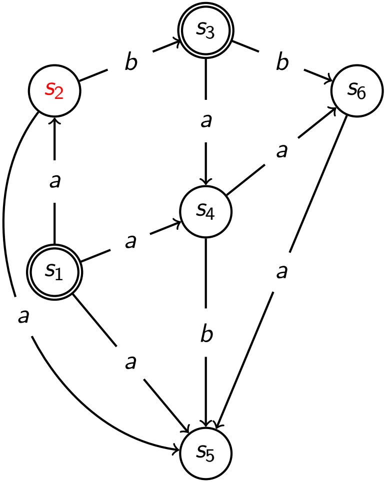


$(\langle a \rangle [b] \mu x (\langle a \rangle x \vee p), s_1)$

$V(p) = \{s_i : s_i \text{ has a double circle}\}$

The evaluation game (example)

At position (φ, s), player $\exists$ wants to show that φ is true s, while player $\forall$ wishes to show that φ is false at s.

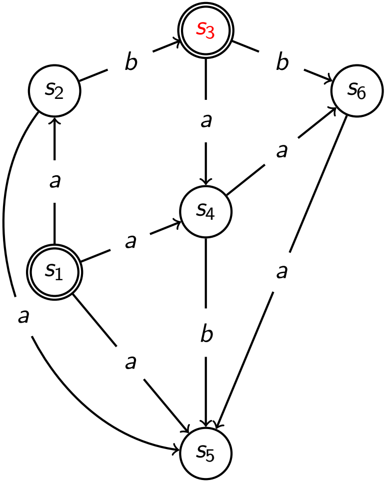


$$(\langle a \rangle [b] \mu x (\langle a \rangle x \vee p), s_1)$$
$$\xrightarrow{\exists} ([b] \mu x (\langle a \rangle x \vee p), s_2)$$

$$V(p) = \{s_i : s_i \text{ has a double circle}\}$$

The evaluation game (example)

At position (φ, s), player $\exists$ wants to show that φ is true s, while player $\forall$ wishes to show that φ is false at s.

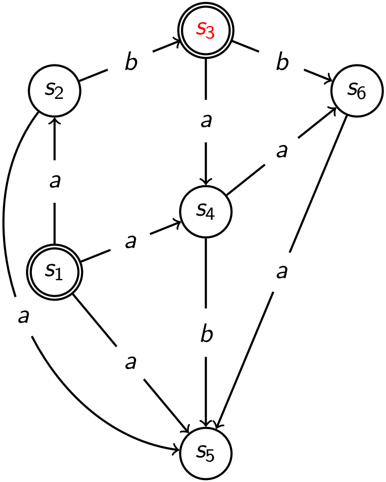


$$(\langle a\rangle[b]\mu x(\langle a\rangle x \vee p), s_1)$$
$$\xrightarrow{\exists} ([b]\mu x(\langle a\rangle x \vee p), s_2)$$
$$\xrightarrow{\forall} (\mu x(\langle a\rangle x \vee p), s_3)$$

$V(p) = \{s_i : s_i \text{ has a double circle}\}$

The evaluation game (example)

At position (φ, s), player $\exists$ wants to show that φ is true s, while player $\forall$ wishes to show that φ is false at s.

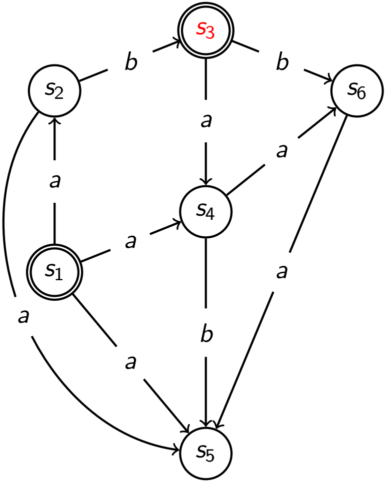


$$(\langle a \rangle [b] \mu x (\langle a \rangle x \vee p), s_1)$$
$$\xrightarrow{\exists} ([b] \mu x (\langle a \rangle x \vee p), s_2)$$
$$\xrightarrow{\forall} (\mu x (\langle a \rangle x \vee p), s_3)$$
$$\xrightarrow{\cdot} (\langle a \rangle \mu x (\langle a \rangle x \vee p) \vee p, s_3)$$

$V(p) = \{s_i : s_i \text{ has a double circle}\}$

The evaluation game (example)

At position (φ, s), player $\exists$ wants to show that φ is true s, while player $\forall$ wishes to show that φ is false at s.



