On Extension of Parameterized Coinduction

Masaki Hara

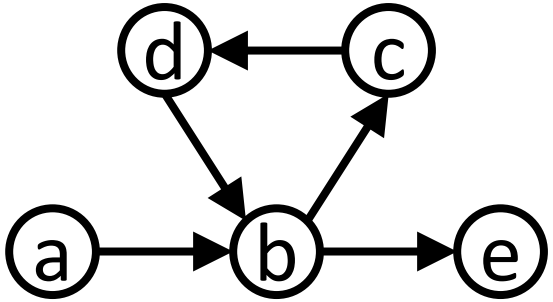
Department of Information Science, Faculty of Science, University of Tokyo

Background

Formal Verification of (Co)Inductive Properties using Proof Assistants

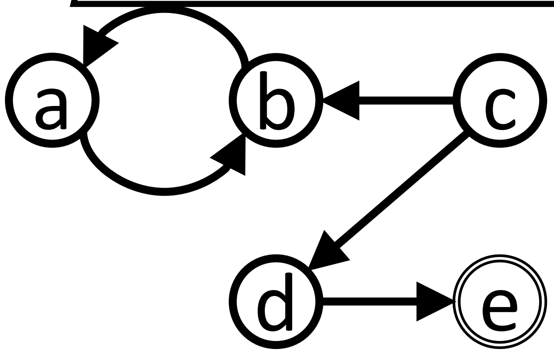
Background

Formal Verification of (Co)Inductive Properties using Proof Assistants



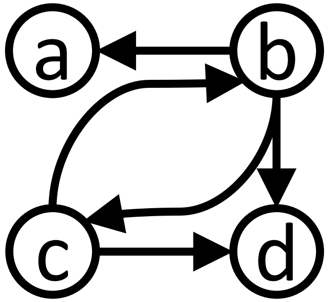
Infinite Path

$\{a\} \subseteq \nu Z. \diamond Z$



Reachability

$\{c\} \subseteq \mu Z. \{e\} \cup \diamond Z$



Bisimulation

$\{(b, c)\} \subseteq \nu R. \operatorname{sim}(R)$

[Hur *et al.*, POPL '13]

Parameterized coinduction
for coinductive properties

Parameterized induction
for inductive properties

No-discovery characterization

How convenient is it?
Mathematical characterization

Our
contribution

[Hur *et al.*, POPL '13]

Parameterized coinduction
for coinductive properties

Parameterized induction
for inductive properties

No-discovery characterization

How convenient is it?
Mathematical characterization

Our
contribution

Complete lattice and monotone function

Def.

$(C, \sqsubseteq)$: complete lattice *i.e.*

- $\forall A \subseteq C.\ \forall x \in C.\ x \sqsubseteq \sqcap A \Leftrightarrow (\forall y \in A.\ x \sqsubseteq y)$
- $\forall A \subseteq C.\ \forall x \in C.\ \bigsqcup A \sqsubseteq x \Leftrightarrow (\forall y \in A.\ y \sqsubseteq x)$
- $x \sqcup y = \bigsqcup\{x, y\}, \bot = \bigsqcup \emptyset$
- $x \sqcap y = \sqcap \{x, y\}, \top = \sqcap \emptyset$

$f : C \to C$: monotone *i.e.*

- $\forall x, y \in C.\ x \sqsubseteq y \Rightarrow f(x) \sqsubseteq f(y)$

Tarski coinduction

Def.

$\nu f = \max\{x \in C \mid x = f(x)\}$ greatest fixpoint

Lem.

$f(\nu f) = \nu f$

$\forall x.\ x \sqsubseteq f(x) \Rightarrow x \sqsubseteq \nu f$ (Tarski)

Coq's built-in coinduction

Parameterized coinduction [Hur *et al.*, POPL '13]

Def.

$$G_f(x) = \nu y.\ f(x \sqcup y)$$ parameterized greatest fixpoint

Lem.

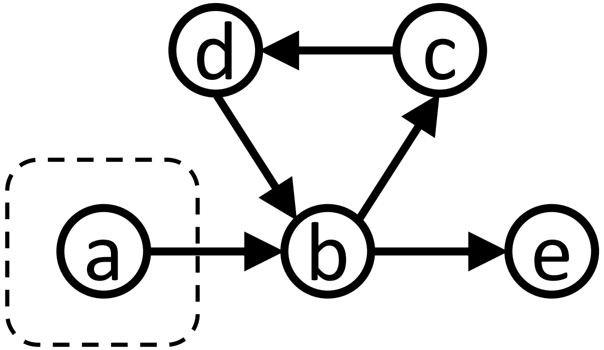
$\forall x, y \in C.\ y \sqsubseteq f\left(x \sqcup G_f(x)\right) \Rightarrow y \sqsubseteq G_f(x)$ (Unfolding)

$\forall x, y \in C.\ y \sqsubseteq G_f(x \sqcup y) \Rightarrow y \sqsubseteq G_f(x)$ (Accumulation)

Implemented on Coq in [Hur *et al.*, POPL '13]

