

Verifying Temporal Properties using Explicit Approximants: Completeness for Context-free Processes

Joint work with Alex Simpson.

Verifying Properties

Sequent calculus for verifying μ -calculus properties

$$\Gamma \vdash \Delta$$

- Γ and Δ contain **verification assertions** $p:\varphi$
- Applicable to a wide class of process algebras by using **transition assertions** $p \xrightarrow{a} q$
- Parameterized verification goals

$$x_1:\varphi_1, \dots, x_k:\varphi_k \vdash p(x_1, \dots, x_k):\varphi$$

- Compositional reasoning

$$\frac{\vdash p(q_1, q_2):\varphi}{\vdash q_1:\psi_1 \quad \vdash q_2:\psi_2 \quad x_1:\psi_1, x_2:\psi_2 \vdash p(x_1, x_2):\varphi}$$

Explicit Approximants

μ -calculus in positive normal form:

$$\varphi ::= X \mid \mathbf{ff} \mid \mathbf{tt} \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \\ \mid \langle a \rangle \varphi \mid [a] \varphi \mid \mu X. \varphi \mid \nu X. \varphi$$

Free propositional variables are interpreted as fixed-point approximants:

Approximants of $\mu X. \varphi$:

$$\emptyset \subseteq \varphi(\emptyset) \subseteq \varphi^2(\emptyset) \subseteq \dots \subseteq \varphi^\omega(\emptyset) \subseteq \dots = \mu X. \varphi$$

Approximants of $\nu X. \varphi$:

$$T \supseteq \varphi(T) \supseteq \varphi^2(T) \supseteq \dots \supseteq \varphi^\omega(T) \supseteq \dots = \nu X. \varphi$$

Use a **declaration context** D to record the definitions:

$$D; \Gamma \vdash \Delta$$

Explicit Approximants

Extended syntax to work with approximants:

$$\Phi ::= \varphi \mid \langle X \leq \varphi \rangle \Phi \mid [X \geq \varphi] \Phi \mid \langle -X \rangle \Phi \mid [+X] \Phi$$

Binders:

$\langle X \leq \psi \rangle \Phi$: Φ holds for some μ -approximant X

$[X \geq \psi] \Phi$: Φ holds for all ν -approximants X

$$[X \geq \varphi] \varphi \equiv \varphi[\nu X. \varphi / X] \equiv \nu X. \varphi$$

Modification modalities:

$\langle -X \rangle \Phi$: $\Phi[X' / X]$ for some μ -approximant $X' \subset X$

$[+X] \Phi$: $\Phi[X' / X]$ for all ν -approximants $X' \supset X$

If X is an approximant of $\nu X. \varphi$, then:

$$X \equiv [+X] \varphi$$

Fixed-point Rules

Fixed-point rules

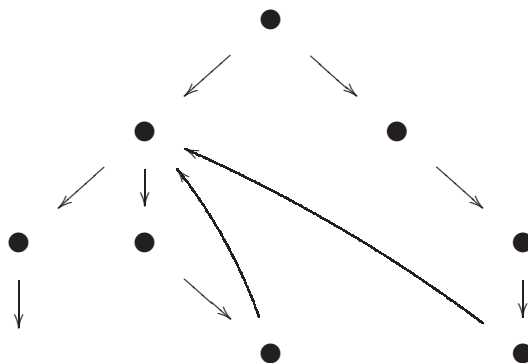
$$\begin{array}{c}
 \frac{\mathbb{D}; \Gamma, p: \nu X. \varphi \vdash \Delta}{\mathbb{D}; \Gamma, p: [X \geq \varphi] \varphi \vdash \Delta} \qquad \frac{\mathbb{D}; \Gamma \vdash \Delta, p: \nu X. \varphi}{\mathbb{D}; \Gamma \vdash \Delta, p: [X \geq \varphi] \varphi} \\
 \\
 \frac{\mathbb{D}; \Gamma, p: [X \geq \varphi] \Phi \vdash \Delta}{\mathbb{D}; \Gamma, p: \Phi[\nu X. \varphi / X] \vdash \Delta} \qquad \frac{\mathbb{D}; \Gamma \vdash \Delta, p: [X \geq \varphi] \Phi}{\mathbb{D}; \Gamma \vdash \Delta, p: \Phi[\nu X. \varphi / X]}
 \end{array}$$