$$(\langle a \rangle [b] \mu x (\langle a \rangle x \vee p), s_1)$$
$$\xrightarrow{\exists} ([b] \mu x (\langle a \rangle x \vee p), s_2)$$
$$\xrightarrow{\forall} (\mu x (\langle a \rangle x \vee p), s_3)$$
$$\xrightarrow{\cdot} (\langle a \rangle \mu x (\langle a \rangle x \vee p) \vee p, s_3)$$
$$\xrightarrow{\exists} (p, s_3)$$

$V(p) = \{s_i : s_i \text{ has a double circle}\}$

The evaluation game (definition)

The game $\mathcal{E}(\xi, \mathbb{S})$ is played on the board $\mathsf{Clos}(\xi) \times S$.

Position	Owner	Admissible moves
$(p, s), s \in V(p)$	$\forall$	$\emptyset$
$(p, s), s \notin V(p)$	$\exists$	$\emptyset$
$(\overline{p}, s), s \notin V(p)$	$\forall$	$\emptyset$
$(\overline{p}, s), s \in V(p)$	$\exists$	$\emptyset$
$(\varphi \vee \psi, s)$	$\exists$	$\{(\varphi, s), (\psi, s)\}$
$(\varphi \wedge \psi, s)$	$\forall$	$\{(\varphi, s), (\psi, s)\}$
$(\langle a \rangle \varphi, s)$	$\exists$	$\{\varphi\} \times R_a[s]$
$([a]\varphi, s)$	$\forall$	$\{\varphi\} \times R_a[s]$
$(\eta x \varphi, s)$	$-$	$\{(\varphi[\eta x \varphi / x], s)\}$

An infinite $\mathcal{E}(\xi, \mathbb{S})$-match is won by $\exists$ if and only if from some point on, every $\eta x \varphi$ is such that $\eta = \nu$.

Example

$\mu x(\langle a \rangle x \vee p) \equiv$ "a p-state is reachable by an a-path"

An annotated proof system (Marti & Venema)

A *sequent* is a finite set Γ consiting of annotated formulas φ^u with $u \in \{\circ, \bullet\}$.

$$\dfrac{}{\varphi^u, \overline{\varphi}^v, \Gamma}\ \mathsf{Ax} \qquad \dfrac{\varphi^u, \psi^u, \Gamma}{\varphi \vee \psi^u, \Gamma}\ \vee \qquad \dfrac{\varphi^u, \Gamma \qquad \psi^u, \Gamma}{\varphi \wedge \psi^u, \Gamma}\ \wedge$$

$$\dfrac{\varphi^u, \Delta}{[a]\varphi^u, \langle a \rangle \Delta, \Gamma}\ [a] \qquad \dfrac{\varphi[\mu x \varphi / x]^\circ, \Gamma}{\mu x \varphi^u, \Gamma}\ \mu \qquad \dfrac{\varphi[\nu x \varphi / x]^u, \Gamma}{\nu x \varphi^u, \Gamma}\ \nu \qquad \dfrac{\Gamma^\bullet}{\Gamma^\circ}\ \mathsf{F}$$

Definition

A non-well-founded derivation is a *proof* if every infinite branch has a final segment on which there is always a formula in focus.

- The (*path-based*) focus system is equivalent to the *trace-based* system.
- The focus annotations allow for a nice soundness condition on cyclic proofs as finite trees with back edges.

The proof search game

The *proof search game* is defined as follows:

- Given a sequent Γ, Prover chooses a rule instance $\dfrac{\Delta_1 \cdots \Delta_n}{\Gamma}\,\mathsf{r}$
- Given a rule instance $\dfrac{\Delta_1 \cdots \Delta_n}{\Gamma}\,\mathsf{r}$, Refuter chooses a sequent Δ_i.
- An infinite match is won by Prover if and only if from some point on, every sequent has a formula in focus.

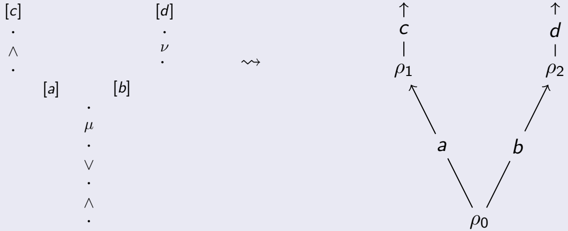
Note: viewed as a tree, a winning strategy for Prover is the same as a proof.

Theorem (Niwinski & Walukiewicz, Marti & Venema)

Every valid sequent Γ *is provable.*

Proof (sketch).

