

形式検証手法の 余代数的抽象化とその応用

郡 茉友子（京都大学 数理解析研究所）

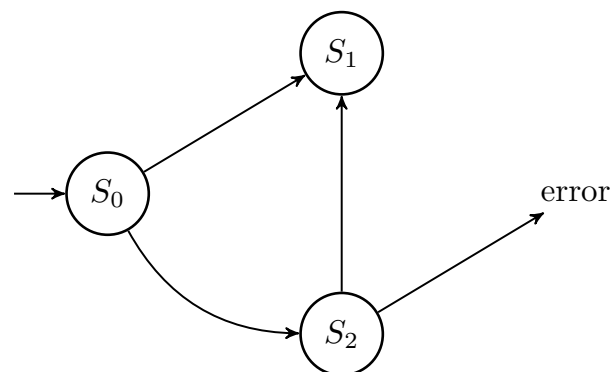
形式検証

- システム（e.g. プログラム）の正しさ・安全性を数学的に検証する
 - e.g. システムが常にエラーを起こさない？ 正常に停止する？
 - システムと検証したい仕様を形式的に記述 → 証明 or 反証
- 形式検証が使われている例
 - エラーが起こると払うコストが高い
→ 自動運転、航空機、ブロックチェーン、…
 - 複雑で人の手で検証するのが大変
→ ハードウェア、ソフトウェア、プログラミング言語の型システム（Haskell, Rustなど）

モデル検査

モデル検査 $M \models \varphi$

- プログラムなどの検証したいシステム
→ 状態遷移システム M
- 仕様 → 時相論理などの論理式 φ (オートマトンで表すことも)
 - e.g. プログラムが必ず停止、エラーを起こす確率(が p 以下)
- 状態遷移システム(モデル)が論理式を満たすかを検査



エラーがずっと起こらない?

$\not\models \Box(\neg \text{error})$

形式検証手法の抽象化

- 手法の様々なシステムへの拡張がそれぞれ開発されている
 - 拡張の妥当性の議論が難しい
 - 拡張が適用できないと経験的に知られていることがある
- 手法群を圏論を用いて抽象化・解析する
 - 手法の本質的な原理、必要な構造がわかる
 - 拡張が一括で手に入る
 - 手法の改善、新手法開発
 - 拡張が単純にはできないことを示せる

今回の講演の主題

目次

1. 背景：モデル検査の余代数、不動点的枠組み
 - 余代数、不動点的意味論
 - 不動点と検証問題
2. product constructionのno-go theorem
 - 余代数的Product construction
 - no-go theorem
3. Recent work：大域的性質のための圏論的フレームワーク