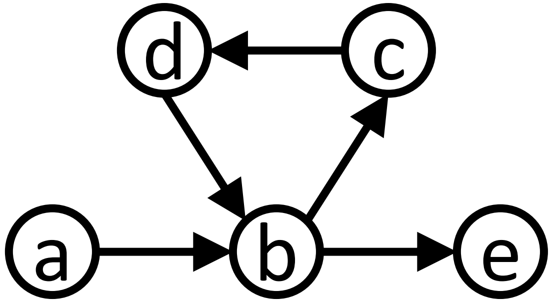
Example

Tarski



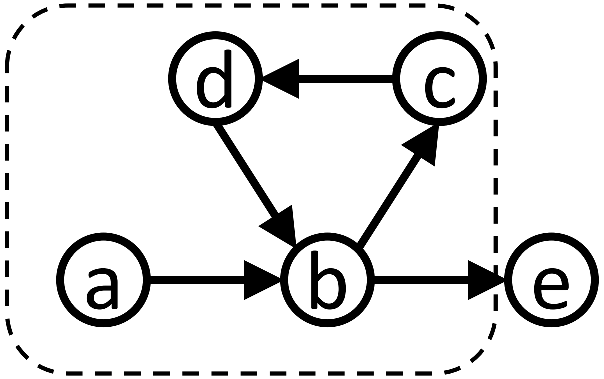
$\{a\} \subseteq \nu Z. \diamond Z$

PaCo



Example

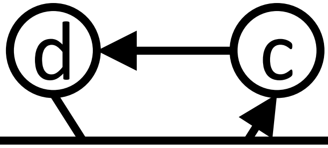
Tarski



$\{a\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$

PaCo



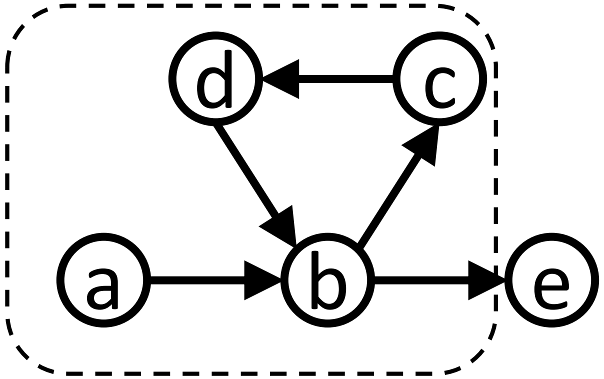
Transitivity

$x \sqsubseteq \nu f$

$\Leftarrow x \sqsubseteq x', x' \sqsubseteq \nu f$

Example

Tarski

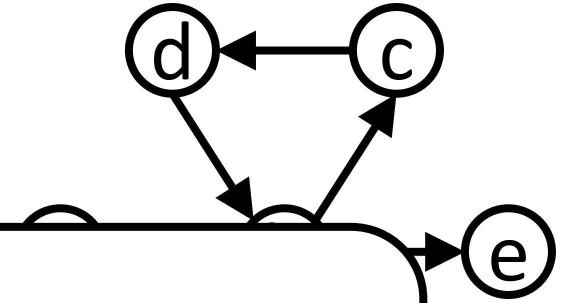


$\{a\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \diamond \{a, b, c, d\}$

PaCo



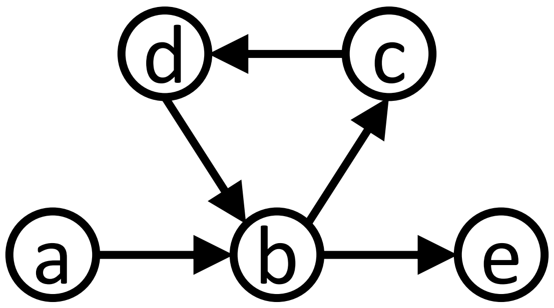
Tarski

$x \sqsubseteq \nu f$

$\Leftarrow x \sqsubseteq f(x)$

Example

Tarski



$\{a\} \subseteq \nu Z. \diamond Z$

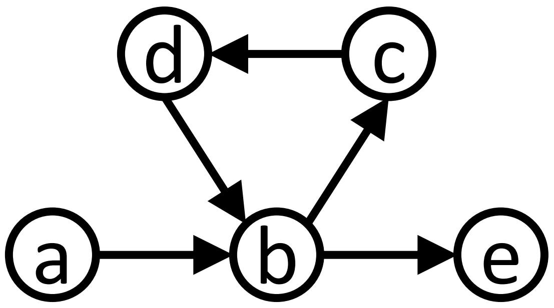
$\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \diamond \{a, b, c, d\}$