Approximant rules

$$\begin{array}{c}
 \frac{\mathbb{D}, X \geq \varphi; \Gamma, p: [X \geq \varphi] \Phi \vdash \Delta}{\mathbb{D}, X \geq \varphi; \Gamma, p: \Phi \vdash \Delta} \qquad \frac{\mathbb{D}; \Gamma \vdash \Delta, p: [X \geq \varphi] \Phi}{\mathbb{D}, X \geq \varphi; \Gamma \vdash \Delta, p: \Phi} \overset{X}{\text{fresh}} \\
 \\
 \frac{\mathbb{D}, X \geq \varphi; \Gamma, p: X \vdash \Delta}{\mathbb{D}, X \geq \varphi; \Gamma, p: [+X] \varphi \vdash \Delta} \qquad \frac{\mathbb{D}, X \geq \varphi; \Gamma \vdash \Delta, p: X}{\mathbb{D}, X \geq \varphi; \Gamma \vdash \Delta, p: [+X] \varphi} \\
 \\
 ([+X]) \frac{\mathbb{D}, X \geq \varphi; [+X] \Gamma, \Gamma' \vdash [+X] \Delta, \Delta'}{\mathbb{D}, X \geq \varphi; \Gamma, \Gamma' \vdash \Delta, \Delta'} \quad \Delta \neq \emptyset, \text{cond.}
 \end{array}$$

Proof

A derivation tree in which each leaf is a repeat of some inner node is a **pre-proof**.



A path **preserves** X if X occurs in all declaration contexts.

X **progresses** along the path if the path preserves X and the rule $([+X])$ is applied along that path.

A pre-proof is a **proof** if every infinite path progresses infinitely often on some X .

Completeness

Closed process term p_0 , closed μ -calculus formula φ_0 .

$$p_0 \models \varphi_0$$

Construct a derivation with root $\vdash p_0 : \varphi_0$.

We have to

1. Make choices, e.g. in $(\forall R)$, $(\langle a \rangle R)$.
2. Find repeats.
3. Satisfy global condition.

Use Stirling's property-checking games:
 "Let the players do the work."

Games provide 1. (the choices made by the players)
 and 3. (the winning condition).

We "only" have to ensure 2.

Property Checking Games

- Two players: **Verifier** and **Refuter**
- A **play** is a finite or infinite sequence of **positions**

$$(s_0, E_0, \varphi_0)(s_1, E_1, \varphi_1) \dots (s_n, E_n, \varphi_n) \dots$$

where s_i is a state in some transition system, φ_i is a formula, and E_i is the list of fixed point definitions for all free variables of φ_i in dependency order.

- A play is produced by **moves**
 - **ff**: **Verifier** is stuck
 - $\psi_1 \vee \psi_2$: **Verifier** chooses ψ_i : (s, E', ψ_i)
 - $\langle a \rangle \psi$: **Verifier** chooses $s \xrightarrow{a} s'$: $(s', E, \langle a \rangle \psi)$
 - $\mu X. \psi$: **Verifier** chooses: $(s, E, \psi[\mu X. \psi / X])$
 - **tt**: **Refuter** is stuck
 - $\psi_1 \wedge \psi_2$: **Refuter** chooses ψ_i : (s, E', ψ_i)
 - $[a] \psi$: **Refuter** chooses $s \xrightarrow{a} s'$: $(s', E, [a] \psi)$
 - $\nu X. \psi$: **Refuter** chooses: $(s, E, X = \psi, \psi)$
 - X : **Refuter** chooses: (s, E, ψ)