目次

1. 背景：モデル検査の余代数、不動点的枠組み

- 余代数、不動点的意味論
- 不動点と検証問題

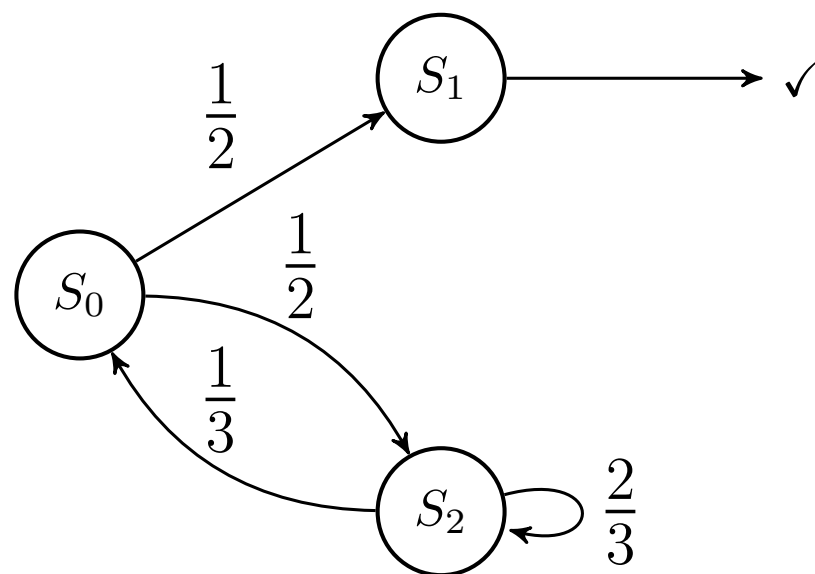
2. product constructionのno-go theorem

- 余代数的Product construction
- no-go theorem

3. Recent work：大域的性質のための圏論的フレームワーク

自己関手に関する余代数

- 余代数 $c: S \rightarrow FS$ (代数 $FA \rightarrow A$) where $F: \mathbb{C} \rightarrow \mathbb{C}$
- 状態遷移システムをモデルするときに使う
 - S が状態の集合、 F が分岐の型、 c が1ステップの振る舞い
 - 例：非決定的な遷移システム $c: S \rightarrow \mathcal{P}S$ ($\mathcal{P}$ は冪集合関手)
 - 例：マルコフ連鎖 $c: S \rightarrow \mathcal{D}S$ ($\mathcal{D}$ は確率分布関手)



$$c(s_0) = (s_1 \mapsto \frac{1}{2}, s_2 \mapsto \frac{1}{2}),$$
$$c(s_2) = (s_0 \mapsto \frac{1}{3}, s_2 \mapsto \frac{2}{3})$$

システムの意味

システム $c: S \rightarrow FS$ の解釈 $FA \rightarrow A$ のもとでの意味 $\llbracket c \rrbracket: S \rightarrow A$

$$\begin{array}{ccc} S & \xrightarrow{\llbracket c \rrbracket} & A \\ c \downarrow & & \uparrow a \\ FS & \xrightarrow{F\llbracket c \rrbracket} & FA \end{array}$$

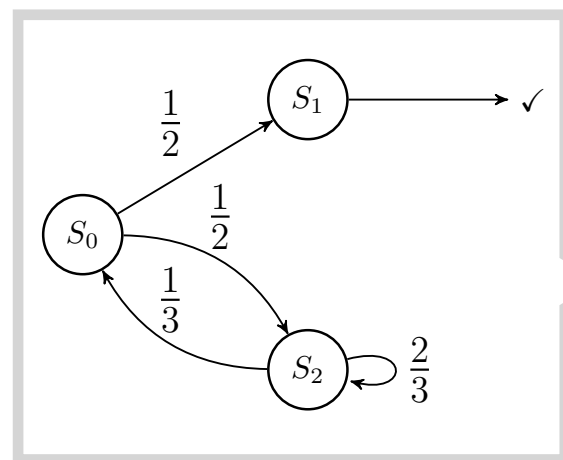
- $\Phi := a \circ F(-) \circ c: \text{Hom}(S, A) \rightarrow \text{Hom}(S, A)$ の不動点
- 検証問題: $\llbracket c \rrbracket$ 自体の計算、 $\llbracket c \rrbracket$ が $\sim$ を満たすか?
- $\llbracket c \rrbracket$ の選び方は様々
 - 最小不動点
 - 普遍性で誘導される射

例 | システムの意味

$\Phi := a \circ F(-) \circ c: A^S \rightarrow A^S$ の最小不動点 $\llbracket c \rrbracket$

存在は $\text{Hom}(S, A)$ の構造で保証 (e.g. $\text{Cpo}_\perp$)

例 (終状態付きマルコフ連鎖)

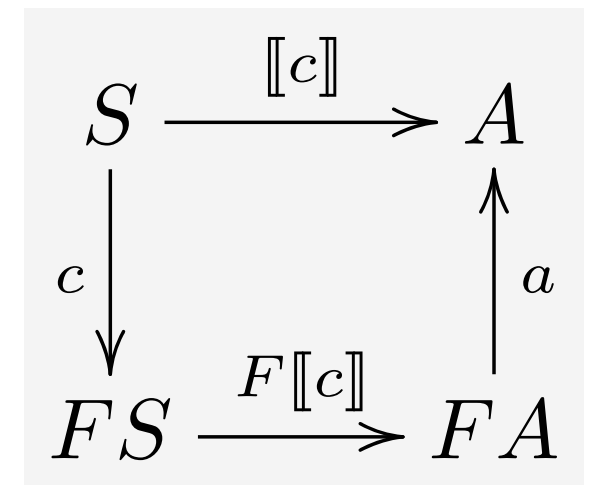


$$\begin{array}{ccc}
 S & \xrightarrow{\llbracket c \rrbracket} & [0, 1] \\
 c \downarrow & & \uparrow a \\
 \mathcal{D}_{\leq 1} S & \xrightarrow{\mathcal{D}_{\leq 1} \llbracket c \rrbracket} & \mathcal{D}_{\leq 1} [0, 1]
 \end{array}$$