$\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$

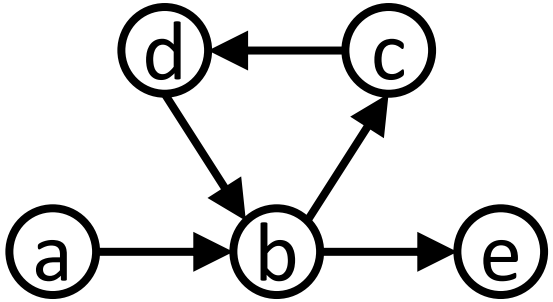
$\square$

PaCo



Example

Tarski



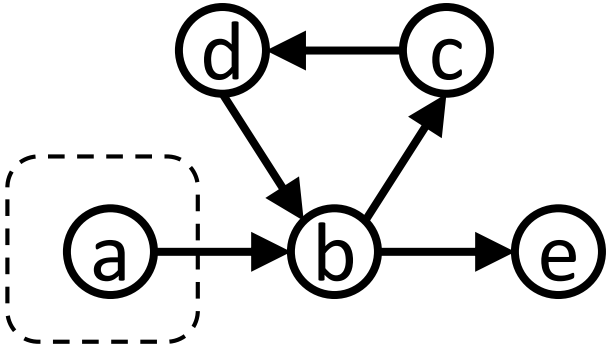
$\{a\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \diamond \{a, b, c, d\}$

$\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$ □

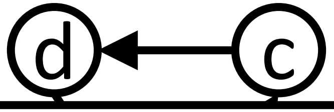
PaCo



$\{a\} \subseteq G_{\diamond}(\emptyset)$

Example

Tarski



Unfolding

$y \sqsubseteq G_f(x)$

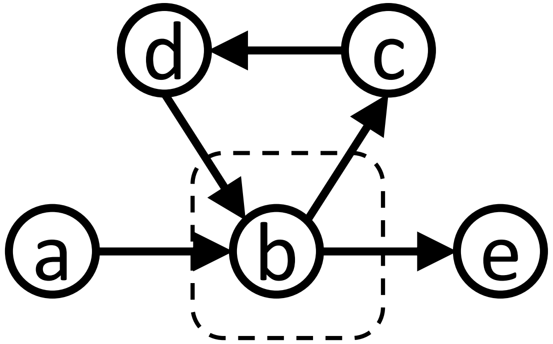
$\Leftarrow y \sqsubseteq f\left(x \sqcup G_f(x)\right)$

$\Leftarrow \{a,b,c,d\} \subseteq \Diamond\{a,b,c,d\}$

$\Leftarrow \{a,b,c,d\} \subseteq \{a,b,c,d\}$

□

PaCo

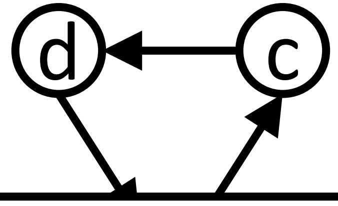


$\{a\} \subseteq G_{\Diamond}(\emptyset)$

$\Leftarrow \{b\} \subseteq G_{\Diamond}(\emptyset)$

Example

Tarski



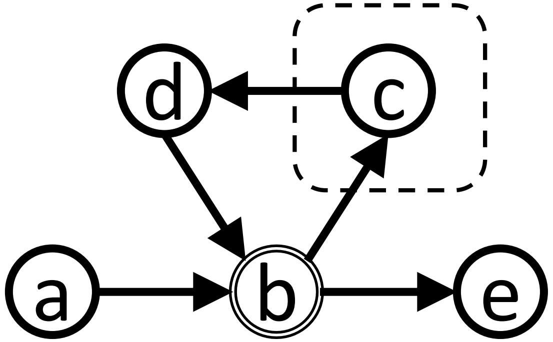
Accumulation

$y \sqsubseteq G_f(x)$

$\Leftarrow y \sqsubseteq G_f(x \sqcup y)$

$\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$ □

PaCo



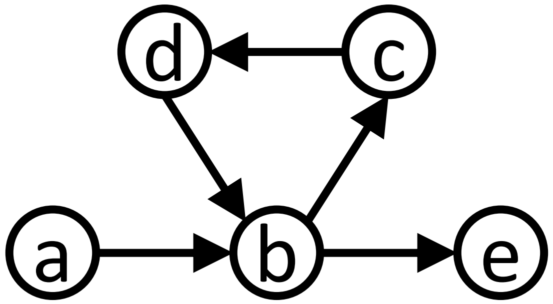
$\{a\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{b\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{c\} \subseteq G_\diamond(\{b\})$

Example

Tarski



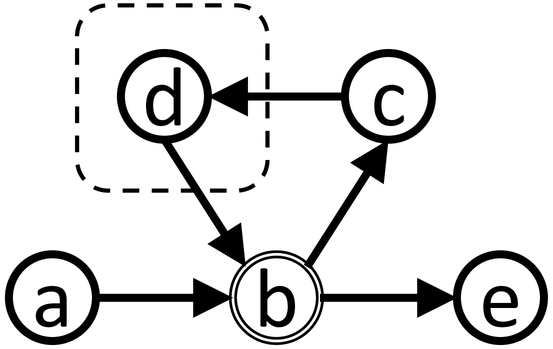
$\{a\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \diamond \{a, b, c, d\}$

$\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$ $\square$

PaCo



$\{a\} \subseteq G_\diamond(\emptyset)$

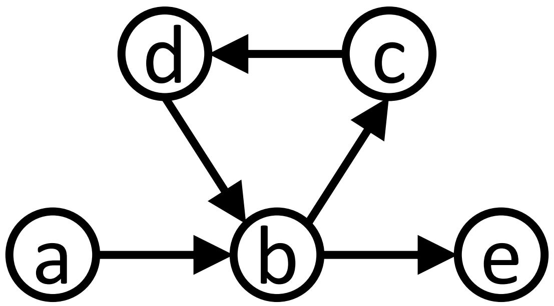
$\Leftarrow \{b\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{c\} \subseteq G_\diamond(\{b\})$