Suppose Γ is not provable. By determinacy, there is a winning strategy T for Refuter in the proof search game. This winning strategy carries a countermodel.



$S^T :=$ {maximal paths ρ in T such that ρ does not pass a modal rule}
$\rho_1 R^T_a \rho_2 :\Leftrightarrow \rho_1$ is connected to ρ_2 by an application of the rule $[a]$
$p \in V^T(\rho) :\Leftrightarrow p$ does *not* occur in a sequent on the path ρ $\square$

The two-way alternation-free modal μ-calculus

- A set P of propositional variables.
- A set D of actions.

Fix an involution operation $\breve{\cdot}$ on D, *i.e.* $a \neq \breve{a}$ and $\breve{\breve{a}} = a$ for every $a \in \mathrm{D}$

$$\varphi ::= p \mid \overline{p} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \langle a \rangle \varphi \mid [a]\varphi \mid \mu x \varphi \mid \nu x \varphi$$

where $\overline{x}$ does not occur in φ.

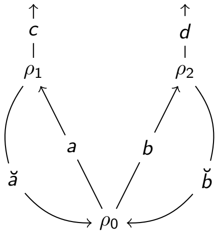
The two-way modal μ-calculus is interpreted over *regular* models:

$$R_{\breve{a}} = \{(t, s) : (s, t) \in R_a\}$$

Example

$\nu x(\langle a \rangle \langle \breve{a} \rangle x) \equiv$ "there is an infinite path of alternating a and $\breve{a}$ transitions"

Problem for completeness



$$(\langle \breve{a} \rangle \psi, \rho_1) \xrightarrow{\exists} (\psi, \rho_0)$$

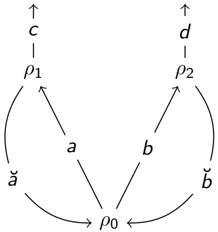
Modal rule for the two-way μ-calculus

$$\dfrac{\varphi, \Delta, [\breve{a}]\Gamma}{[a]\varphi, \langle a\rangle\Delta, \Gamma}\ \mathsf{R}_{[a]} \qquad\qquad \dfrac{\varphi^\circ, \Gamma \qquad \overline{\varphi}^\circ, \Gamma}{\Gamma}\ \mathsf{cut}$$

$$\dfrac{\Gamma_1}{\Gamma_0}\ \mathsf{R}_{[a]}$$

$$\langle\breve{a}\rangle\psi \in \Gamma_1 \Rightarrow [\breve{a}]\overline{\psi} \notin \Gamma_1 \Rightarrow \overline{\psi} \notin \Gamma_0 \Rightarrow \psi \in \Gamma_0$$

Another problem for completeness



If $\langle \breve{a} \rangle \psi^{\bullet}$ occurs in ρ_1, then ψ^{u} occurs in ρ_0. But how do we get $u = \bullet$?

Trace atoms (inspired by Vardi)

Definition

Given φ, ψ, there is a *trace atom* $\varphi \rightsquigarrow \psi$ and a *negated trace atom* $\varphi \not\rightsquigarrow \psi$.

The semantics of trace atoms is defined relative to a strategy for $\forall$.

Definition

Given a strategy f for $\forall$ in $\mathcal{E}$, we say that $\varphi \rightsquigarrow \psi$ is *satisfied* in $\mathbb{S}$ at s with respect to f (and write $\mathbb{S}, s \Vdash_f \varphi \rightsquigarrow \psi$) if there is an f-guided match

$$(\varphi, s) = (\varphi_0, s_0) \cdot (\varphi_1, s_1) \cdots (\varphi_n, s_n) = (\psi, s) \quad (n \geq 0)$$

such that for no $i < n$ the formula φ_i is a μ-formula. We say that $\mathbb{S}$ *satisfies* $\varphi \not\rightsquigarrow \psi$ at s with respect to f (and write $\mathbb{S}, s \Vdash_f \varphi \not\rightsquigarrow \psi$) iff $\mathbb{S}, s \nVdash_f \varphi \rightsquigarrow \psi$.

Some examples

Example

1. $\mu x \varphi \rightsquigarrow \chi$ is only satisfiable if $\chi = \mu x \varphi$.
2. $\nu x \varphi \rightsquigarrow \varphi[\nu x \varphi / x]$ is always true.
3. If $\mathbb{S}, s \Vdash_f \varphi \rightsquigarrow \psi$ and $\mathbb{S}, s \Vdash_f \psi \rightsquigarrow \varphi$ for some $\varphi \neq \psi$, then $\mathbb{S}, s \Vdash_f \varphi$.
4. $\mathbb{S}, s \Vdash_f \varphi \rightsquigarrow \langle a \rangle \psi$ implies $\mathbb{S}, t \Vdash_f \langle \breve{a} \rangle \varphi \rightsquigarrow \psi$ for every a-successor t of s.

