Extension of Kleisli Simulation to Infinite Traces

クライスリ模倣の無限トレースへの拡張

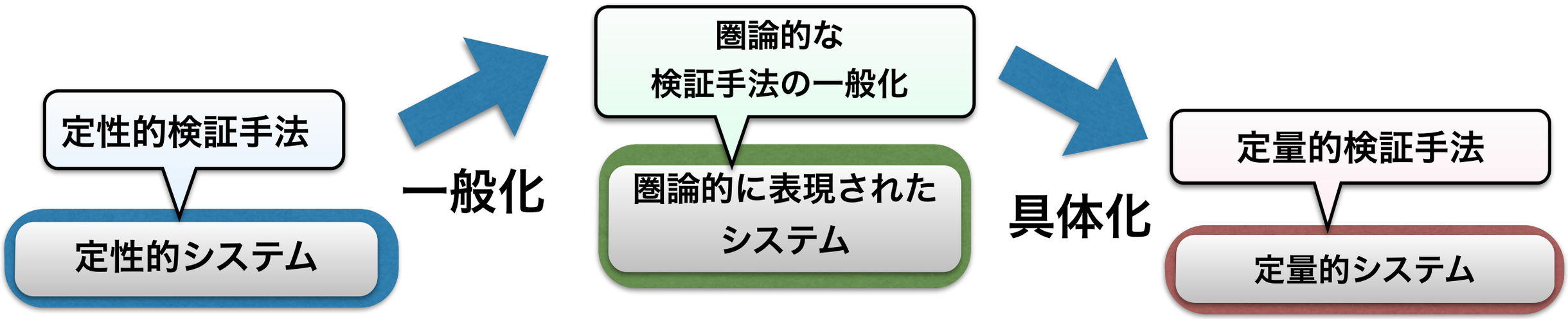
2016 February 1　修士論文発表

蓮尾研 M2　卜部夏木

動機

- **定量的システム**の形式検証
  - 与えられた定量的システムがある定量的性質を満たす事を示す
  - 例：確率，エネルギー消費，時間，etc…
- 既存の定性的検証手法を，
  - 圏論的に一般化し，
  - 定量的システムに具体化することで，

定量的検証手法を導出



本研究の位置づけ

クライスリ模倣が無限トレースに関しても

健全である事を示した

有限トレースについて健全

クライスリ模倣 [Hasuo '06]

有限トレースについて健全

模倣

定性的検証手法

定性的システム

一般化

圏論的な検証手法の一般化

圏論的に表現されたシステム

具体化

確率的木オートマトンの模倣

定量的検証手法

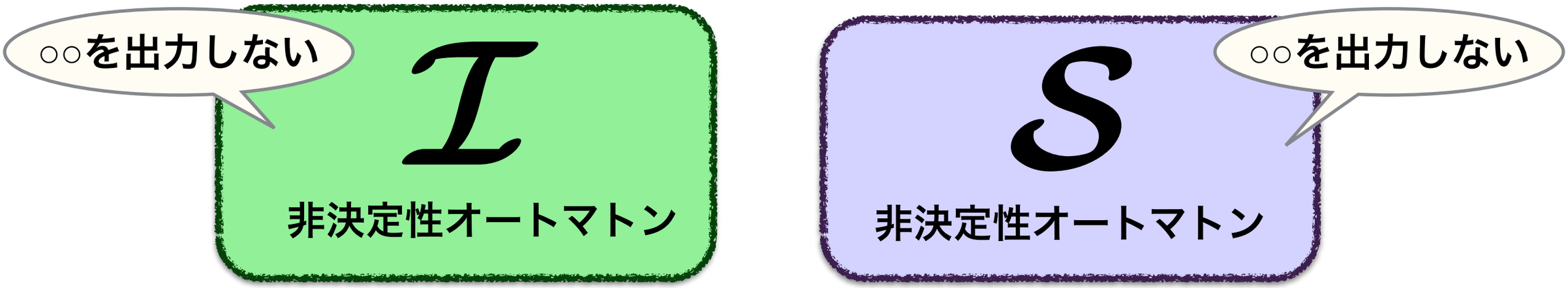
定量的システム

アウトライン

- Preliminaries
  - 模倣を用いた検証
  - クライスリ模倣
  - Forward Partial Execution
- Contribution
  - 無限トレースに対するクライスリ模倣
  - 無限トレースに対するForward Partial Execution
- まとめ
- 博士課程での研究計画

模倣を用いた定性的システムの検証

- 目標：定性的システム間の **language inclusion** を調べる



$$L(\mathcal{I}) \subseteq L(\mathcal{S})$$

- 問題：language inclusion の直接の検証は難しい

step-wise な language inclusion を示す

= 模倣 (simulation)

模倣の健全性と完全性

A から *B* への 模倣関係 が存在 (stepwise language inclusion)

健全性 ⇓　　⇑̸　**完全性は必ずしも成り立たない**

A の language は *B* の language に含まれる (language inclusion)

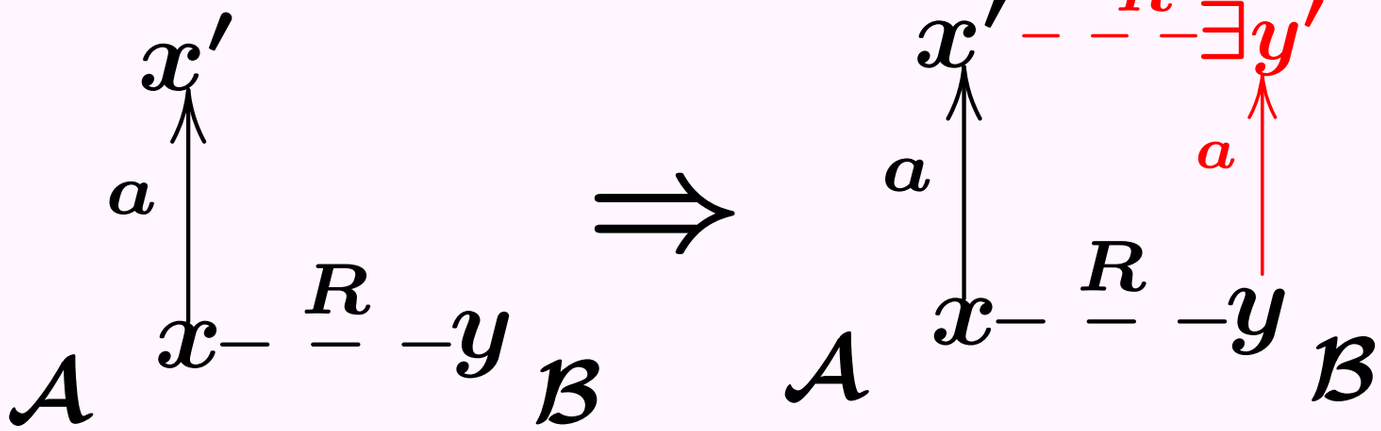
例：順方向・逆方向模倣

[Lynch & Vaandrager ‘95]

- 非決定性オートマトンに対する模倣
- 状態集合間の関係Rとして定義される

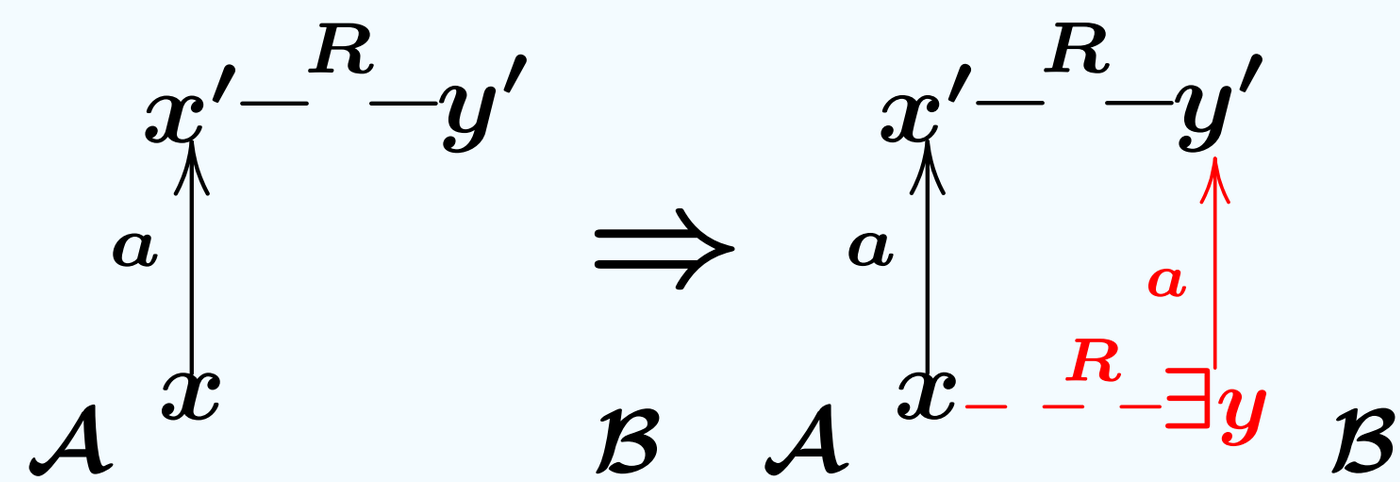
順方向:

$$\mathcal{A} \sqsubseteq_{\mathbf{F}} \mathcal{B} \quad \overset{\text{def}}{\Leftrightarrow} \quad \exists R.$$



逆方向:

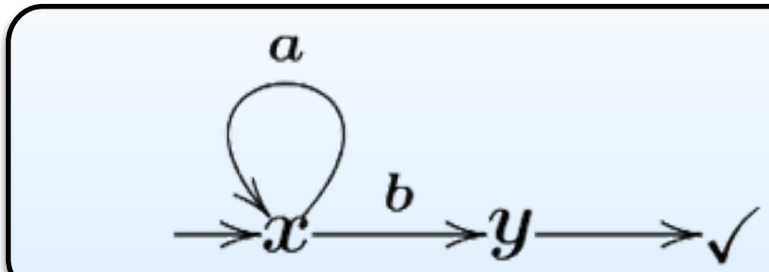
$$\mathcal{A} \sqsubseteq_{\mathbf{B}} \mathcal{B} \quad \overset{\text{def}}{\Leftrightarrow} \quad \exists R.$$



例：順方向・逆方向模倣

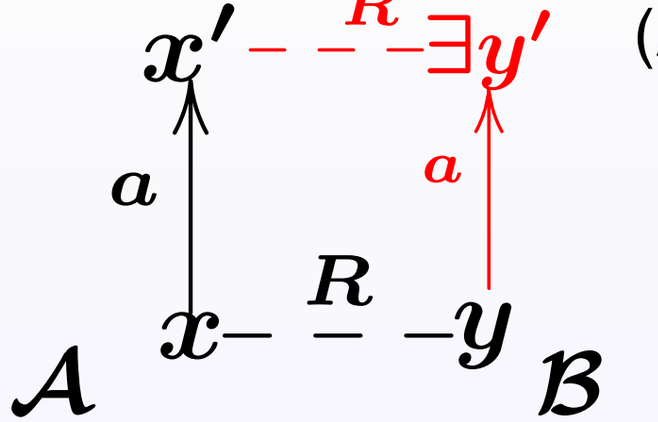
[Lynch & Vaandrager '95]

・ 順方向・逆方向模倣は**有限トレース**に関して**健全**



$$L(\mathcal{A}) = \{b, ab, aab, \ldots\}$$

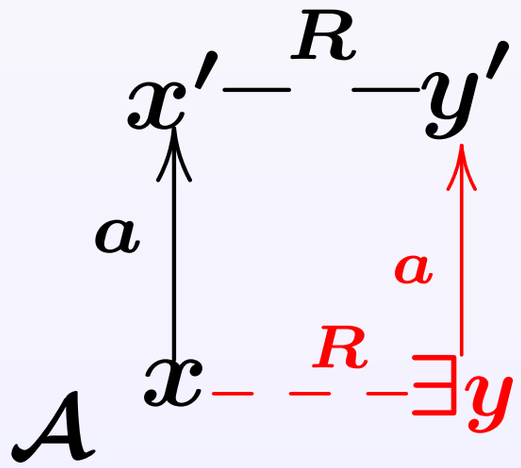
Thm.