given by

$$a(d) := \sum_{r \in [0,1]} r \cdot d(r) + d(\checkmark)$$

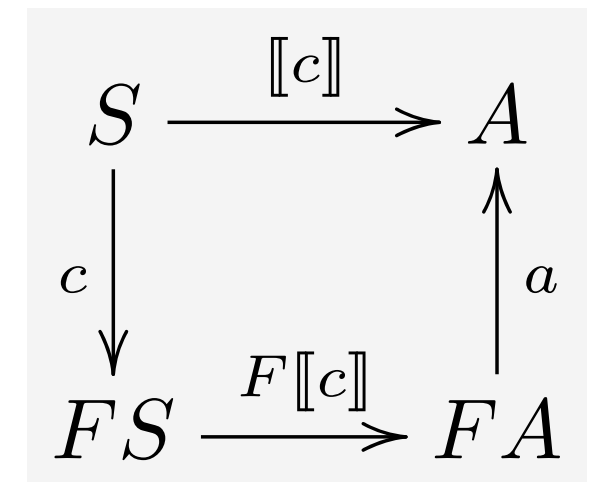
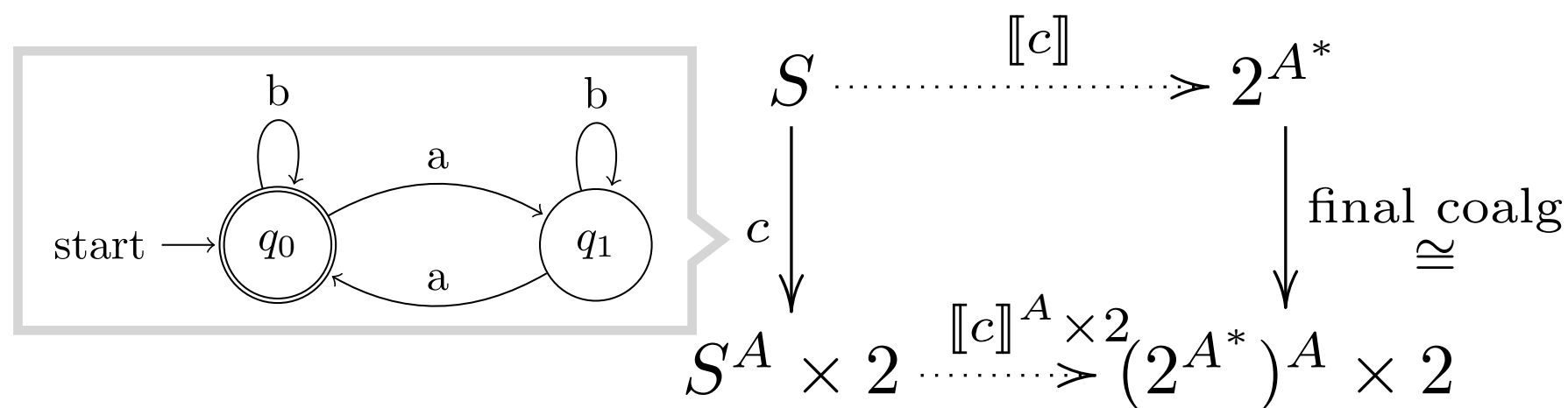
- 確率 $c(s, s')$ で遷移 $s \rightarrow s'$ をする。確率 $(1 - \sum_{s'} c(s, s'))$ で $s \rightarrow \checkmark$
- $\llbracket c \rrbracket(s) \in [0,1]$ は s から終状態 $\checkmark$ に到達する確率



例 | システムの意味

終余代数 a の普遍性で誘導される射 $\llbracket c \rrbracket$

例(決定性オートマトン c)