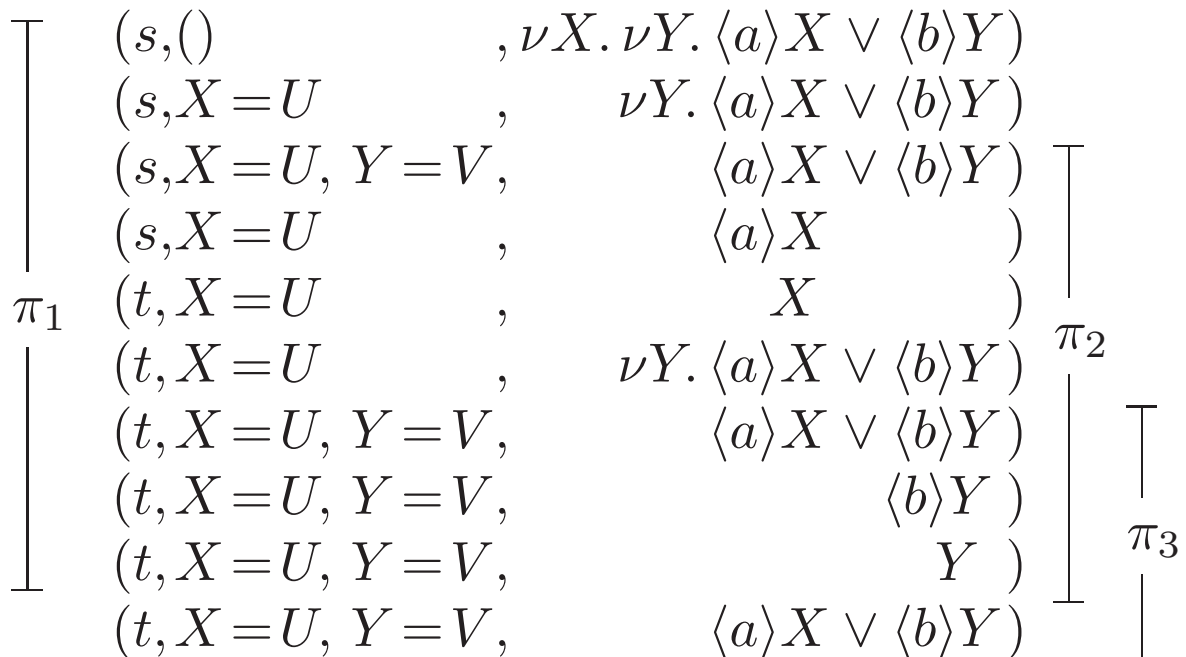
Preservation, Progress

Play $\pi = (s_0, E_0, \varphi_0)(s_1, E_1, \varphi_1) \dots$

A fixed-point variable X is **preserved** by π if X is defined in all E_i .

A fixed-point variable X **progresses** along π if X is preserved by π and π contains a move away from (s_n, E_n, X) .

Example: $U = \nu Y. \langle a \rangle X \vee \langle b \rangle Y, V = \langle a \rangle X \vee \langle b \rangle Y$.



π_1 : no preservation/progress

π_2 : X is preserved, X progresses

π_3 : X and Y are preserved, Y progresses

Property Checking Games

The **game** $G(p, \varphi)$ is played beginning with $(p, (), \varphi)$.

Winning Condition:

Verifier wins a *finite* play if Refuter is stuck.

She wins an *infinite* play π if there exists an X which **progresses infinitely often** along some tail of π .