The key lemma

Lemma

Let $\rho \in S^T$. Suppose $\mathbb{S}^T, \rho \Vdash_f \varphi \rightsquigarrow \psi$. Then $\varphi \not\rightarrowtail \psi$ occurs in ρ.

$$
\begin{tikzcd}
\rho_0 \arrow[r] \arrow[loop below] & \rho_1 \arrow[r] \arrow[loop below] & \rho_2 \arrow[r] \arrow[loop below] & \cdots
\end{tikzcd}
$$

Results

Let Γ be a sequent consisting of annotated formulas φ^u with $u \in \{\circ, \bullet\}$), trace atoms $\varphi \rightsquigarrow \psi$, and negated trace atoms $\varphi \not\rightsquigarrow \psi$.

Theorem (Soundness)

If Γ is provable, then for every model $\mathbb{S}$, state s of $\mathbb{S}$ and optimal positional strategy f for $\forall$ in $\mathcal{E}$, there is an $A \in \Gamma$ such that $\mathbb{S}, s \Vdash_f A$.

Let Γ^- be the set of annotated formulas in Γ (so we remove the trace atoms).

Theorem (Completeness)

If Γ^- is valid, then Γ is provable.

Remark

The infinitary proof system naturally restricts to a finitary cyclic system.

Corollary

The two-way alternation-free modal μ-calculus is decidable and has the regular tree model property.

Future work

- Completeness for all sequents, *e.g.* $\{\varphi_1 \wedge \varphi_2 \rightsquigarrow \varphi_1, \varphi_1 \wedge \varphi_2 \rightsquigarrow \varphi_2\}$.
- Craig interpolation
- Incorporating trace atoms in the syntax?
- Extending this system to the full two-way modal μ-calculus (*i.e.* with alternation)

Thank you

https://staff.fnwi.uva.nl/j.m.w.rooduijn/

$$\frac{}{\varphi^u, \overline{\varphi}^v, \Gamma}\ \mathsf{Ax1} \qquad \frac{}{\varphi \rightsquigarrow \psi, \varphi \not\rightsquigarrow \psi, \Gamma}\ \mathsf{Ax2} \qquad \frac{}{\varphi \rightsquigarrow \varphi, \Gamma}\ \mathsf{Ax3}$$

$$\frac{(\varphi \vee \psi) \not\rightsquigarrow \varphi, (\varphi \vee \psi) \not\rightsquigarrow \psi, \varphi^u, \psi^u, \Gamma}{\varphi \vee \psi^u, \Gamma}\ \mathsf{R}_\vee \qquad \frac{\varphi^\circ, \Gamma \qquad \overline{\varphi}^\circ, \Gamma}{\Gamma}\ \mathsf{cut}$$

$$\frac{(\varphi \wedge \psi) \not\rightsquigarrow \varphi, \varphi^u, \Gamma \qquad (\varphi \wedge \psi) \not\rightsquigarrow \psi, \psi^u, \Gamma}{\varphi \wedge \psi^u, \Gamma}\ \mathsf{R}_\wedge \qquad \frac{\varphi[\mu x \varphi / x]^\circ, \Gamma}{\mu x \varphi^u, \Gamma}\ \mathsf{R}_\mu$$

$$\frac{\nu x \varphi \not\rightsquigarrow \varphi[\nu x \varphi / x], \varphi[\nu x \varphi / x] \rightsquigarrow \nu x \varphi, \varphi[\nu x \varphi / x]^u, \Gamma}{\nu x \varphi^u, \Gamma}\ \mathsf{R}_\nu \qquad \frac{\Gamma^{[a]\varphi^u}}{[a]\varphi^u, \Gamma}\ \mathsf{R}_{[a]}$$

$$\frac{\Gamma^\bullet}{\Gamma^\circ}\ \mathsf{F} \qquad \frac{\varphi \not\rightsquigarrow \psi, \psi \not\rightsquigarrow \chi, \varphi \not\rightsquigarrow \chi, \Gamma}{\varphi \not\rightsquigarrow \psi, \psi \not\rightsquigarrow \chi, \Gamma}\ \mathsf{trans} \qquad \frac{\varphi \rightsquigarrow \psi, \Gamma \qquad \varphi \not\rightsquigarrow \psi, \Gamma}{\Gamma}\ \mathsf{tc}$$