$\Leftarrow \{d\} \subseteq G_\diamond(\{b\})$

Example

Tarski



$\{a\} \subseteq \nu Z. \diamond Z$

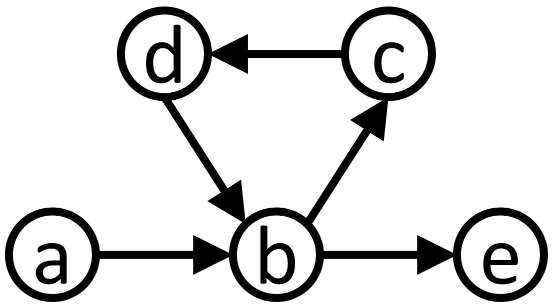
$\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \diamond \{a, b, c, d\}$

$\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$

□

PaCo



$\{a\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{b\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{c\} \subseteq G_\diamond(\{b\})$

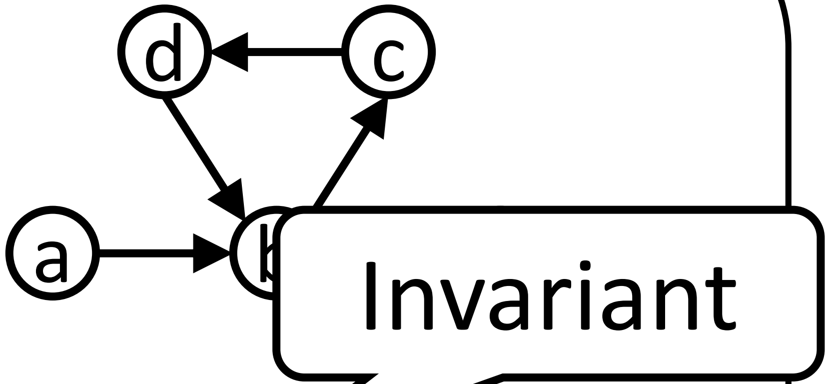
$\Leftarrow \{d\} \subseteq G_\diamond(\{b\})$

$\Leftarrow \{b\} \subseteq \{b\}$

□

Example

Tarski



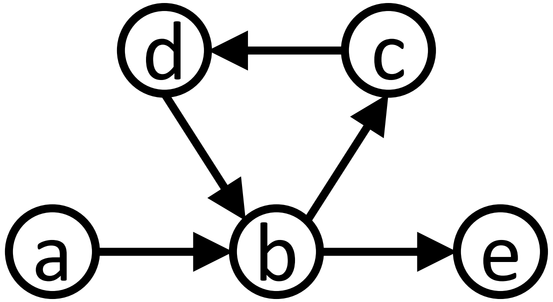
$\{a\} \subseteq \nu Z.\diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \nu Z.\diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \diamond\{a, b, c, d\}$

$\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$ $\square$

PaCo



No Invariant

$\{a\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{b\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{c\} \subseteq G_\diamond(\{b\})$

$\Leftarrow \{d\} \subseteq G_\diamond(\{b\})$

$\Leftarrow \{b\} \subseteq \{b\}$ $\square$

Functional characterization

Def.