- $c(s)$ は(1) 遷移 $s \xrightarrow{a} s'$ 、(2) s が受理状態かどうかを表す

- $\llbracket c \rrbracket(s) \in 2^{A^*}$ は、 s から受理される言語 偶数個の a を含む文字列

$\{\vec{a} \in A^* \mid \exists s'. s \xrightarrow{\vec{a}} s' \text{ かつ } s' \text{ が受理状態}\}$ を表す

(脱線) 様々なシステムの意味論

- 計算効果付きのシステムの意味
 - Kleisli, EM categoryを使ったトレース意味論[JacobsSS, JCSS'15]
- Φ を F のfibration ($\mathbb{C}/A \rightarrow \mathbb{C}$)に沿った持ち上げで考える
 - 代数と持ち上げの対応[Aguirre&Katsumata, ENTCS'20]
 - Φ のより一般的な取り方:
代数を持ち上げる最大の持ち上げ (codensity lifting)
 - 述語 $\llbracket c \rrbracket: S \rightarrow A$ ではなく、関係 $\llbracket c \rrbracket: S \times S \rightarrow A$ など拡張できる
- Φ でプログラムの最弱述語変換子をモデル
 - $P \leq \Phi(Q) \Leftrightarrow P\{c\}Q \Leftrightarrow$ 事前に P が成り立ち、プログラム c を実行したら必ず Q が成り立つ

目次

1. 背景：モデル検査の余代数、不動点的枠組み

- 余代数、不動点的意味論
- **不動点と検証問題**

2. product constructionのno-go theorem

- 余代数的Product construction
- no-go theorem

3. Recent work：大域的性質のための圏論的フレームワーク

検証問題

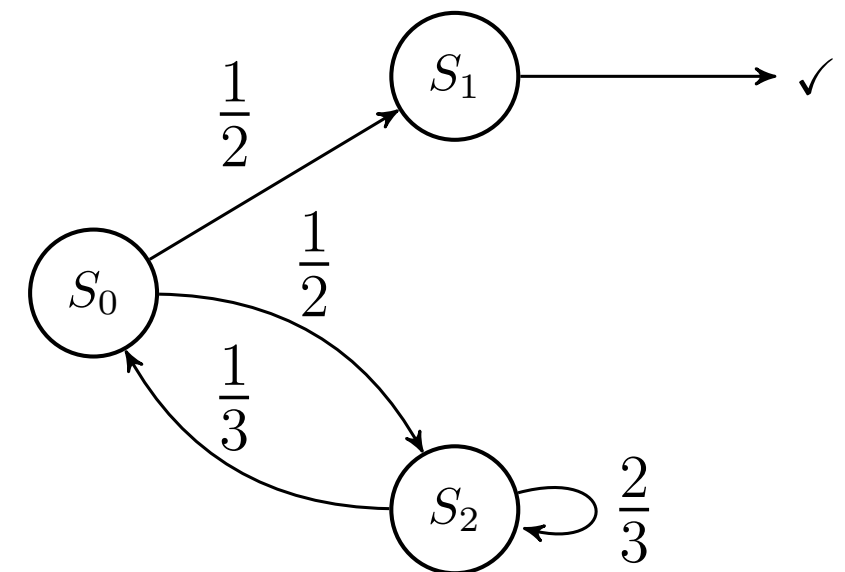
検証問題：システム(の意味 $\llbracket c \rrbracket$, 不動点)が仕様を満たすか？

例(遷移システムの安全性)

- 到達可能な状態の集合($\llbracket c \rrbracket(s_0)$) $\subseteq$? 安全な状態の集合

例(マルコフ連鎖の停止性)