(順方向模倣)

$$L(\mathcal{A}) \subseteq L(\mathcal{B})$$

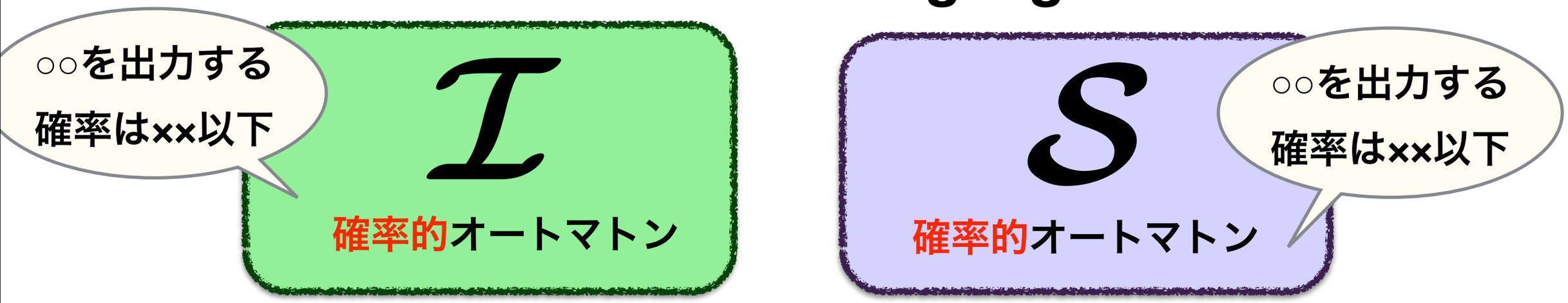
(**finite** language inclusion)



(逆方向模倣)

模倣を用いた定量的システムの検証

- 目標：定量的システム間の **language inclusion** を調べる



$$L(\mathcal{I}) \leq L(\mathcal{S})$$

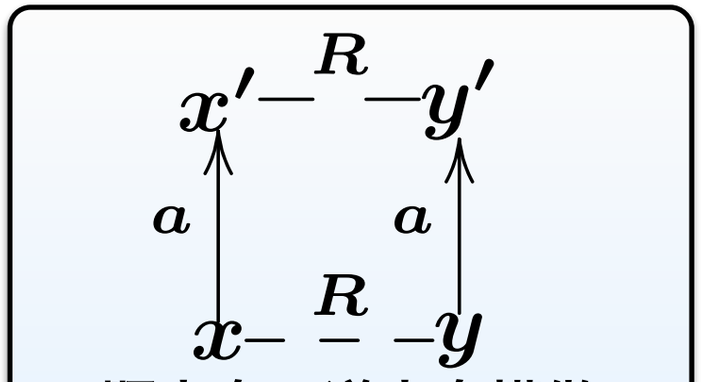
- 定量的模倣の例：
  - JonssonとLarsenによる模倣（確率的システム，[Jonsson & Larsen, '91]）
  - Chatterjeeらによる模倣（コスト付きシステム，[Chatterjee et. al., '10]）

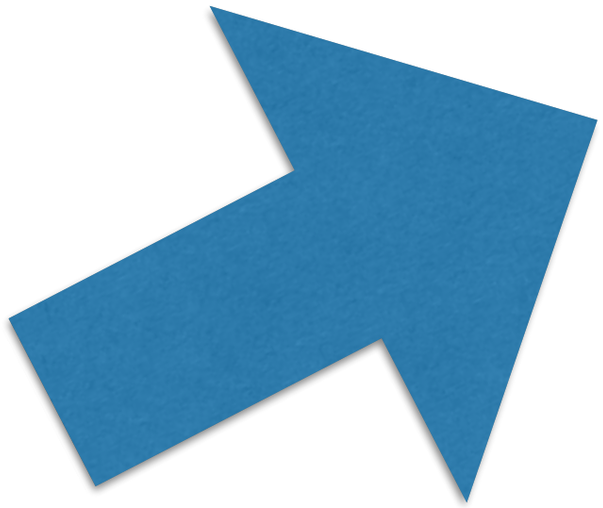
アウトライン

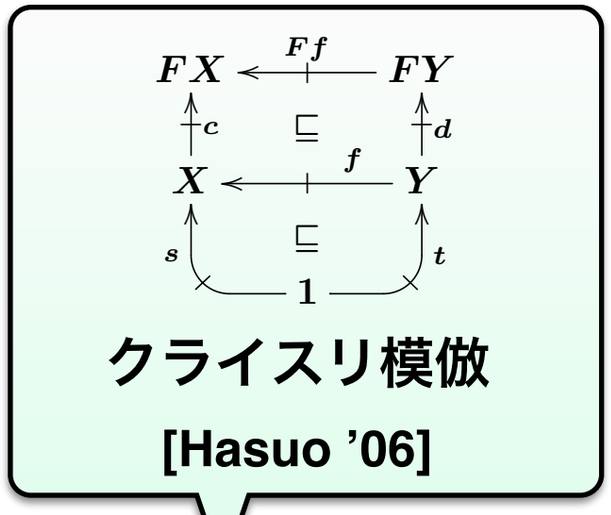
- Preliminaries
  - 模倣を用いた検証
  - クライスリ模倣
  - Forward Partial Execution
- Contribution
  - 無限トレースに対するクライスリ模倣
  - 無限トレースに対するForward Partial Execution
- まとめ
- 博士課程での研究計画

クライスリ模倣 [Hasuo, ‘06]

- LynchとVaandragerによる模倣の**圏論的**な一般化

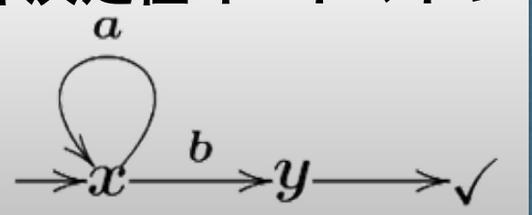






一般化

非決定性オートマトン



圏論的に表現された
システム

$1 \overset{s}{\nrightarrow} X \overset{c}{\nrightarrow} \overline{F}X$

- 順方向・逆方向の２種類

クライスリ模倣の健全性

[Hasuo, ‘06]

- **有限トレース**に対する健全性が**圏論的に**示されている

Thm. **(健全性)**

(順方向**クライスリ**模倣)

$$\mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y}$$

$\Rightarrow$

$$\mathbf{tr}(\mathcal{X}) \sqsubseteq \mathbf{tr}(\mathcal{Y})$$

(**圏論的 finite** language inclusion)

[Hasuo, Jacobs & Sokolova, ’07]

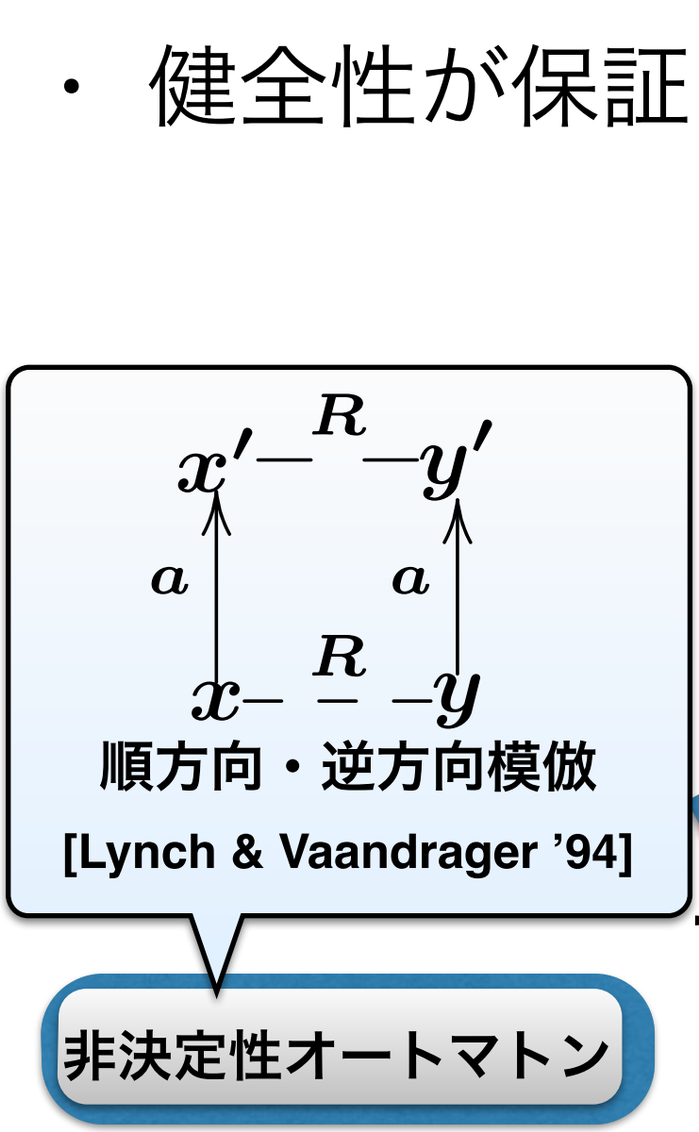
$$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y}$$

$\Rightarrow$

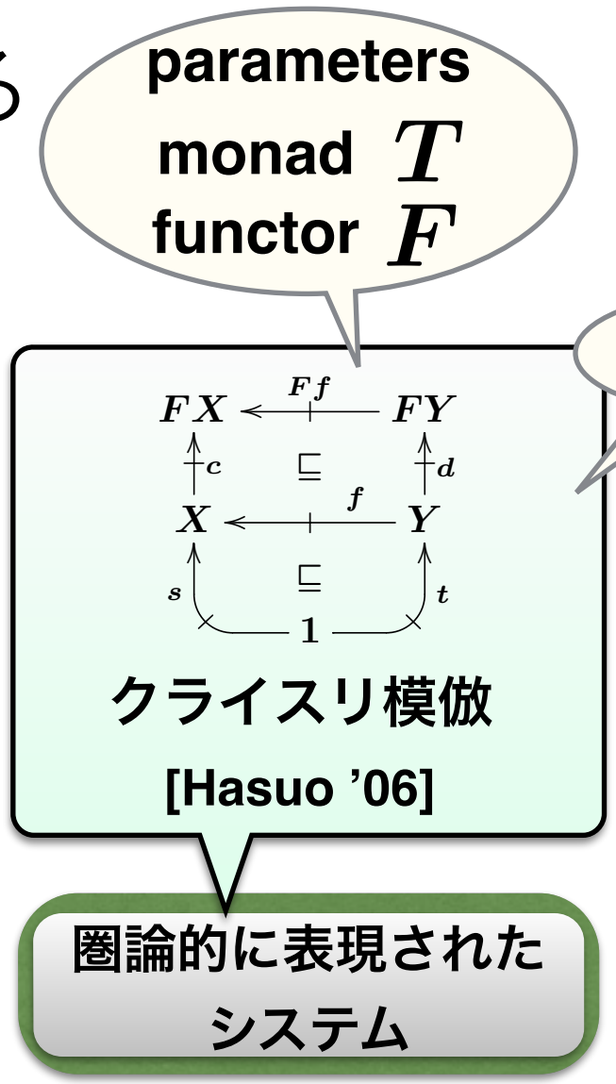
(逆方向**クライスリ**模倣)