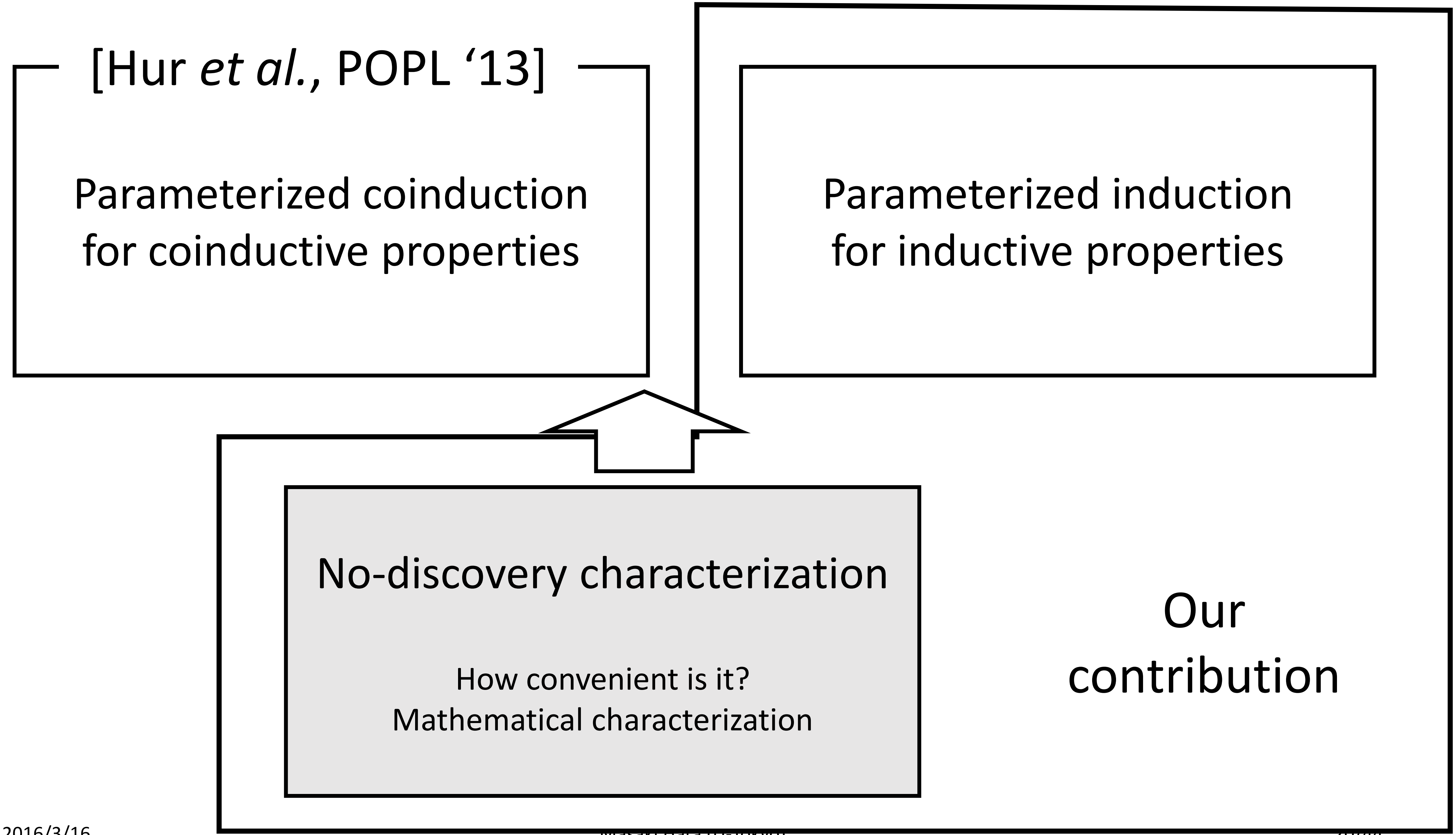
For $F : C \to C$ a function,

- F satisfies *Unfolding*, if $\forall x, y \in C.\ y \sqsubseteq f\big(x \sqcup F(x)\big) \Rightarrow y \sqsubseteq F(x)$
- F satisfies *Accumulation*, if $\forall x, y \in C.\ y \sqsubseteq F(x \sqcup y) \Rightarrow y \sqsubseteq F(x)$

Thm.

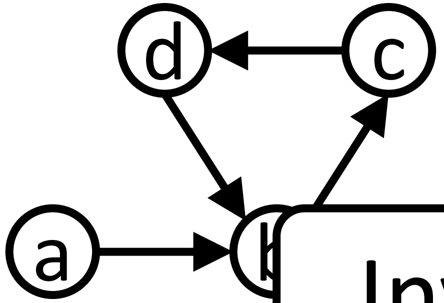
For F satisfying Unfolding and Accumulation,

$G_f(x) \sqsubseteq F(x)$.


[Hur *et al.*, POPL ‘13]
Parameterized coinduction for coinductive properties
Parameterized induction for inductive properties
No-discovery characterization
How convenient is it?
Mathematical characterization
Our contribution

Review : comparison of two proofs

Tarski



Invariant

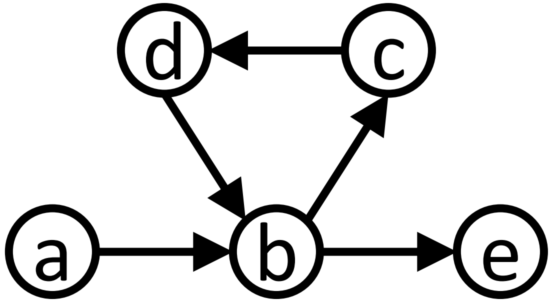
$\{a\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a, b, c, d\} \subseteq \diamond \{a, b, c, d\}$

$\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$ □

PaCo



No Invariant

$\{a\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{b\} \subseteq G_\diamond(\emptyset)$

$\Leftarrow \{c\} \subseteq G_\diamond(\{b\})$

$\Leftarrow \{d\} \subseteq G_\diamond(\{b\})$

$\Leftarrow \{b\} \subseteq \{b\}$ □

Review : comparison of two proofs

Tarski

PaCo

Question:

1. What is invariant discovery?
2. Doesn't PaCo need invariant discovery?

$\{a\} \subseteq$

$\Leftarrow \{a, b$

$\Leftarrow \{a, b,$

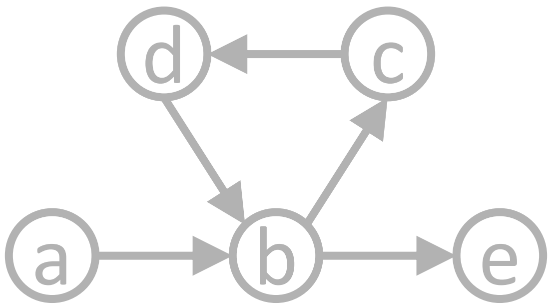
$\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$ □

ant

$\Leftarrow \{b\} \subseteq \{b\}$ □

Invariant discovery : informal definition

Tarski



$\{a\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a,b,c,d\} \subseteq \nu Z. \diamond Z$