- システムの停止確率($\llbracket c \rrbracket(s_0)$) $\geq$? p
- 仕様を満たす確率自体を計算することも



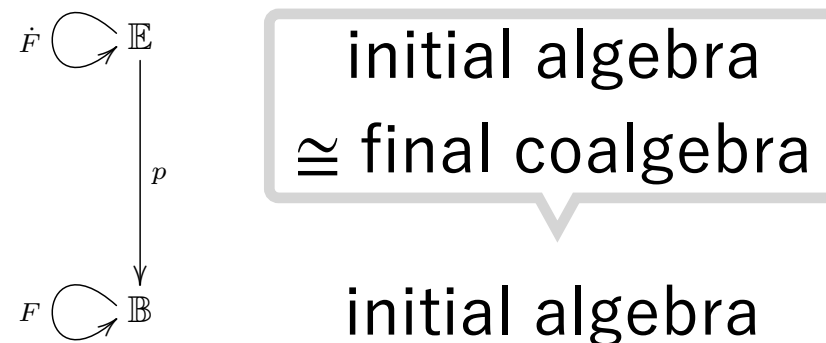
不動点を使った検証手法

- 不動点(Φ の不動点 $\llbracket c \rrbracket$)自体を計算する
 - 最小不動点 $\mu\Phi$ を $\perp \leq \Phi \perp \leq \dots$ の極限として計算する (Kleene theorem)
 - 止まるとは限らない・遅いこともあるので、より早く収束する上昇列を計算する
- 不動点を近似して検証する
 - $\Phi X \leq X \Rightarrow \mu\Phi \leq X$ by Knaster-Tarski theorem
 - このような X はinvariantと呼ばれる。invariantを生成するのは一般に難しく、様々な研究がされている (e.g. constraint-based [GulwaniSV, PLDI'08, SrivastavaG, PLDI'09])

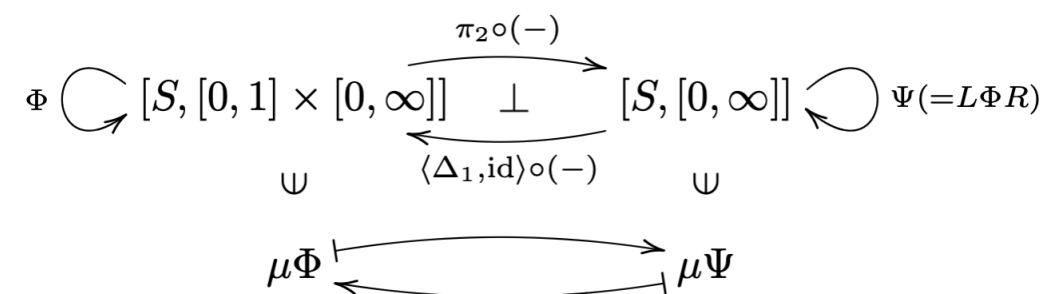
不動点を使った(検証)手法開発

性質によって使える検証手法が異なる → 不動点の性質を調べる

- 最小不動点、最大不動点が一致するのはいつか？
→ 最小不動点の上で(ある条件下で)一致する [Kori+, CONCUR'21]



- 2つの異なる不動点意味論が対応するのはいつか？
→ 到達可能性条件(不動点がある部分に含まれている)
で対応する [Kori+, LICS'25]