クライスリ模倣 [Hasuo, ‘06]

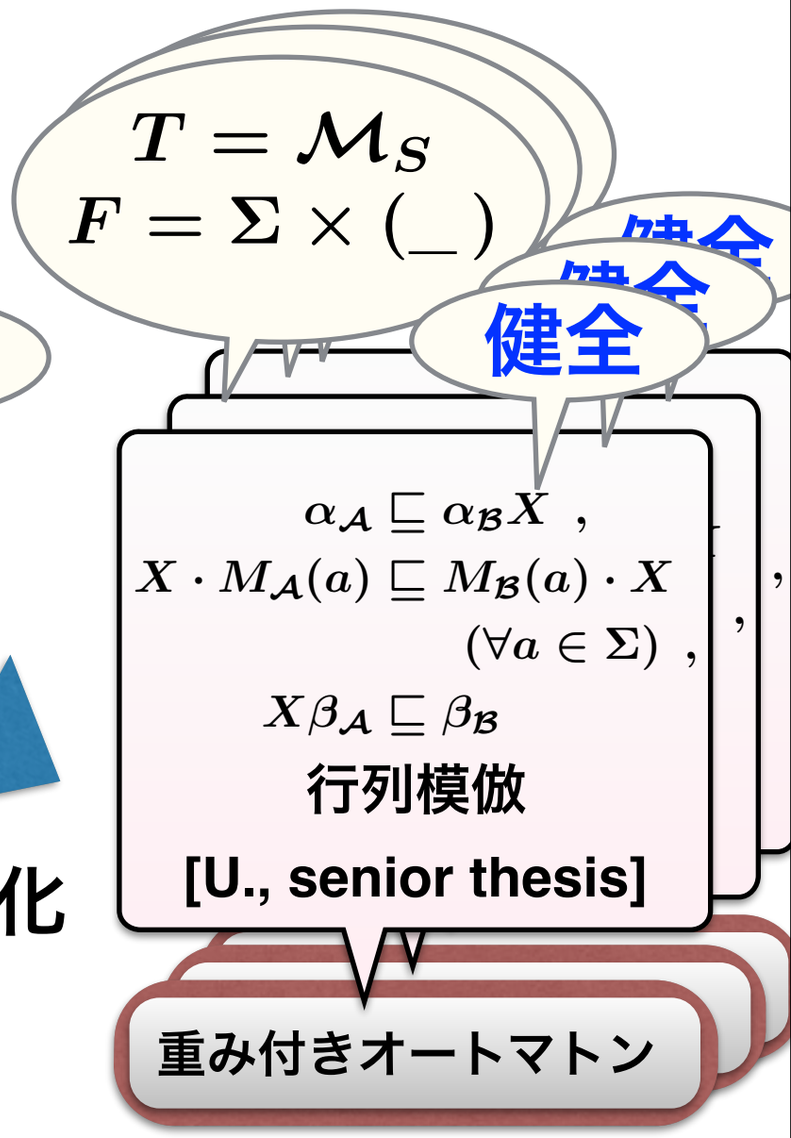
- 具体化により，様々なシステムへ模倣を定義できる
- 例：重み付きオートマトンに対する**行列模倣** [U. senior thesis]
- 健全性が保証される



一般化



具体化



アウトライン

- Preliminaries
  - 模倣を用いた検証
  - クライスリ模倣
  - Forward Partial Execution
- Contribution
  - 無限トレースに対するクライスリ模倣
  - 無限トレースに対するForward Partial Execution
- まとめ
- 博士課程での研究計画

模倣の不完全性

A から *B* への 模倣関係 が存在 (stepwise language inclusion)

健全性 ⇓　　⇑ ✗　　**完全性は必ずしも成り立たない**

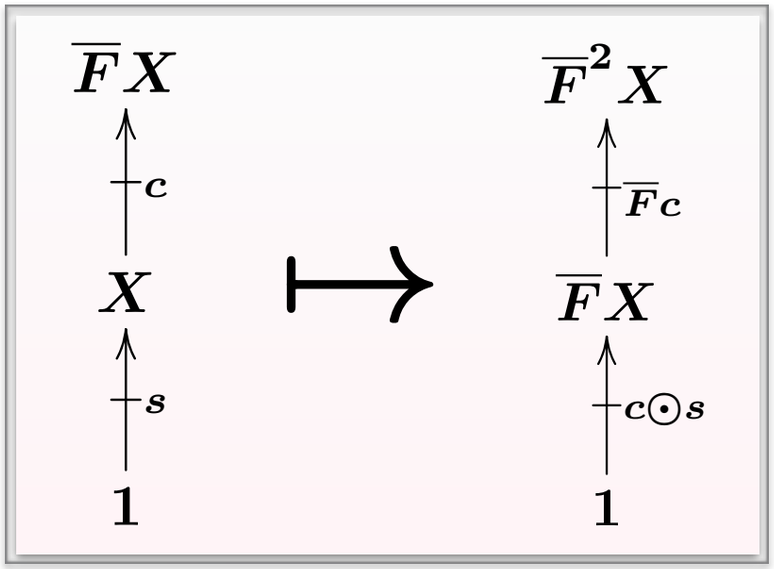
A の language は *B* の language に含まれる (language inclusion)

It can be that

$$L(\mathcal{A}) \subseteq L(\mathcal{B}) \qquad \text{but} \qquad \mathcal{A} \not\preceq_{\mathbf{F}} \mathcal{B}$$

Forward Partial Execution [U. & Hasuo, '14]

- 圏論的に定義されたシステムの変形



$$\mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y}$$

$$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y}$$

- クライスリ模倣を「増やす」ことができる

Thm(soundness):
$$\mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} \;\Rightarrow\; \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y}$$
$$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) \;\Rightarrow\; \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y}$$

Thm(adequacy):
$$\mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y} \;\Rightarrow\; \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y}$$
$$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y} \;\Rightarrow\; \mathcal{X} \sqsubseteq_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y})$$

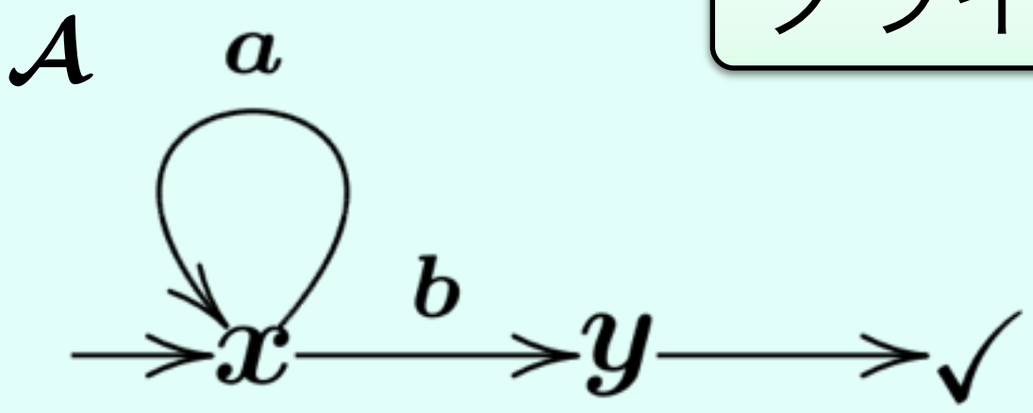
アウトライン

- Preliminaries
  - 模倣を用いた検証
  - クライスリ模倣
  - Forward Partial Execution
- Contribution
  - 無限トレースに対するクライスリ模倣
  - 無限トレースに対するForward Partial Execution
- まとめ
- 博士課程での研究計画

有限トレースと無限トレース

有限トレース

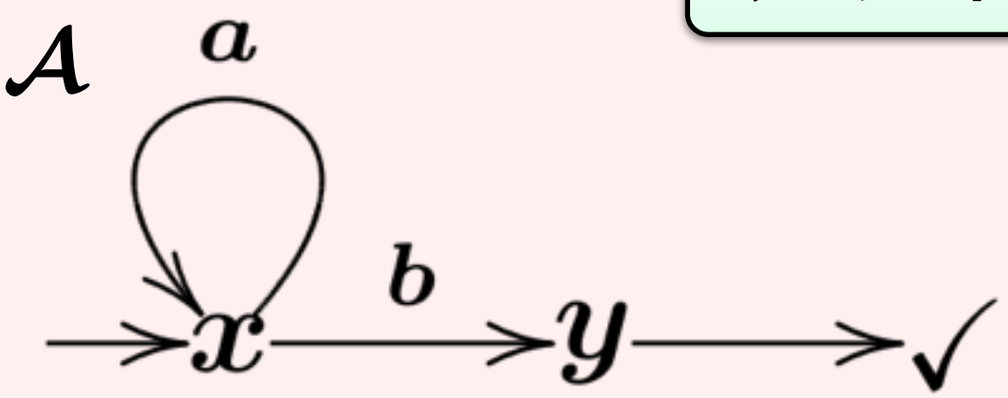
クライスリ模倣は健全，FPE



$$L(\mathcal{A}) = \{b, ab, aab, \ldots\}$$

無限トレース

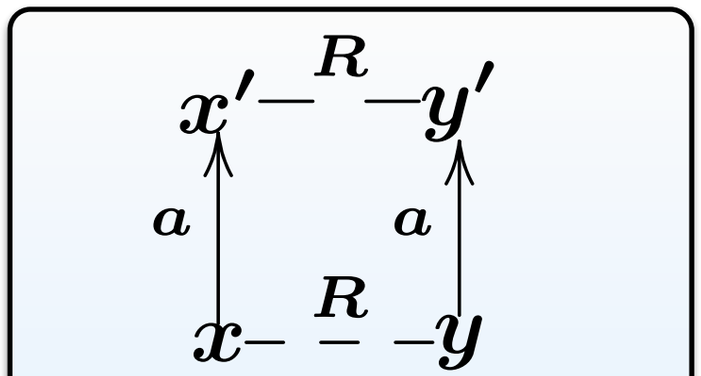
クライスリ模倣は健全？ FPEは？



$$L^{\infty}(\mathcal{A}) = \{b, ab, aab, \ldots\} \cup \{aaa\ldots\}$$

- 同様の事は確率的システムでも

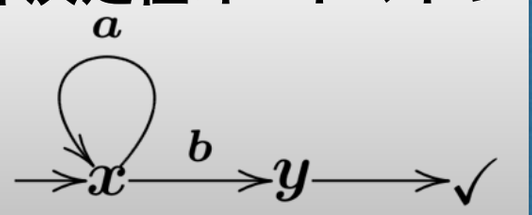
クライスリ模倣



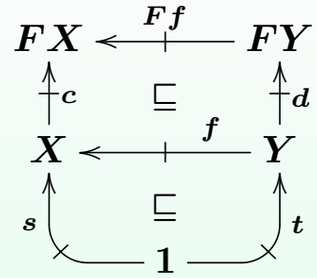
順方向・逆方向模倣

[Lynch & Vaandrager ’94]

非決定性オートマトン



一般化



クライスリ模倣

[Hasuo ’06]

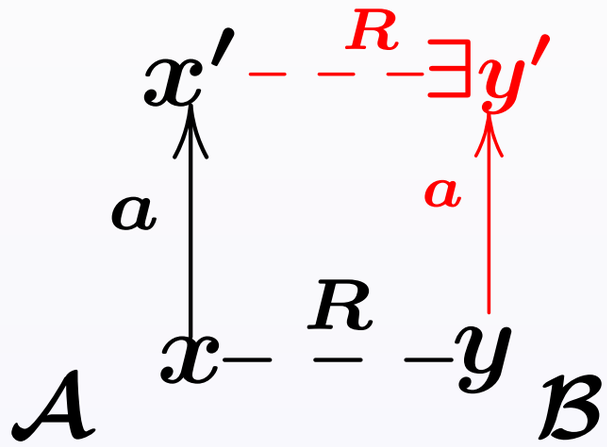
圏論的に表現された
システム

$1 \overset{s}{\nrightarrow} X \overset{c}{\nrightarrow} \overline{F}X$

順方向・逆方向模倣の
無限トレースに対する健全性

[Lynch & Vaandrager '95]

Thm.