Theorem (Stirling). *If $p \models \varphi$ then Verifier has a history-free winning strategy for the game $G(p, \varphi)$.*

From now on:

- Fix a history-free winning strategy for Verifier for the game $G(p_0, \varphi_0)$.
- Consider only **V-plays**, i.e. plays of $G(p_0, \varphi_0)$ in which Verifier plays her winning strategy

Building the derivation along V-plays

- $(p, E, \psi_1 \vee \psi_2)$: **Verifier** chooses a disjunct ψ_i .

$$\frac{D_E; \vdash p:\psi_1 \vee \psi_2}{D_E; \vdash p:\psi_1, p:\psi_2} (\vee R) \quad (p, E, \psi_1 \vee \psi_2)$$

$$\frac{D_E; \vdash p:\psi_1, p:\psi_2}{D_{E'}; \vdash p:\psi_i} (\text{Weak}) \quad (p, E', \psi_i)$$

- $(p, E, \psi_1 \wedge \psi_2)$: **Refuter** may choose either conjunct.

$$\frac{(p, E, \psi_1 \wedge \psi_2) \quad D_E; \vdash p:\psi_1 \wedge \psi_2}{D_E; \vdash p:\psi_1, D_E; \vdash p:\psi_2} (\wedge R) \quad (p, E, \psi_1 \wedge \psi_2)$$

$$\frac{D_E; \vdash p:\psi_1}{D_{E'}; \vdash p:\psi_1} (\text{Weak}) \quad \frac{D_E; \vdash p:\psi_2}{D_{E'}; \vdash p:\psi_2} (\text{Weak}) \quad (p, E', \psi_1) \quad (p, E', \psi_2)$$

Building the derivation along V-plays

- $(p, E, \nu X. \psi)$ **Refuter** has to choose $(p, E, X = \psi, \psi)$.

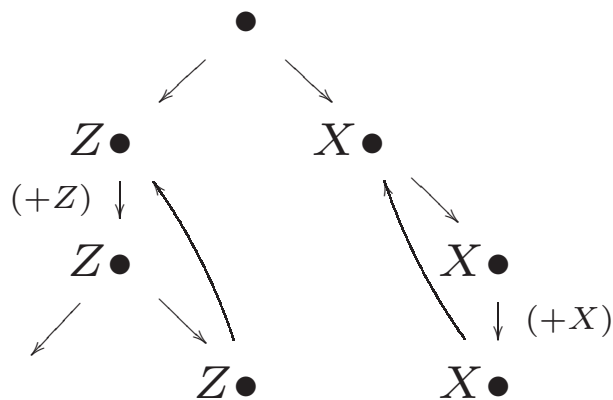
$$\frac{\frac{D_E; \vdash p: \nu X. \psi}{D_E; \vdash p: [X \geq \psi] \psi}}{D_{E, X = \psi}; \vdash p: \psi} \quad \begin{array}{l} (p, E, \nu X. \psi) \\ (p, E, X = \psi, \psi) \end{array}$$

- (p, E, X) : **Refuter** has to choose (p, E, ψ) where $X = \psi \in E$.

$$\frac{\frac{D_E; \vdash p: X}{D_E; \vdash p: [+X] \psi}}{D_E; \vdash p: \psi} \quad \begin{array}{l} (p, E, X) \\ ([+X]) \\ (p, E, \psi) \end{array}$$

Finite State Completeness

This builds a derivation tree for $\vdash p_0 : \varphi_0$ in steps.
 Continue construction until the derivation is of the following form:



- Each leaf is repeat of some sequent on the unique path from the root to that leaf
- The path between a repeat and its companion progresses on some X

This is possible because:

- Each path between steps corresponds to a V-play and inherits preservation and progress.
- ⇒ Winning condition transfers from V-play to path.
 (Every V-play is won by Verifier!)
- ⇒ Since there are repeats (finite state!), this ensures the existence of repeats of the form above

Completeness for Context-free processes

Context-free processes:

- Finite set of **nonterminals**: $\Sigma = \{P, Q, \dots\}$
- Finite set \mathcal{P} of **productions**: $P \xrightarrow{a} p$ where $p \in \Sigma^*$

Transition system $(T, \{\xrightarrow{a}\}_{a \in A})$:

- States: Σ^*
- $Pq \xrightarrow{a} pq$ if $P \xrightarrow{a} p \in \mathcal{P}$

Infinite state \Rightarrow Cannot always find repeats:

Process: $P \xrightarrow{a} PP, P \xrightarrow{b} \varepsilon$

Transition system:

$$\varepsilon \xleftarrow[b]{a} P \xrightleftharpoons[b]{a} PP \xrightleftharpoons[b]{a} PPP \xrightleftharpoons[b]{a} \dots$$

Decomposition

Consider only sequents of the form

$$D; x : \Psi_1, \dots, x : \Psi_n \vdash px : \Phi$$

Start the derivation with

$$\frac{}{; \vdash p : \varphi} \text{ (Cut)}$$

$$\frac{}{; \vdash \varepsilon : \psi} \text{ (Sub)}$$

$$\frac{}{; \varepsilon : \psi \vdash p : \varphi} \text{ (Cut)}$$

$$\frac{}{; x : \psi \vdash px : \varphi} \text{ (Sub)}$$

Decompose processes eagerly:

$$\frac{}{D; x : \psi \vdash Pqx : \varphi} \text{ (Cut)}$$

$$\frac{}{D; x : \psi \vdash qx : \theta} \text{ (Sub)}$$

$$\frac{}{D; qx : \theta \vdash Pqx : \varphi} \text{ (Cut)}$$

$$\frac{}{D; x : \theta \vdash Px : \varphi} \text{ (Sub)}$$

Only finitely many process terms of the form Px .

Decomposition and Completeness

$$D; x : \Psi_1, \dots, x : \Psi_n \vdash p x : \Phi$$

Use the same game-based construction as before:

- Build a derivation along V-plays such that paths inherit preservation and progress from plays.
- Use the winning condition of the V-plays to choose good repeats.

This raises a lot of questions:

- Does the constructions with plays work in presence of (Cut) and (Sub)?
- How do terms $P x$ correspond to the states in plays?
- What are the assumptions Ψ_i ?
- Are preservation and progress reflected in paths?
- Are there repeats?

Decomposition

$$\begin{array}{c}
 (\mathbf{P} \mathbf{P} \mathbf{q}, \mathbf{E}, \mathbf{X}) \\
 | ? \\
 (\mathbf{P} \mathbf{q}, \mathbf{E}, ?)
 \end{array}
 \frac{
 \begin{array}{c}
 \vdots \\
 \mathbf{X} \geq \mathbf{U}, \mathbf{Y} \geq \mathbf{V}; \mathbf{x} : \Psi \vdash \mathbf{P} \mathbf{P} \mathbf{x} : \mathbf{X}
 \end{array}
 }{
 \begin{array}{c}
 \mathbf{X} \geq \mathbf{U}, \mathbf{Y} \geq \mathbf{V}; \mathbf{x} : \Psi \vdash \mathbf{P} \mathbf{x} : ? \quad \mathbf{X} \geq \mathbf{U}, \mathbf{Y} \geq \mathbf{V}; \mathbf{x} : ? \vdash \mathbf{P} \mathbf{x} : \mathbf{X}
 \end{array}
 }
 \begin{array}{c}
 (\mathbf{P} \mathbf{P} \mathbf{q}, \mathbf{E}, \mathbf{X}) \\
 (\mathbf{P} \mathbf{P} \mathbf{q}, \mathbf{E}, \mathbf{X})
 \end{array}$$

$$U = \nu Y. \langle a \rangle X \vee \langle b \rangle Y, \quad V = \langle a \rangle X \vee \langle b \rangle Y, \quad \varepsilon \xleftarrow[b]{a} P \xrightleftharpoons[b]{a} PP \xrightleftharpoons[b]{a} PPP \xrightleftharpoons[b]{a} \dots$$