不動点を使った(検証)手法開発

既存の(検証)手法の圏論・束論的不動点による理解、拡張、改善

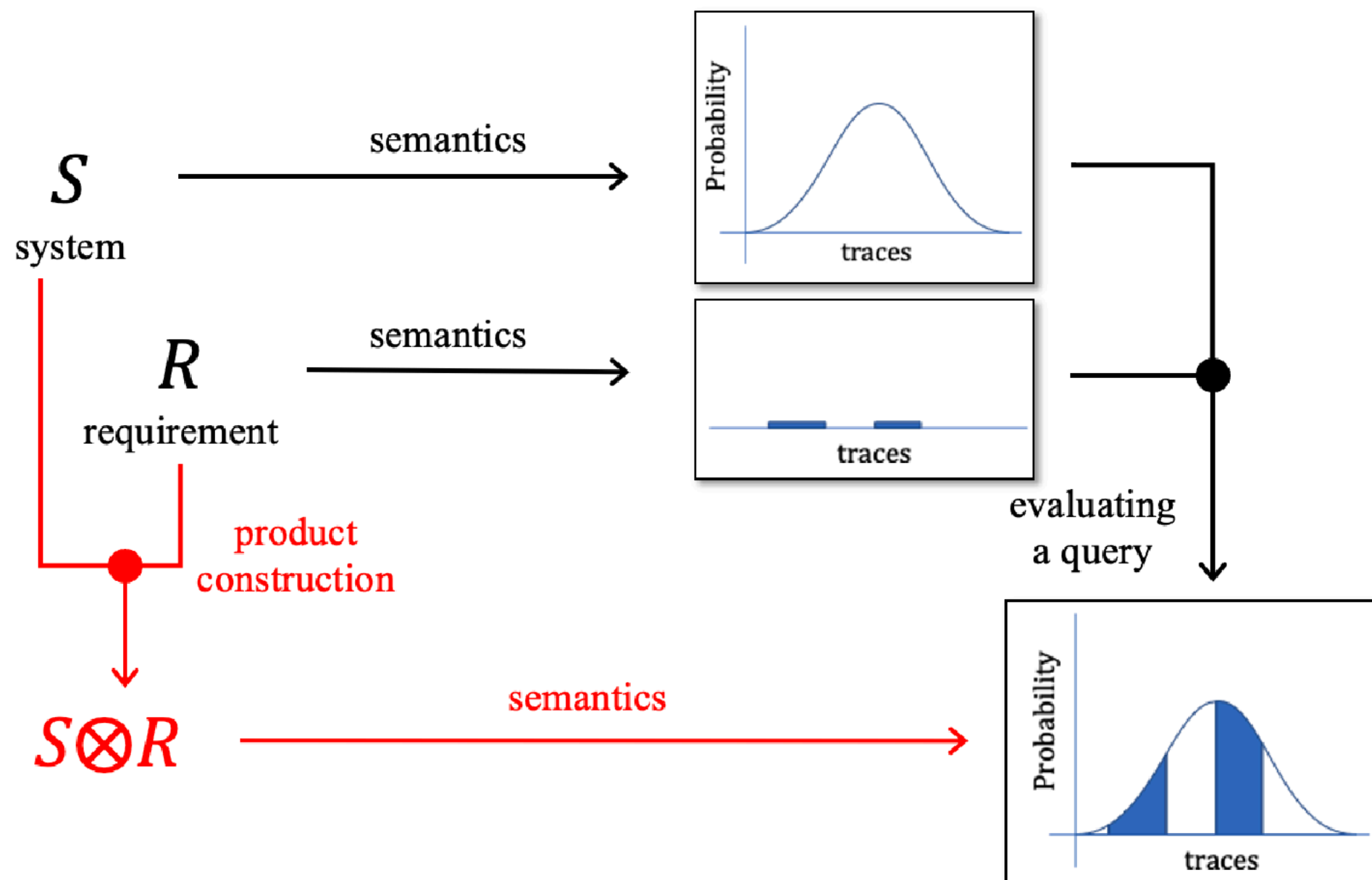
- モデル検査アルゴリズムPDRの抽象化[Kori+, CAV'22, 23]
 - システムに対し双方向の関数 Φ が作れるとき、効率的に不動点の近似を計算している
- Product Constructionの余代数的理解
 - できないことの証明 & 新しいProduct Constructionの提案
[Kori&Watanabe, FoSSaCS'26]
- 強化学習の古典的手法である信念構成の余代数的抽象化
[Kori&Watanabe, CONCUR'26]
 - 信念構成 = 余代数的決定化 + 信念の分割

目次

1. 背景：モデル検査の余代数、不動点的枠組み
 - 余代数、不動点的意味論
 - 不動点と検証問題
2. **product constructionのno-go theorem**
 - **余代数的Product construction**
 - no-go theorem
3. Recent work：大域的性質のための圏論的フレームワーク