$\Leftarrow \{a,b,c,d\} \subseteq \diamond \{a,b,c,d\}$

$\Leftarrow \{a,b,c,d\} \subseteq \{a,b,c,d\}$ □

Def. (Informal)

Invariant Discovery is a proof like this:

$x \sqsubseteq \nu f$

$\Leftarrow x \sqsubseteq x', \; x' \sqsubseteq \nu f$

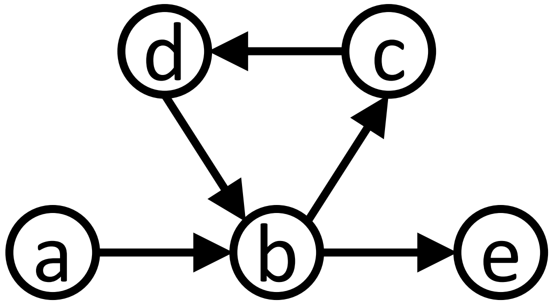
$\Leftarrow x \sqsubseteq x', \; x' \sqsubseteq f(x')$

Invariant discovery : example

	With invariant	**Without invariant**	
		Finite	Infinite
Tarski	✓	✘	✘
PaCo	✓	✓	✘

Invariant discovery : example

- Proof with invariant discovery
- $\{a\} \subseteq \nu Z. \diamond Z$
  $\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$
  $\Leftarrow \{a, b, c, d\} \subseteq \diamond \{a, b, c, d\}$
  $\Leftarrow \{a, b, c, d\} \subseteq \{a, b, c, d\}$ □

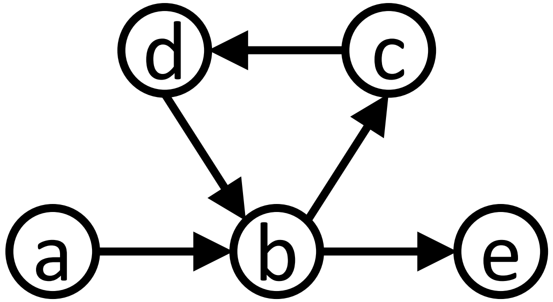


	With invariant	Without invariant	
		Finite	Infinite
Tarski	✓	×	×
PaCo	✓	✓	×

Invariant discovery : example

- Proof without invariant discovery : Tarski case
- $\{a\} \subseteq \nu Z. \diamond Z$
  $\Leftarrow \{b\} \subseteq \nu Z. \diamond Z$
  $\Leftarrow \{b\} \subseteq \diamond \{b\}$
  $\Leftrightarrow \{b\} \subseteq \{a, d\}$

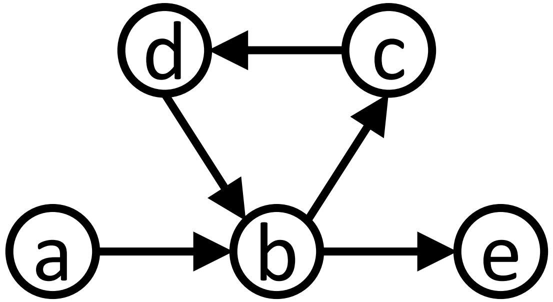
Unsuccessful proof



	With invariant	Without invarian	
		Finite	Infinite
Tarski	✓	×	×
PaCo	✓	✓	×

Invariant discovery : example

- Proof without invariant discovery : Tarski case
- $\{a\} \subseteq \nu Z. \diamond Z$
  $\Leftarrow \{b\} \subseteq \nu Z. \diamond Z$
  $\Leftarrow \{c\} \subseteq \nu Z. \diamond Z$
  $\Leftarrow \{d\} \subseteq \nu Z. \diamond Z$
  $\Leftarrow \quad \vdots$