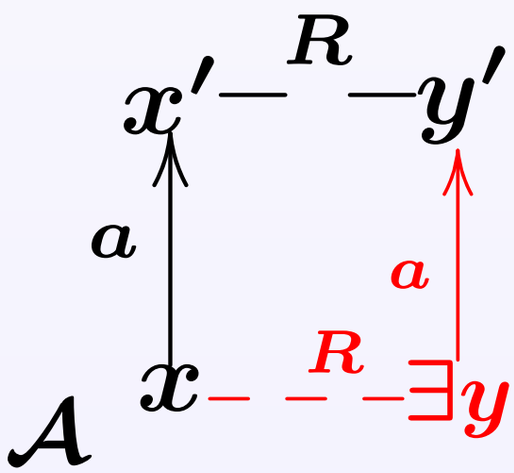


(順方向模倣)

$$\Rightarrow \quad L^\infty(\mathcal{A}) \subseteq L^\infty(\mathcal{B})$$

(**infinite** language inclusion)

$\not\Rightarrow$

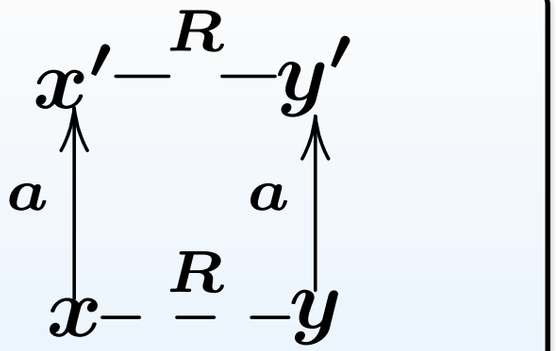


(逆方向模倣)

$+$

$$\begin{cases} \cdot\ \forall x.\, \exists y.\, R(x,y) & \textbf{(totality)} \\ \cdot\ \forall x.\, (R(x,\_) \text{ is finite}) & \textbf{(image-finiteness)} \end{cases}$$

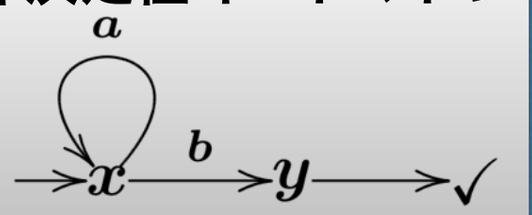
クライスリ模倣



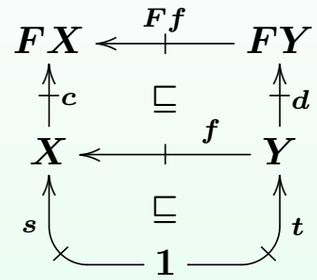
順方向・逆方向模倣

[Lynch & Vaandrager ’94]

非決定性オートマトン



一般化



クライスリ模倣

[Hasuo ’06]

圏論的に表現された
システム

$1 \overset{s}{\nrightarrow} X \overset{c}{\nrightarrow} \overline{F}X$

Contribution I: クライスリ模倣の無限トレースに対する健全性

[U. & Hasuo, '15]

Thm. For $T \in \{\mathcal{P}, \mathcal{G}, \mathcal{L}\}$ and polynomial F,

(順方向**クライスリ**模倣)

$$\mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y}$$

$\Rrightarrow$

$$\mathbf{tr}^{\infty}(\mathcal{X}) \sqsubseteq \mathbf{tr}^{\infty}(\mathcal{Y})$$

(**圏論的 infinite** language inclusion)

[Jacobs, '04]

$\Lleftarrow$

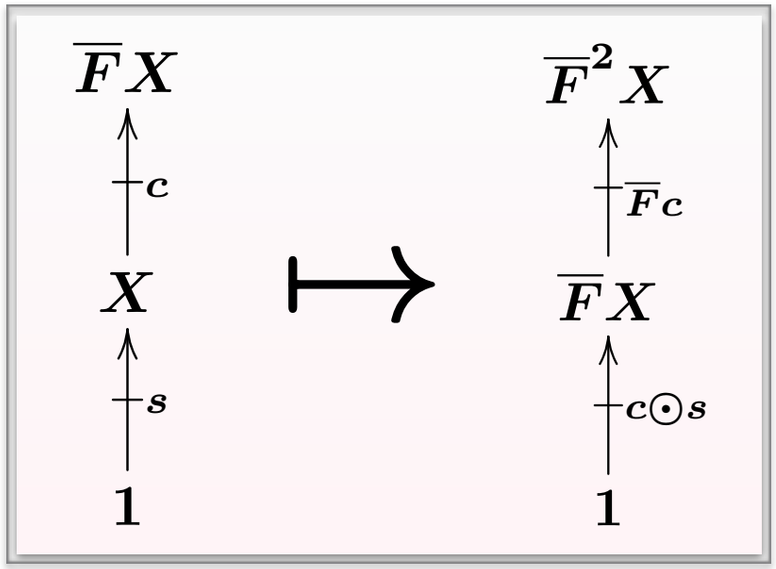
$$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y}$$

(逆方向**クライスリ**模倣)

$+$

$$\begin{cases} \top_{Y,Z} \odot b = \top_{X,Z} & \textbf{(圏論的 “totality”)} \\ \prod_{i \in a}(g_i \odot b) = (\prod_{i \in a} g_i) \odot b & \textbf{(圏論的 “image-finiteness”)} \end{cases}$$

Contribution II: 無限トレースに対する Forward Partial Execution [U. & Hasuo, '15]



$$\mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y}$$

$$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y}$$

- **無限トレース**の場合,

If the transition of $\mathcal{Y}$ is "total" and "image-finite",

Thm(soundness): $\mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} \Rightarrow \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y}$

$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) \Rightarrow \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y}$

Thm(adequacy): $\mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y} \Rightarrow \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y}$

~~$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y} \Rightarrow \mathcal{X} \sqsubseteq_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y})$~~

アウトライン

- Preliminaries
  - 模倣を用いた検証
  - クライスリ模倣
  - Forward Partial Execution
- Contribution
  - 無限トレースに対するクライスリ模倣
  - 無限トレースに対するForward Partial Execution
- まとめ
- 博士課程での研究計画

まとめ

- クライスリ模倣が**無限トレース**の inclusion の証明にも使える事を示した

  ➡ 具体化により,
  - 非決定性木オートマトン,
  - 確率的木オートマトン,
  - 例外付き木オートマトン

  等に**無限トレース**に関し健全な**模倣**を定義できる

- Forward partial execution が**無限トレース**の場合にもクライスリ模倣を増やせることを示した

Refereed papers

[1] **Natsuki Urabe** and Ichiro Hasuo,
"Generic Forward and Backward Simulations III: Quantitative Simulations by Matrices".
In *25th International Conference on Concurrency Theory (CONCUR 2014)*,
Vol. 8704 of *Lect. Notes Comp. Sci*, pp. 451-466. Springer, 2014. (Best Paper Award)

[2] **Natsuki Urabe** and Ichiro Hasuo, "Coalgebraic Infinite Traces and Kleisli Simulations".
In *6th Conference on Algebra and Coalgebra in Computer Science (CALCO 2015)*,
Vol. 35 of *LIPIcs*, pp. 320-335. Schloss Dagstuhl - Leibniz Zentrum fuer Informatik, 2015.

[3] **Natsuki Urabe** and Ichiro Hasuo, "Quantitative Simulations by Matrices".
To appear in *Information and Computation*. ([1]の論文のジャーナル版)

Submitted papers

[4] **Natsuki Urabe** and Ichiro Hasuo, "Coalgebraic Infinite Traces and Kleisli Simulations".
Submitted to *Logical Methods in Computer Science* ([2]の論文のジャーナル版)

[5] **Natsuki Urabe**, Shunsuke Shimizu and Ichiro Hasuo, "Coalgebraic Studies of Buechi Automata"
Submitted to *31st Annual ACM/IEEE Symposium on Logic and Computer Science (LICS 2016).*

Oral presentations

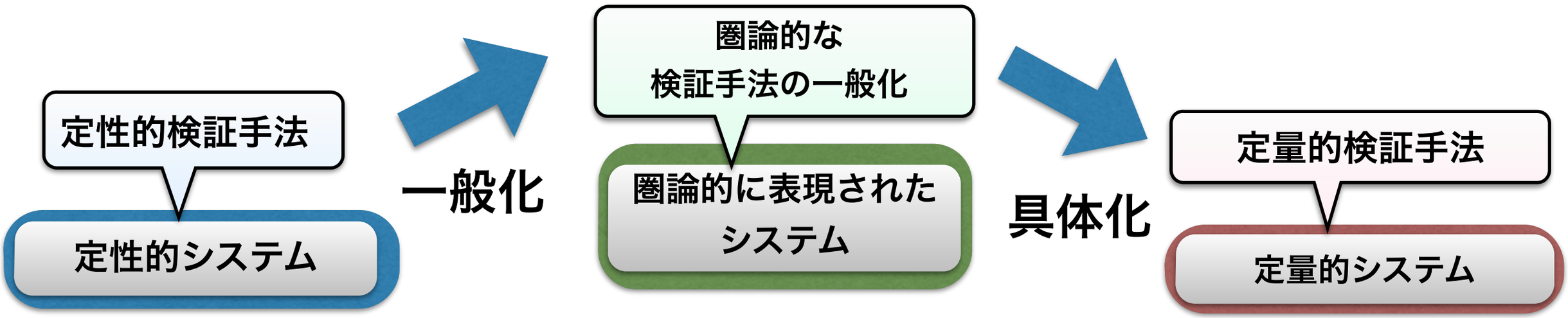
1. "Kleisli Simulation for Real-Weighted Automata and its Algorithm".
   理論計算機科学と圏論ワークショップ（CSCAT）2014, 神奈川大学, 2014年3月
2. "Generic Forward and Backward Simulations III: Quantitative Simulations by Matrices".
   CONCUR 2014, Rome, Italy, 2014年9月. （上記 [1] に伴う発表）
3. "Kleisli Simulation for Infinite Trace".
   理論計算機科学と圏論ワークショップ（CSCAT）2015, 鹿児島大学, 2015年3月
4. "Coalgebraic Infinite Traces and Kleisli Simulations".
   CALCO 2015, Nijmegen, Netherlands, 2015年6月. （上記 [2] に伴う発表）

アウトライン

- Preliminaries
  - 模倣を用いた検証
  - クライスリ模倣
  - Forward Partial Execution
- Contribution
  - 無限トレースに対するクライスリ模倣
  - 無限トレースに対するForward Partial Execution
- まとめ
- 博士課程での研究計画

博士課程の計画

- Parityオートマトン，alternating Parity オートマトン等の模倣を圏論的に一般化，具体化し定量的派生を導出
  [Henzinger, ’02]
  [Fritz & Wilke, ’06]
  - Büchi オートマトンについては既に一定の結果
    [U., Shimizu, Hasuo, ’16, submitted]
- 得られた定量的模倣に**ロバスト性**を加える
- 模倣以外の形式検証の手法についても圏論的に一般化，具体化し定量的派生を導出



Coalgebraic Representation of System

- Represent a system as a pair of Kleisli arrows

initial state　　transition

$$1 \overset{s}{\nrightarrow} X \overset{c}{\nrightarrow} \overline{F}X \quad \text{in} \quad \mathcal{K}\ell(T)$$