Decomposition

$$\begin{array}{c}
 (\mathbf{P P q}, \mathbf{E}, X) \\
 | ? \\
 (\mathbf{P q}, \mathbf{E}, ?)
 \end{array}
 \frac{
 \begin{array}{c}
 \vdots \\
 X \geq U, Y \geq V; x: \Psi \vdash \mathbf{P P} x: X \\
 \hline
 X \geq U, Y \geq V; x: \Psi \vdash \mathbf{P} x: ? \\
 \hline
 X \geq U, Y \geq V; x: ? \vdash \mathbf{P} x: X \\
 \hline
 X \geq U, Y \geq V; x: ? \vdash \mathbf{P} x: [+X] U \\
 \hline
 X \geq U, Y \geq V; x: ? \vdash \mathbf{P} x: U \\
 \hline
 X \geq U; x: ? \vdash \mathbf{P} x: [Y \geq V] V \\
 \hline
 X \geq U, Y \geq V; x: ? \vdash \mathbf{P} x: V \\
 \hline
 X \geq U, Y \geq V; x: ? \vdash \mathbf{P} x: \langle b \rangle Y \\
 \hline
 X \geq U, Y \geq V; x: ? \vdash x: Y
 \end{array}
 }{
 \begin{array}{c}
 (\mathbf{P P q}, \mathbf{E}, X) \\
 (\mathbf{P P q}, \mathbf{E}, X) \\
 | \\
 (\mathbf{P P q}, \mathbf{E}, U) \\
 | \\
 (\mathbf{P P q}, \mathbf{E}, V) \\
 | \\
 (\mathbf{P P q}, \mathbf{E}, \langle b \rangle Y) \\
 (\mathbf{P q}, \mathbf{E}, Y)
 \end{array}
 }$$

$$U = \nu Y. \langle a \rangle X \vee \langle b \rangle Y, \quad V = \langle a \rangle X \vee \langle b \rangle Y, \quad \varepsilon \xleftarrow[b]{a} \mathbf{P} \xrightleftharpoons[b]{a} \mathbf{P P} \xrightleftharpoons[b]{a} \mathbf{P P P} \xrightleftharpoons[b]{a} \dots$$

Decomposition

$$\begin{array}{c}
 (\mathbf{P P q}, \mathbf{E}, X) \\
 | \pi \\
 (\mathbf{P q}, \mathbf{E}, Y)
 \end{array}
 \frac{
 \begin{array}{c}
 \vdots \\
 X \geq U, Y \geq V; x: \Psi \vdash \mathbf{P P} x: X \\
 \hline
 X \geq U, Y \geq V; x: \Psi \vdash \mathbf{P} x: Y \quad X \geq U, Y \geq V; x: Y \vdash \mathbf{P} x: X \\
 \hline
 X \geq U, Y \geq V; x: Y \vdash \mathbf{P} x: [+X] U \\
 \hline
 X \geq U, Y \geq V; x: Y \vdash \mathbf{P} x: U \\
 \hline
 X \geq U; x: Y \vdash \mathbf{P} x: [Y \geq V] V \\
 \hline
 X \geq U, Y \geq V; x: Y \vdash \mathbf{P} x: V \\
 \hline
 X \geq U, Y \geq V; x: Y \vdash \mathbf{P} x: \langle b \rangle Y \\
 \hline
 X \geq U, Y \geq V; x: Y \vdash x: Y
 \end{array}
 }{
 \begin{array}{c}
 (\mathbf{P P q}, \mathbf{E}, X) \\
 (\mathbf{P P q}, \mathbf{E}, X) \\
 (\mathbf{P q}, \mathbf{E}, Y)
 \end{array}
 }
 \begin{array}{c}
 \\
 \\
 \pi \\
 \\
 \\
 \\
 \end{array}$$

π is

$$\begin{array}{l}
 (\mathbf{P P q}, X=U, X) \\
 (\mathbf{P P q}, X=U, \nu Y. \langle a \rangle X \vee \langle b \rangle Y) \\
 (\mathbf{P P q}, X=U, Y=V, \langle a \rangle X \vee \langle b \rangle Y) \\
 (\mathbf{P P q}, X=U, Y=V, \langle b \rangle Y) \\
 (\mathbf{P q}, X=U, Y=V, Y)
 \end{array}
 \quad
 \begin{array}{l}
 U = \nu Y. \langle a \rangle X \vee \langle b \rangle Y \\
 V = \langle a \rangle X \vee \langle b \rangle Y
 \end{array}$$