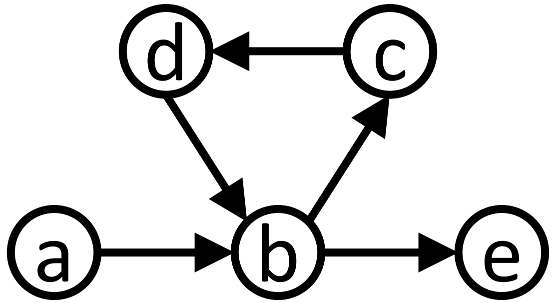


Unsuccessful proof

	With invariant	**Without invariant**	
		Finite	Infinite
Tarski	✓	✗	✗
PaCo	✓	✓	✗

Invariant discovery : example

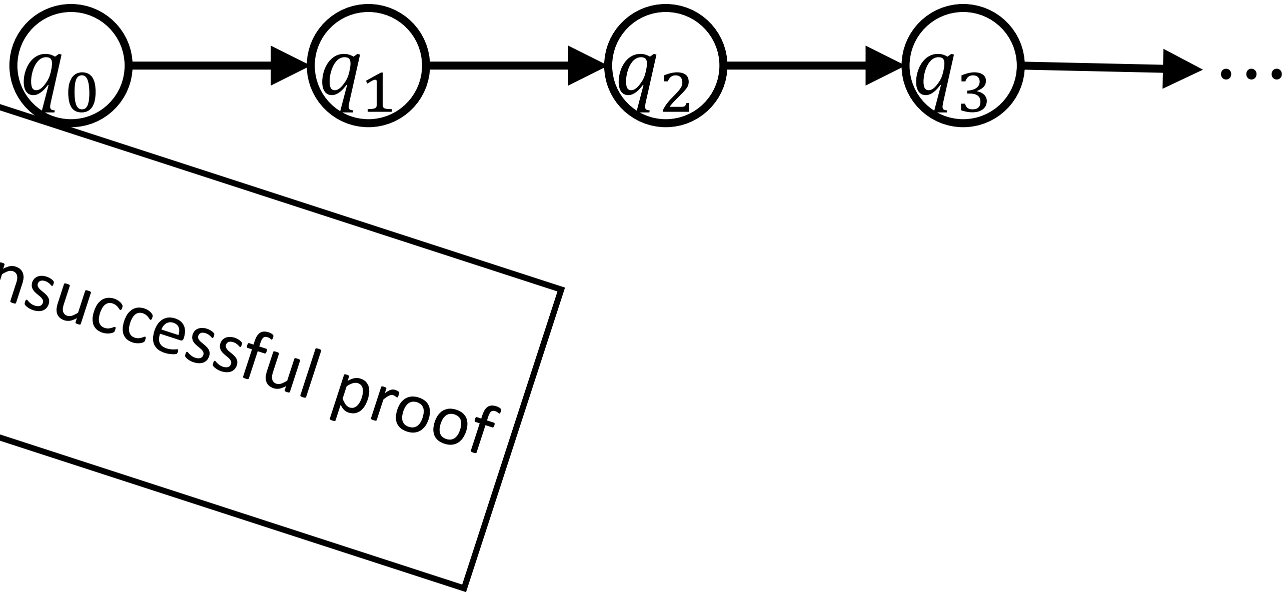
- Proof without invariant discovery : PaCo case
- $\{a\} \subseteq G_\diamond(\emptyset)$
  $\Leftarrow \{b\} \subseteq G_\diamond(\emptyset)$
  $\Leftarrow \{c\} \subseteq G_\diamond(\{b\})$
  $\Leftarrow \{d\} \subseteq G_\diamond(\{b\})$
  $\Leftarrow \{b\} \subseteq \{b\}$ $\square$



	With invariant	Without invariant	
		Finite	Infinite
Tarski	✓	✗	✗
PaCo	✓	✓	✗

Invariant discovery : example

- Proof without invariant discovery : PaCo case
- $\{q_0\} \subseteq G_\diamond(\emptyset)$
  $\Leftarrow \{q_1\} \subseteq G_\diamond(\{q_0\})$
  $\Leftarrow \{q_2\} \subseteq G_\diamond(\{q_0, q_1\})$
  $\Leftarrow \{q_3\} \subseteq G_\diamond(\{q_0, q_1, q_2\})$
  $\Leftarrow \vdots$



	With invariant	Without invariant	
		Finite	Infinite
Tarski	✓	×	×
PaCo	✓	✓	×

Invariant discovery : example

	With invariant	Without invariant	
		Finite	Infinite
Tarski	✓	✗	✗
PaCo	✓	✓	✗

Aim: to make these rigorous

Invariant discovery : analysis

$\{a\} \subseteq \nu Z. \diamond Z$
$\Leftarrow \{a, b, c, d\} \subseteq \nu Z. \diamond Z$

Invariant discovery uses <u>transitivity</u>

<u>Forget transitivity</u>

$y \sqsubseteq G_f(x) \longrightarrow P(x, y)$

Invariant discovery : assumption

Asm.

From now on, we assume that for all x, $\lambda y.\ f(x \sqcup y)$ preserves directed infima.

Invariant discovery : definition

Def.

For $P(x, y)$: predicate,

- Downward closure :

$$\forall y, y' \in C.\ y \sqsubseteq y', P(x, y') \quad \Rightarrow \quad P(x, y)$$

cf. transitivity $y \sqsubseteq y', y' \sqsubseteq G_f(x) \ \Rightarrow\ y \sqsubseteq G_f(x)$

- Join closure :

$$\forall x \in C.\ \forall Y \subseteq C. \big(\forall y \in Y.\ P(x, y)\big) \ \Rightarrow\ P(x, \bigsqcup Y)$$

Invariant discovery : definition

Def.

For $P(x, y)$: predicate,

- Unfolding : for all x, y, z, $P(x, y)$ holds if
  - z is minimal among $\{ z' \mid y \sqsubseteq f(z') \}$
  - $P(x, z)$.
- Accumulation : $\forall x, y.\ P(x \sqcup y, y) \Rightarrow P(x, y)$
- Tarski : $\forall x, y.\ y \sqsubseteq f(x \sqcup y) \Rightarrow P(x, y)$

Invariant discovery : definition

Thm.