T ・・・ monad for branching type

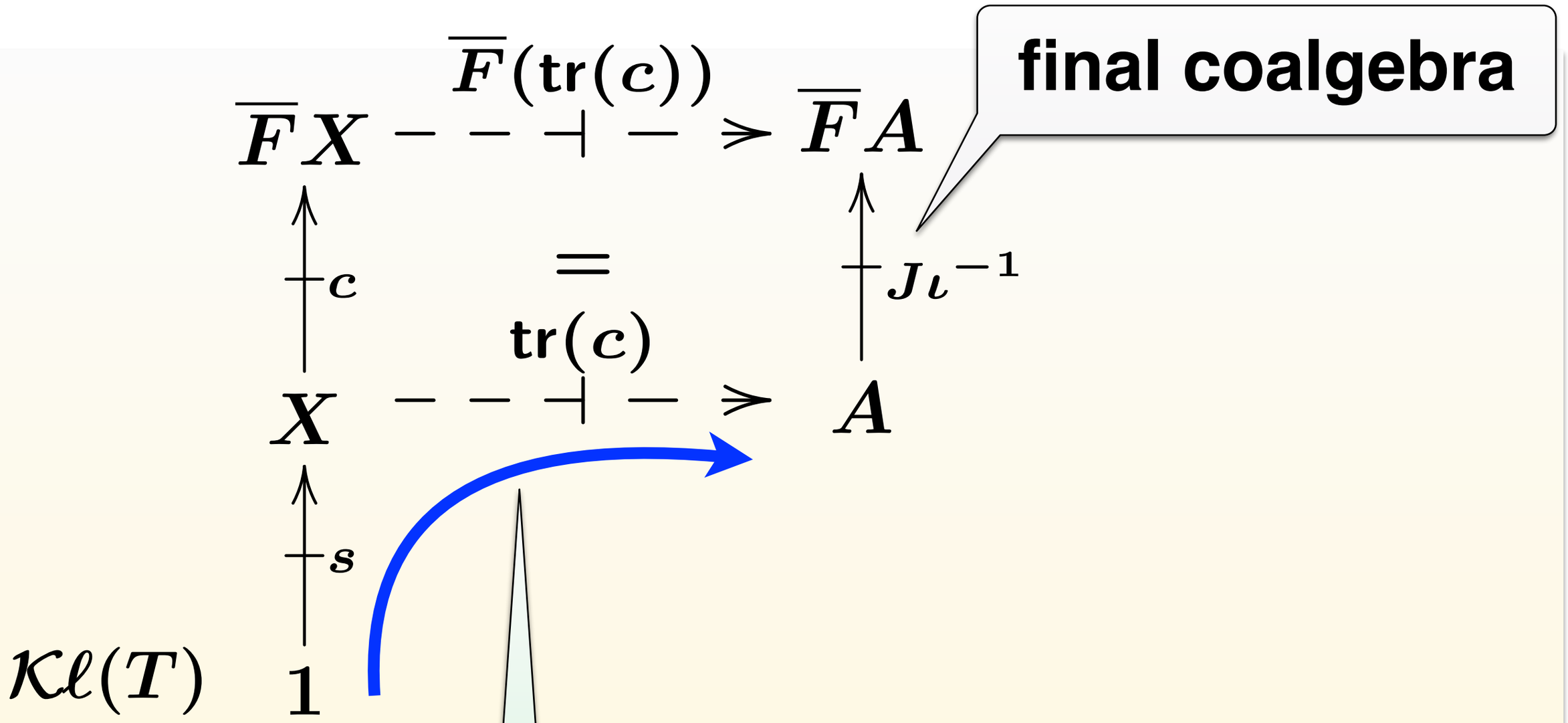
F ・・・ functor for transition type

$\overline{F} : \mathcal{K}\ell(T) \to \mathcal{K}\ell(T)$

Coalgebraic Finite Trace Semantics

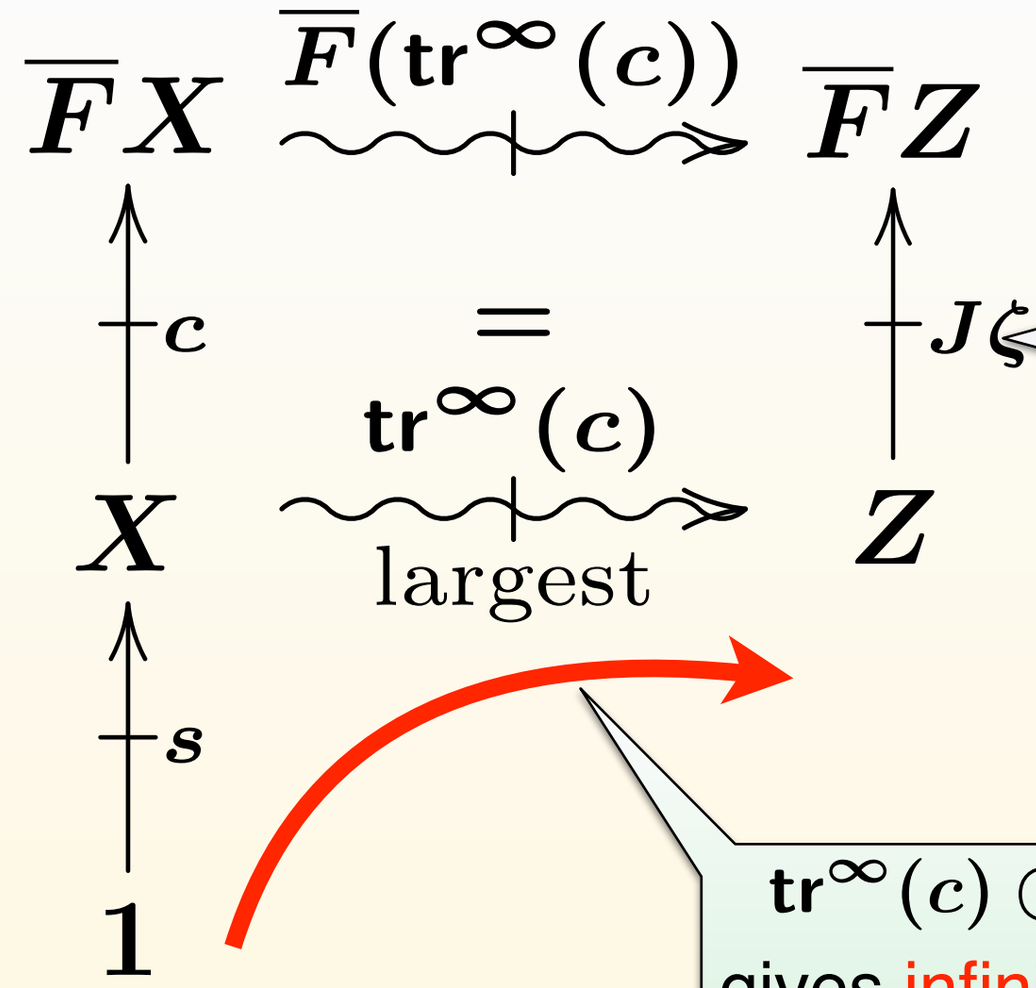
[Hasuo, Jacobs, and Sokolova, '07]

- Finite trace via *final coalgebra*



Coalgebraic Infinite Trace Semantics for **Nondeterministic** system [Jacobs, '04]

- Finite
- Infinite trace via *weakly final coalgebra*



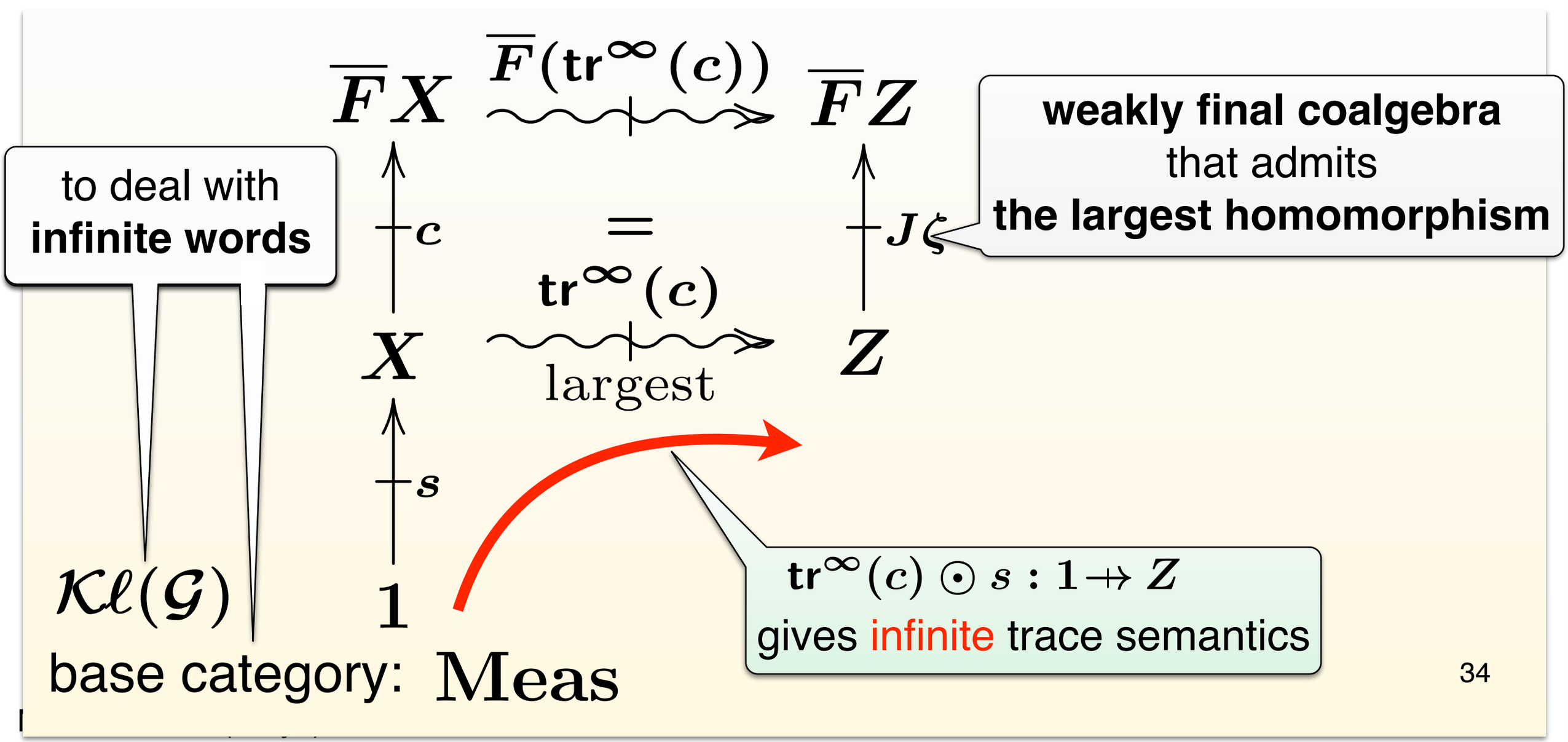
weakly final coalgebra
that admits
the largest homomorphism