Definition

Let Γ be a sequent and let $[a]\varphi^b$ be an annotated formula. The *jump* $\Gamma^{[a]\varphi^b}$ of Γ with respect to $[a]\varphi^b$ consists of:

1.
   1. $\varphi^{s([a]\varphi,\Gamma)}$;
   2. $\psi^{s(\langle a\rangle\psi,\Gamma)}$ for every $\langle a\rangle\psi^c \in \Gamma$;
   3. $[\breve{a}]\chi^\circ$ for every $\chi^d \in \Gamma$ such that $[\breve{a}]\chi \in \Sigma$;
2.
   1. $\varphi \rightsquigarrow \langle\breve{a}\rangle\chi$ for every $[a]\varphi \rightsquigarrow \chi \in \Gamma$ such that $\langle\breve{a}\rangle\chi \in \Sigma$;
   2. $\langle\breve{a}\rangle\chi \not\rightarrow \varphi$ for every $\chi \not\rightarrow [a]\varphi \in \Gamma$ such that $\langle\breve{a}\rangle\chi \in \Sigma$;
   3. $\psi \rightsquigarrow \langle\breve{a}\rangle\chi$ for every $\langle a\rangle\psi \rightsquigarrow \chi \in \Gamma$ such that $\langle\breve{a}\rangle\chi \in \Sigma$;
   4. $\langle\breve{a}\rangle\chi \not\rightarrow \psi$ for every $\chi \not\rightarrow \langle a\rangle\psi \in \Gamma$ such that $\langle\breve{a}\rangle\chi \in \Sigma$.

where $s(\xi,\Gamma)$ is defined by:

$$s(\xi,\Gamma) = \begin{cases} \bullet & \text{if } \xi^\bullet \in \Gamma, \\ \bullet & \text{if } \theta \not\rightarrow \xi \in \Gamma \text{ for some } \theta^\bullet \in \Gamma \\ \circ & \text{otherwise.} \end{cases}$$

When taking the strategy tree T, we assume that Prover adheres to the following non-deterministic strategy:

- Only apply a modal rule when all of the propositional rules are exhausted.
- Apply the rule F whenever possible.

The canonical strategy f for $\forall$ in $\mathcal{E}(\Gamma, \mathbb{S}^T)$ is given by:

- At $(\varphi \wedge \psi, \rho)$ choose the conjunct corresponding to the choice of Refuter when $\varphi \wedge \psi$ is principal in an application of the rule $\wedge$ in ρ.
- At $([a]\varphi, \rho)$ choose an a-successor ρ' of ρ such that ρ and ρ' are separated by an application of $[a]$.

Example

Define $\varphi := \nu x \langle a \rangle \langle \breve{a} \rangle x$, *i.e.* φ expresses that there is an infinite path of alternating a and $\breve{a}$ transitions. Clearly this holds at every state with an a-successor. Hence the implication $\langle a \rangle p \to \varphi$ is valid. As context Σ we consider the least negation-closed set containing both $\langle a \rangle p$ and φ, *i.e.*,

$$\{\langle a \rangle p, p, \varphi, \langle a \rangle \langle \breve{a} \rangle \varphi, \langle \breve{a} \rangle \varphi, [a]\overline{p}, \overline{p}, \overline{\varphi}, [a][\breve{a}]\overline{\varphi}, [\breve{a}]\overline{\varphi}\}.$$

The following is a Focus^2_∞-proof of $\langle a \rangle p \to \varphi$.

$$\dfrac{\dfrac{\dfrac{}{\overline{p}^\bullet, \langle \breve{a} \rangle \varphi^\bullet, \langle \breve{a} \rangle \varphi \not\rightsquigarrow \langle \breve{a} \rangle \varphi, \langle \breve{a} \rangle \varphi \rightsquigarrow \langle \breve{a} \rangle \varphi}\text{Ax2}}{[a]\overline{p}^\bullet, \langle a \rangle \langle \breve{a} \rangle \varphi^\bullet, \varphi \not\rightsquigarrow \langle a \rangle \langle \breve{a} \rangle \varphi, \langle a \rangle \langle \breve{a} \rangle \varphi \rightsquigarrow \varphi}\text{R}_{[a]}}{[a]\overline{p}^\bullet, \varphi^\bullet}\text{R}_\nu$$

Note that it is also possible to use Ax3 instead of Ax2 in the above proof.