- $y \sqsubseteq \nu f$

  $\Leftrightarrow \quad \forall P.$ Downward closure, Join closure, Unfolding, Tarski

  $\Rightarrow P(\bot, y)$

- $y \sqsubseteq G_f(x)$

  $\Leftrightarrow \quad \forall P.$ Downward closure, Join closure, Unfolding, Accumulation

  $\Rightarrow P(x, y)$

Invariant discovery : definition

Def.

- $y \sqsubseteq \nu f$ is *no-discovery Tarski provable*
  $\Leftrightarrow \quad \forall P.$ Join closure, Unfolding, Tarski
  $\Rightarrow P(\bot, y)$
- $y \sqsubseteq G_f(x)$ is *no-discovery PaCo provable*
  $\Leftrightarrow \quad \forall P.$ Join closure, Unfolding, Accumulation
  $\Rightarrow P(x, y)$

Invariant discovery : main theorem

Thm.

- For finite lattices, $y \sqsubseteq G_f(x)$ is no-discovery PaCo provable, if it holds.
- For infinite lattices, $y \sqsubseteq G_f(x)$ is not necessarily no-discovery PaCo provable.
- $y \sqsubseteq \nu f$ is not necessarily no-discovery Tarski provable.

Invariant discovery : main theorem

Thm.

- For finite lattices, $y \sqsubseteq G_f(x)$ is no-discovery PaCo provable, if it holds.
- For infinite lattices, $y \sqsubseteq G_f(x)$ is not necessarily no-discovery PaCo provable.
- $y \sqsubseteq \nu f$ is not necessarily no-discovery Tarski provable.

	With invariant	**Without invariant**	
		Finite	Infinite
Tarski	✓	✗	✗
PaCo	✓	✓	✗

[Hur *et al.*, POPL '13]

Parameterized coinduction
for coinductive properties

Parameterized induction
for inductive properties

No-discovery characterization

How convenient is it?
Mathematical characterization

Our
contribution

Parameterized induction

Def.

$L_f(x) = \mu y.\ f(x \sqcup y)$ parameterized least fixpoint

Lem.

$\forall x, y.\ y \sqsubseteq f\left(x \sqcup L_f(x)\right) \Rightarrow\ y \sqsubseteq L_f(x)$ (Unfolding)

$\forall x, y : \alpha' \to C$ (x increasing).

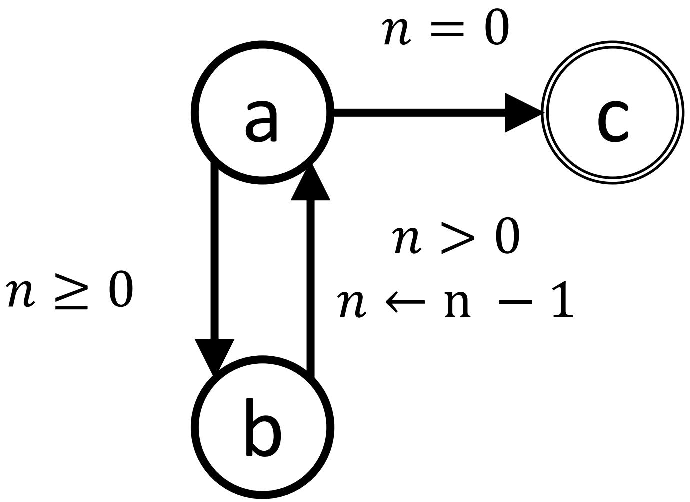
$$\left(\forall \alpha. y(\alpha) \sqsubseteq L_f\left(x(\alpha) \sqcup \bigsqcup_{\beta<\alpha} y(\beta)\right)\right)$$

$$\Rightarrow\ \left(\forall \alpha.\ y(\alpha) \sqsubseteq L_f\big(x(\alpha)\big)\right)$$

(Indexed Accumulation)

Parameterized induction : pushdown example

- $\forall n. \{a(n)\} \subseteq L_f(\emptyset)$
  $\Leftarrow \forall n. \{a(n)\} \subseteq L_f(\{a(m) | m < n\})$
  $\Leftarrow \forall n. \{b(n)\} \subseteq L_f(\{a(m) | m < n + 1\})$
  $\Leftarrow \forall n. \{a(n)\} \subseteq \{a(m) | m < n + 1\}$ □



$f(Z) = \{c(n)\} \cup \diamond Z$

Conclusion & Future Work

- No-discovery characterization
  - Gave mathematical framework to characterize power of parameterized coinduction
  - No-go theorem : perhaps useful for future proof-technique development.
- Future work
  - Syntactic Approach
  - Trying non-Boolean examples

Conclusion & Future Work

- **Parameterized Induction**
  - Applied PaCo-like strategy to inductive properties.
  - Perhaps useful for pushdown systems
- Future Work
  - Implementation to a proof assistant
  - Generalization to mixed μ/ν formulas

[Hur *et al.*, POPL '13]

Parameterized coinduction
for coinductive properties

Parameterized induction
for inductive properties

No-discovery characterization

How convenient is it?
Mathematical characterization

Our
contribution