$\mathbf{tr}^\infty(c) \odot s : 1 \nrightarrow Z$
gives infinite trace semantics

base category: $\mathbf{Sets}$

Coalgebraic Infinite Trace Semantics for **Probabilistic** system

- Finite
- Infinite trace via *weakly final coalgebra*



Coalgebraic Representation of System

- Various $\mathbf{T}$ and $\mathbf{F}$ for various systems

Example: $1 \overset{s}{\nrightarrow} X \overset{c}{\nrightarrow} \overline{F}X$

Powerset monad

$$T = P \quad PX = \{A \subseteq X\}$$

$$F = 1 + \Sigma \times (\_)$$

→ Non-deterministic automaton

Subdistribution monad

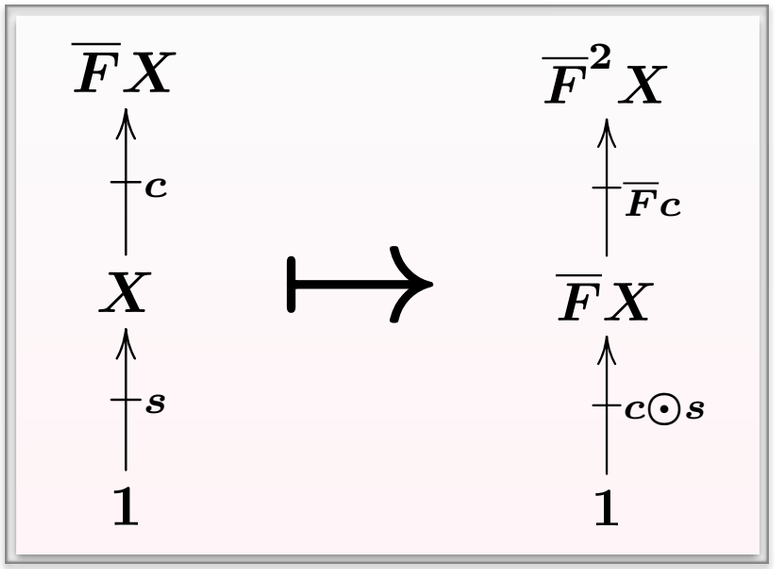
$$T = D \quad DX = \{f : X \to [0,1] \mid \sum_x f(x) \leq 1\}$$

$$F = 1 + \Sigma \times (\_)$$

→ Probabilistic automaton

Forward Partial Execution [U. & Hasuo, '14]

- 圏論的に定義されたシステムの変形



$$\mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y}$$

$$\mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y}$$

- クライスリ模倣を「増やす」ことができる

$$\text{Thm(soundness):}\quad \begin{array}{l} \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} \;\Rightarrow\; \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y} \\ \mathcal{X} \sqsubseteq_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) \;\Rightarrow\; \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y} \end{array}$$

$$\text{Thm(adequacy):}\quad \begin{array}{l} \mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y} \;\Rightarrow\; \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} \\ \mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y} \;\Rightarrow\; \mathcal{X} \sqsubseteq_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) \end{array}$$

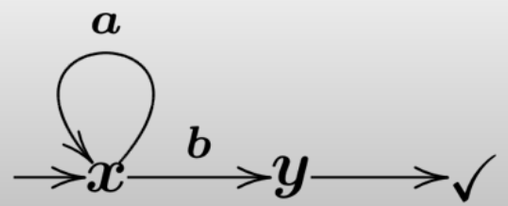
Intuition for FPE

Why incomplete?

How FPE works?

Game-theoretic characterization gives an intuition

Non-det. automaton

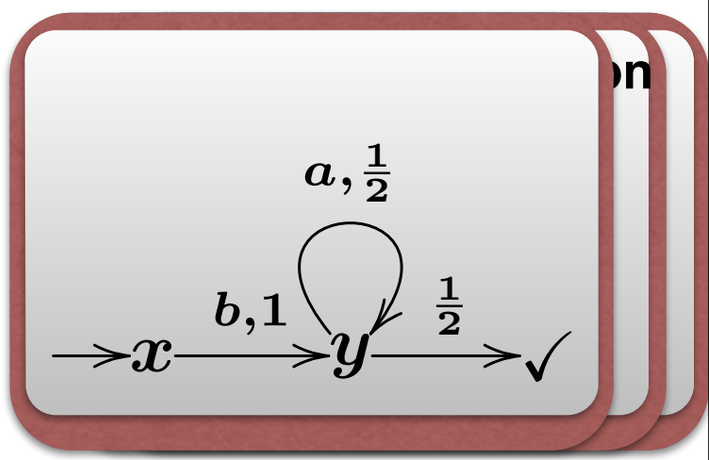


categorical generalization

Systems represented as a coalgebra

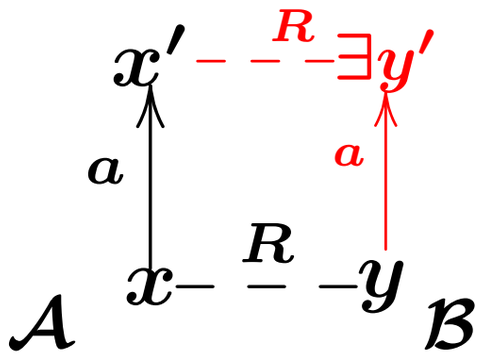
$$1 \xrightarrow{s} X \xrightarrow{c} \overline{F}X$$