Decomposition

$$\frac{
 \frac{
 \frac{
 X, Y; x: \Psi \vdash \mathbf{P} \mathbf{P} x: X
 }{
 X, Y; x: \Psi \vdash \mathbf{P} x: [+X] [Y \geq V] Y
 }
 }{
 X; x: \Psi \vdash \mathbf{P} x: [Y \geq V] Y
 }
 }{
 X, Y; x: \Psi \vdash \mathbf{P} x: Y
 }
 \quad
 X, Y; x: \underbrace{[+X] [Y \geq V] Y}_{\chi(\pi)} \vdash \mathbf{P} x: X
 }{
 }$$

where π is the V-Play $(\mathbf{P} \mathbf{P} \mathbf{q}, E, X) \dots (\mathbf{P} \mathbf{q}, E, Y)$.

⇒ Enough assumptions in the right-hand branch

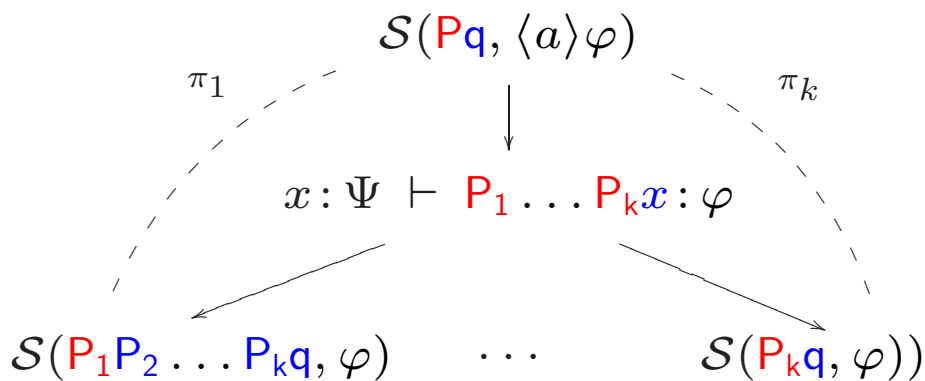
⇒ Each of the two paths reflect preservation and progress of V-plays

In general use the following **canonical sequents**, of which are **only finitely many**.

$$D_E; \{ x: \chi(\pi) \mid \text{V-play } \pi = (\mathbf{P} \mathbf{q}, E, \varphi) \dots (\mathbf{q}, E', \theta) \} \vdash \mathbf{P} x: \varphi,$$

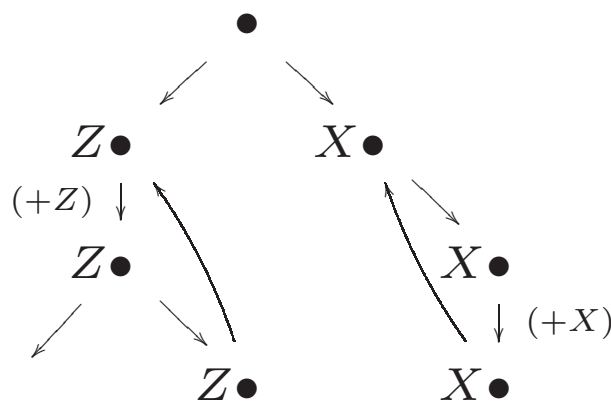
Completeness for Context-free Processes

Build the derivation in steps between canonical sequents, e.g.



Paths inherit Preservation and Progress from the corresponding V-plays π_i .

Using the winning condition we can choose repeats of the form: (finitely many sequents!)



This pre-proof is a proof.

Happy End.