specialize

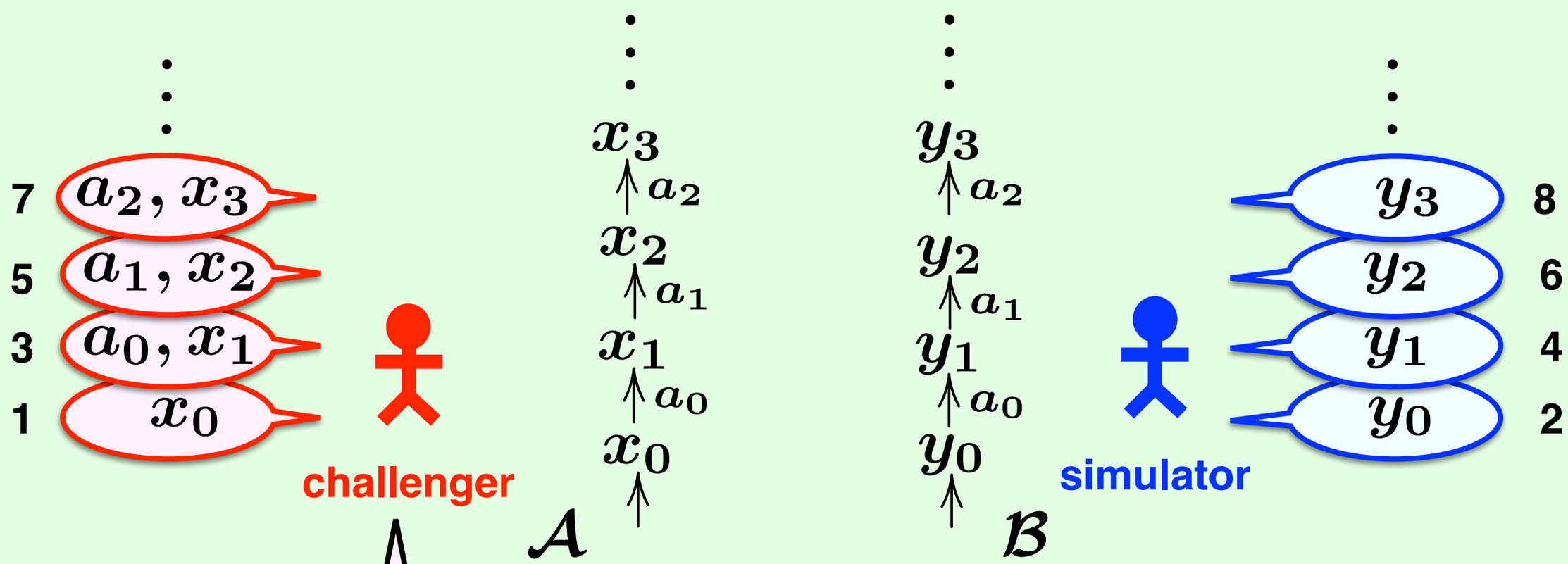


Game-theoretic Characterization of Forward Simulation

- Forward simulation as a two-player game



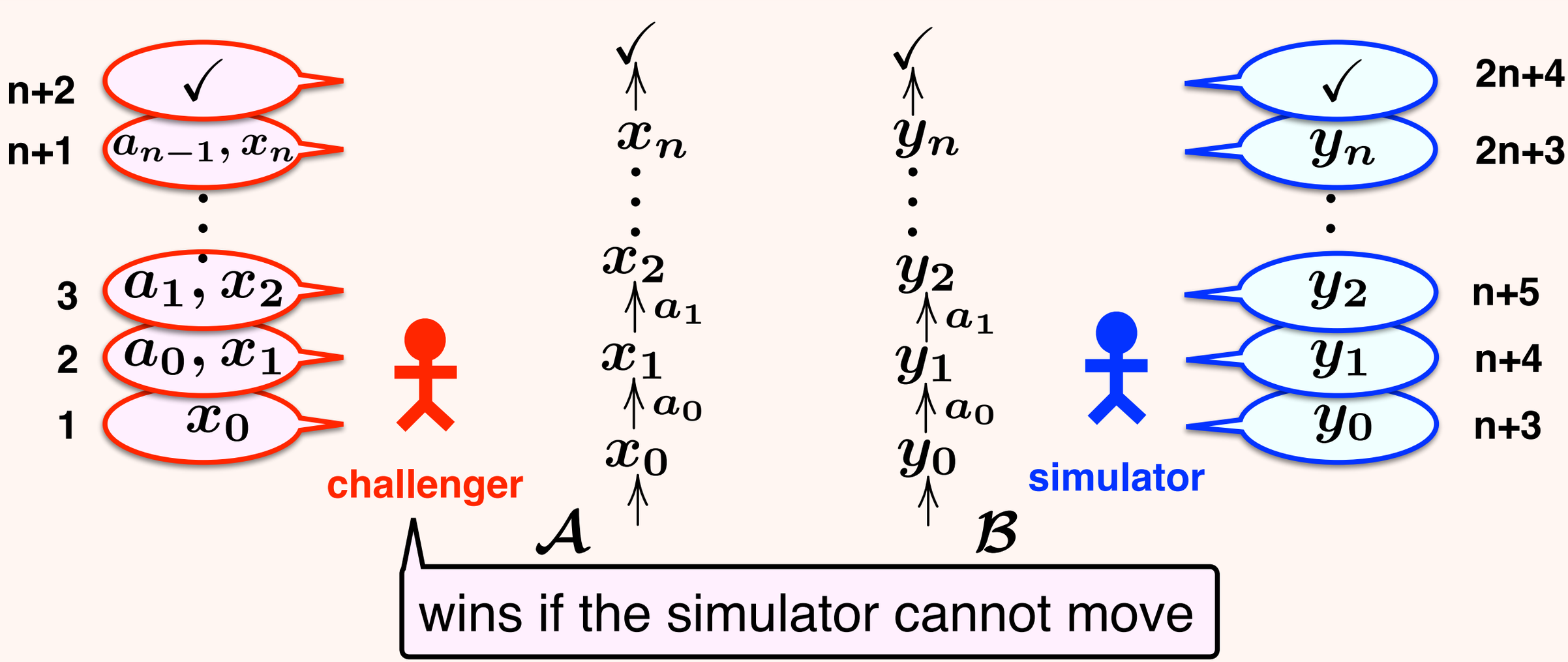
$\Leftrightarrow$ **simulator wins**



Game-theoretic Characterization of Incompleteness

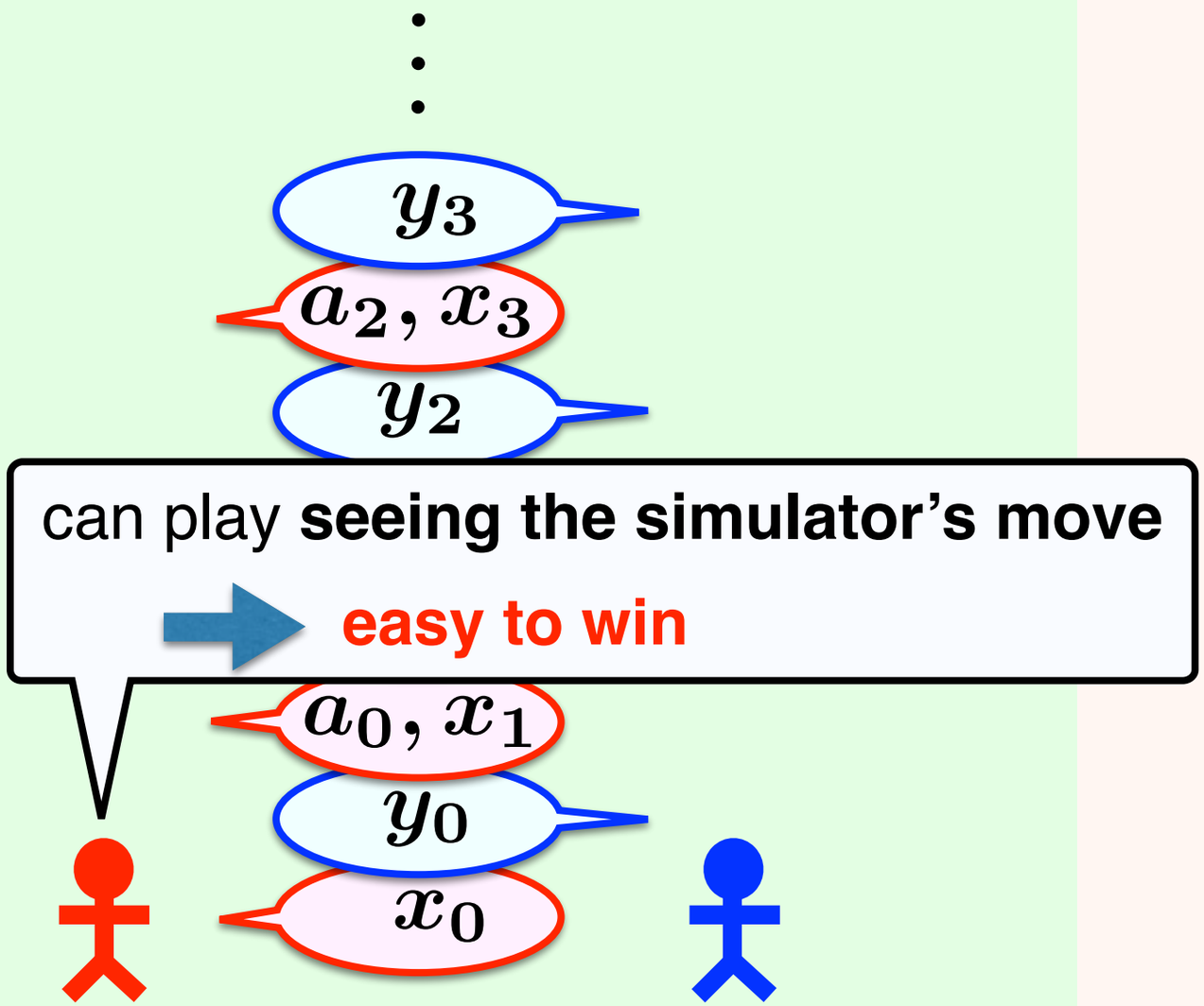
- Language inclusion as a two-player game

$$L(\mathcal{A}) \subseteq L(\mathcal{B}) \iff \textbf{simulator wins}$$

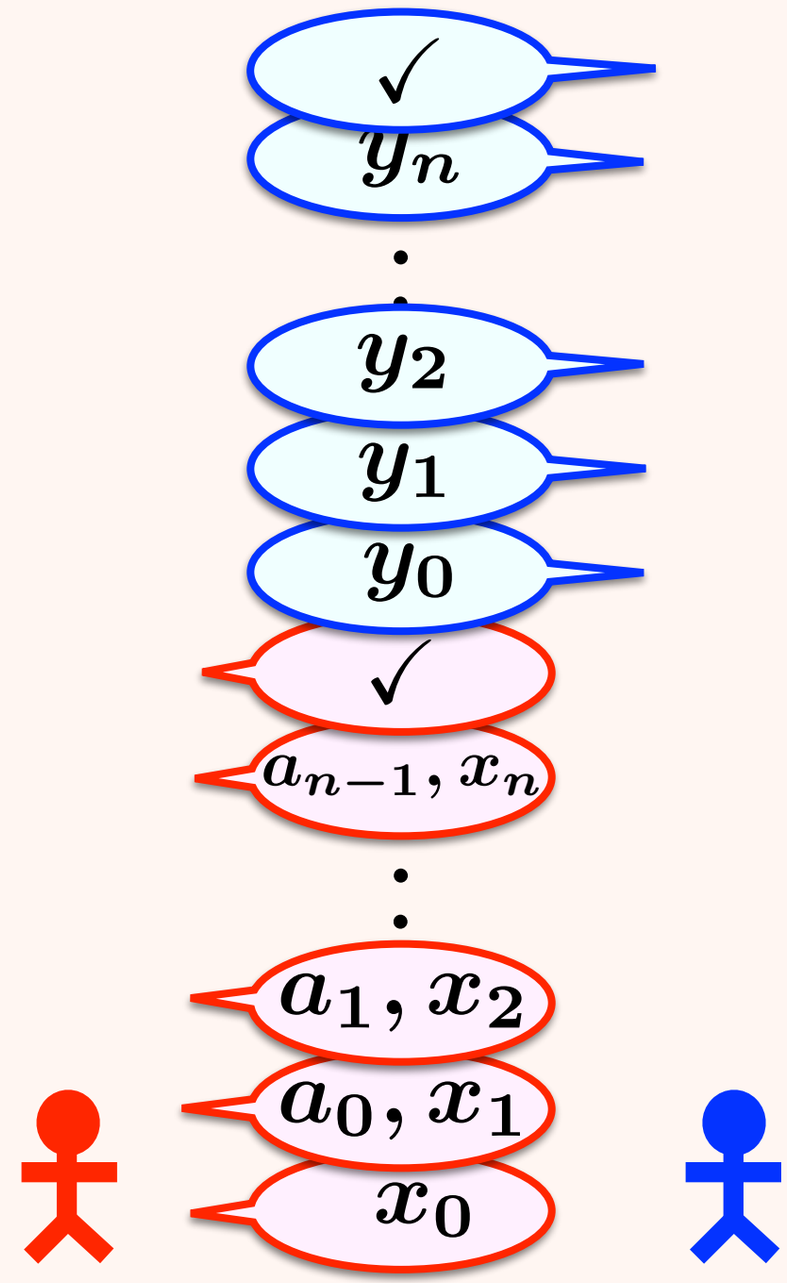


Difference

In simulation game,

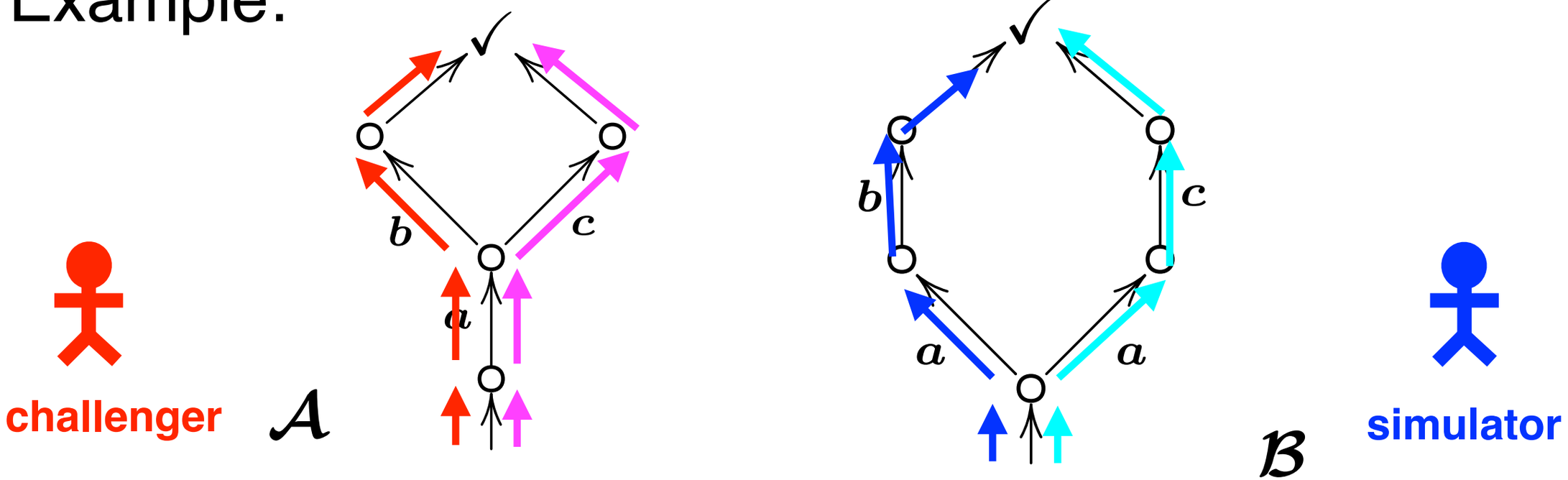


In lang. inclusion game,



Game-theoretic Characterization of Incompleteness

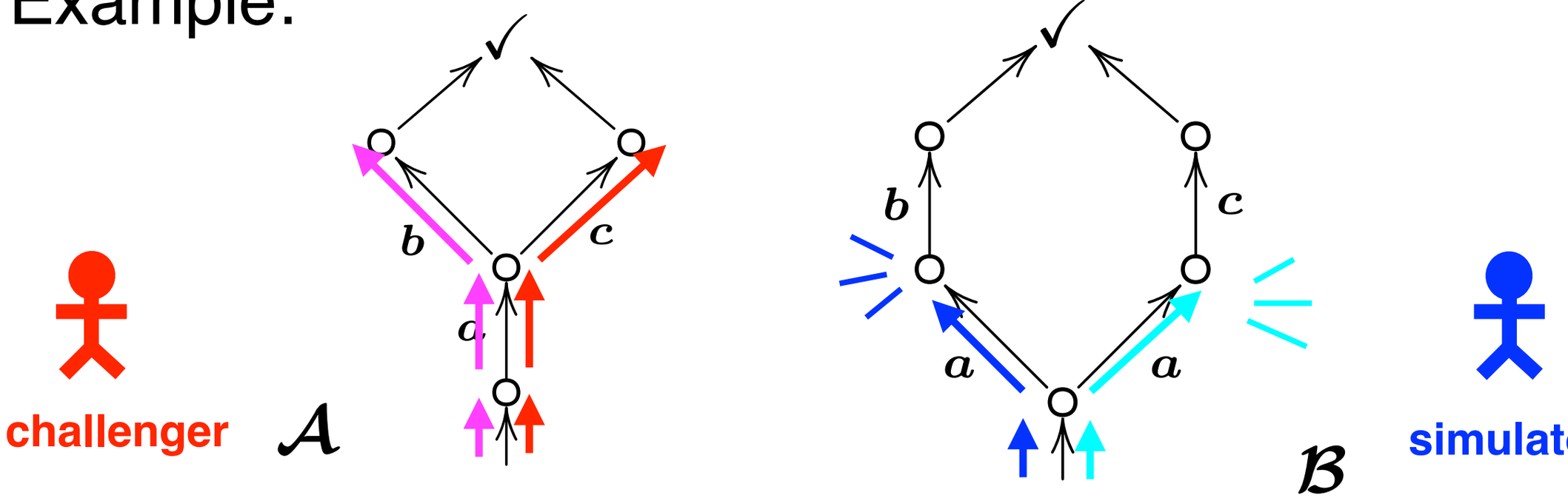
- Example:



- In language inclusion game: simulator wins, i.e. $L(\mathcal{A}) \subseteq L(\mathcal{B})$

Game-theoretic Characterization of Incompleteness

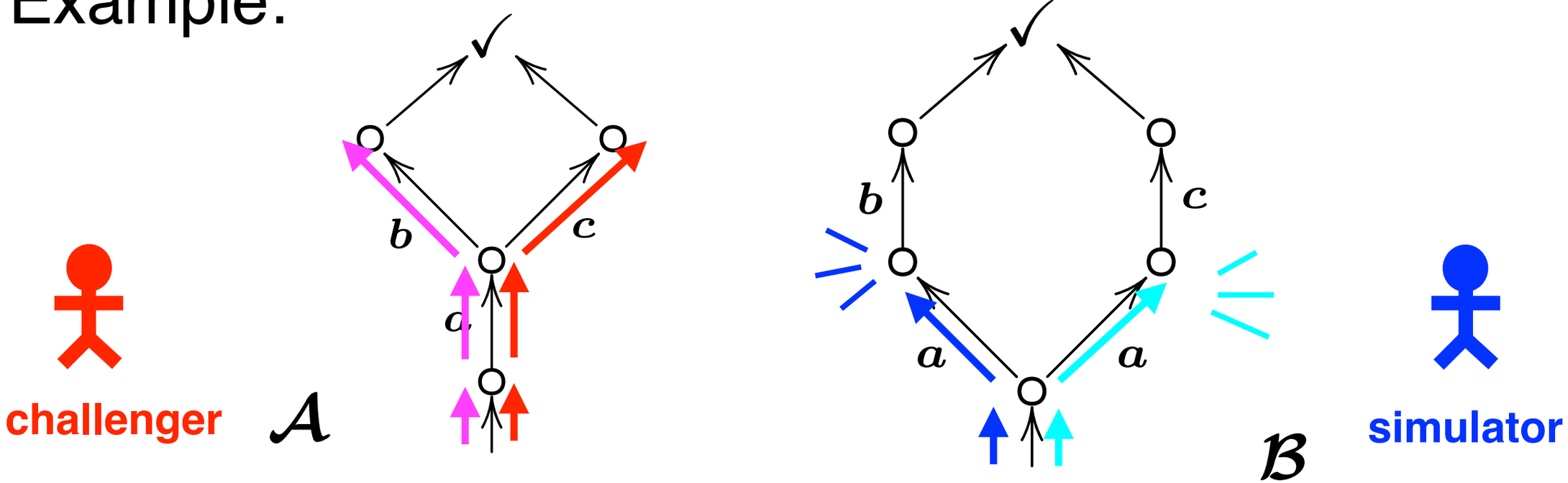
- Example:



- In language inclusion game: simulator wins, i.e. $L(\mathcal{A}) \subseteq L(\mathcal{B})$
- In forward simulation game: challenger wins, i.e. $\mathcal{A} \not\sqsubseteq_{\mathbf{F}} \mathcal{B}$

Game-theoretic Characterization of Incompleteness

- Example:



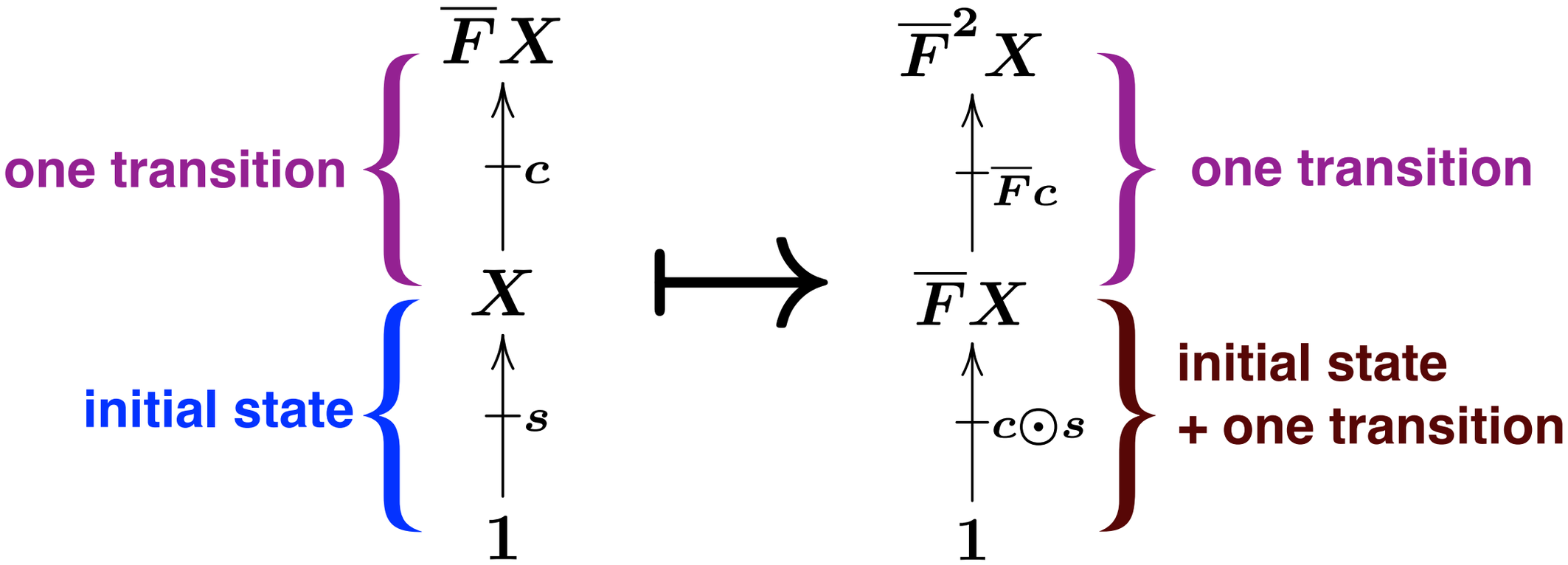
intuition

Earlier decision is a **disadvantage**

Put forward the challenger's decision ⇨ **Simulator wins**

Forward Partial Execution Again

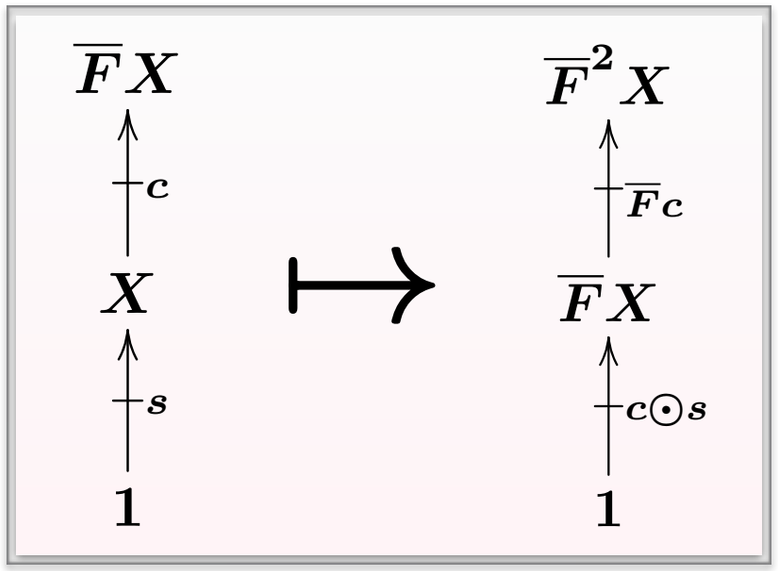
- Transformation of system



- FPE “increases” Kleisli simulations if applied to **proper side**

$$\mathcal{A} \sqsubseteq_{\mathbf{F}} \mathcal{B}$$

Forward Partial Execution (FPE)

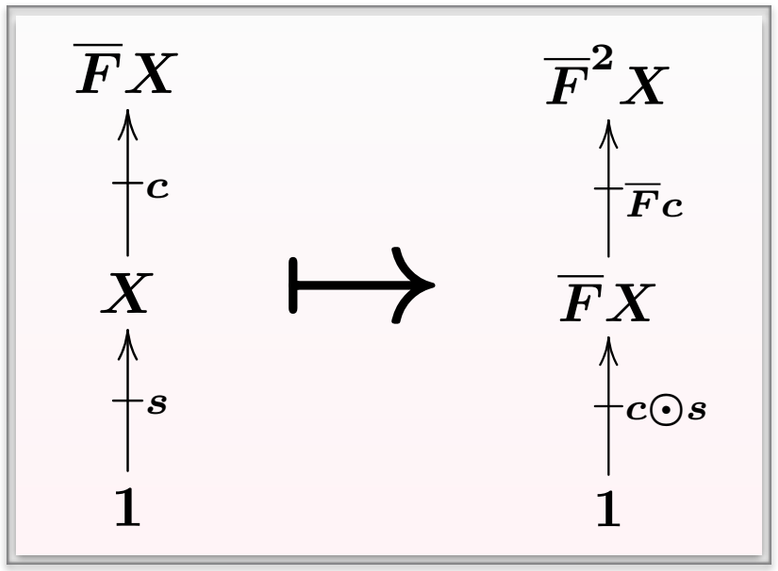


- In finite trace setting, FPE “increases” simulation

$$\text{Thm(soundness):}\quad \begin{aligned} \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} &\Rightarrow \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y} \\ \mathcal{X} \sqsubseteq_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) &\Rightarrow \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y} \end{aligned}$$

$$\text{Thm(adequacy):}\quad \begin{aligned} \mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y} &\Rightarrow \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} \\ \mathcal{X} \sqsubseteq_{\mathbf{B}} \mathcal{Y} &\Rightarrow \mathcal{X} \sqsubseteq_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) \end{aligned}$$

Forward Partial Execution (FPE)



- In infinite trace setting, restricted bwd. sim. is **not** increased

$$\text{Thm(soundness):}\quad \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} \;\Rightarrow\; \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y}$$
$$\mathcal{X} \sqsubseteq^{\infty}_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) \;\Rightarrow\; \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y}$$

$$\text{Thm(adequacy):}\quad \mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y} \;\Rightarrow\; \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y}$$
$$\cancel{\mathcal{X} \sqsubseteq^{\infty}_{\mathbf{B}} \mathcal{Y} \;\Rightarrow\; \mathcal{X} \sqsubseteq^{\infty}_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y})}$$

Sufficient Conditions for Adequacy

- In infinite trace setting,

  If $\mathcal{Y}$ satisfies

  For $T = \mathcal{P}$, $\begin{cases} \forall y \in Y.\ d(y) \neq \emptyset \\ \forall y \in Y.\ d(y) \text{ is finite} \end{cases}$

  total

  image-finite

  For $T = \mathcal{G}$, $\forall y \in Y.\ \int_{y \in FY} dd(y) = 1$

  total

  then

$$\text{Thm(soundness):} \quad \begin{array}{l} \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} \Rightarrow \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y} \\ \mathcal{X} \sqsubseteq^{\infty}_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) \Rightarrow \mathcal{X} \sqsubseteq_{\mathrm{tr}} \mathcal{Y} \end{array}$$

$$\text{Thm(adequacy):} \quad \begin{array}{l} \mathcal{X} \sqsubseteq_{\mathbf{F}} \mathcal{Y} \Rightarrow \mathrm{FPE}(\mathcal{X}) \sqsubseteq_{\mathbf{F}} \mathcal{Y} \\ \mathcal{X} \sqsubseteq^{\infty}_{\mathbf{B}} \mathcal{Y} \Rightarrow \mathcal{X} \sqsubseteq^{\infty}_{\mathbf{B}} \mathrm{FPE}(\mathcal{Y}) \end{array}$$