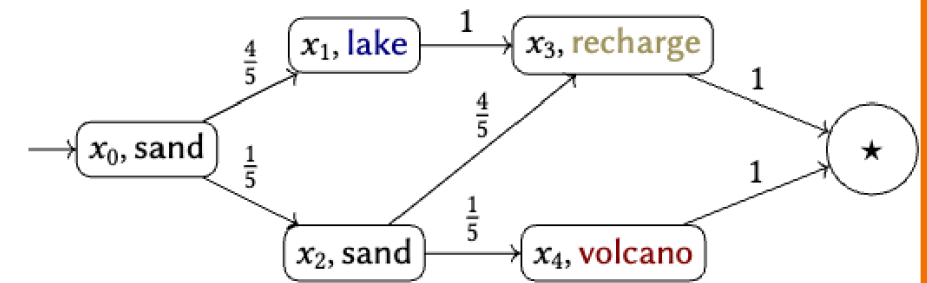
モデル検査のProduct Construction

考える問題：システムの出力が仕様をどのくらい満たすのか？

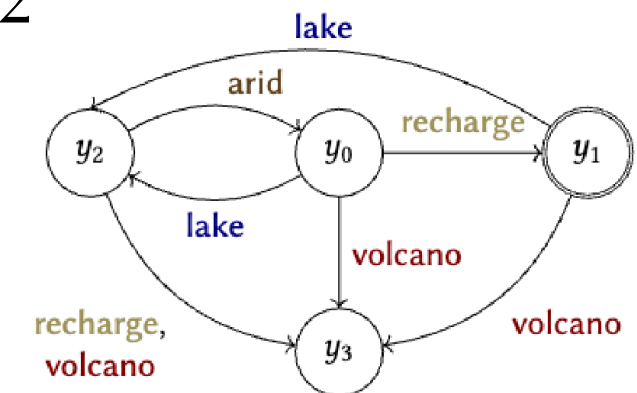


例 | MCとDFAのモデル検査

- システム：マルコフ連鎖 $c: X \rightarrow \mathcal{D}_{\leq 1}(X) \times A$
- $\llbracket c \rrbracket: X \rightarrow \mathcal{D}_{\leq 1}(A^+)$
- $\llbracket c \rrbracket(x)(w)$ は x から w を出力して止まる確率



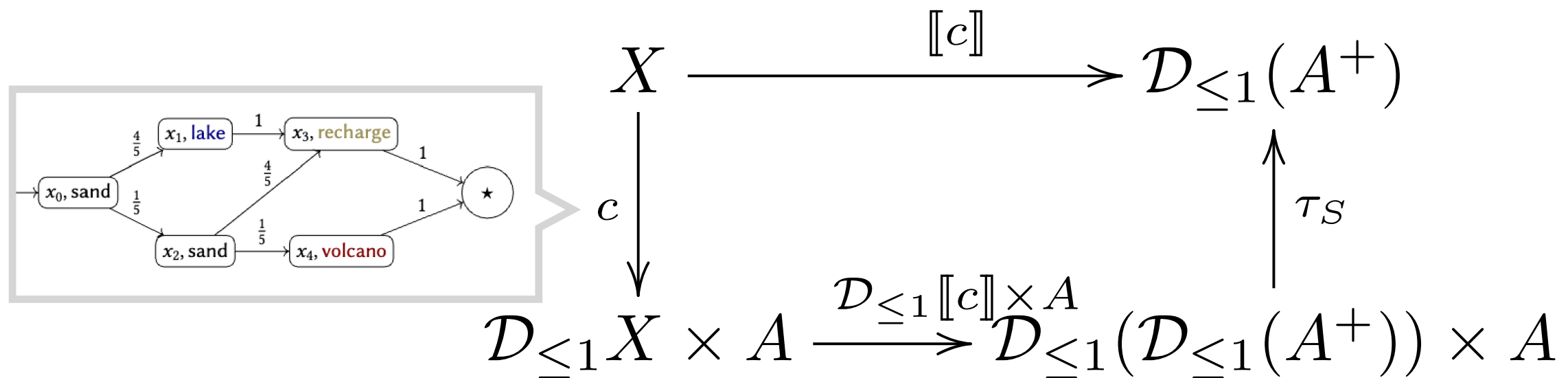
- 仕様：決定性有限オートマトン(DFA) $d: Y \rightarrow (Y \times 2^A)$
- $\llbracket d \rrbracket: Y \rightarrow \mathcal{P}(A^+)$
- $\llbracket d \rrbracket(y) \subseteq A^+$ は y から受理される言語
- モデル検査問題：仕様を満たす出力列 w の確率



(x, y) に対し $\sum_{w \in \llbracket d \rrbracket(y)} \llbracket c \rrbracket(x)(w)$ を計算

例 | MCとDFAのモデル検査

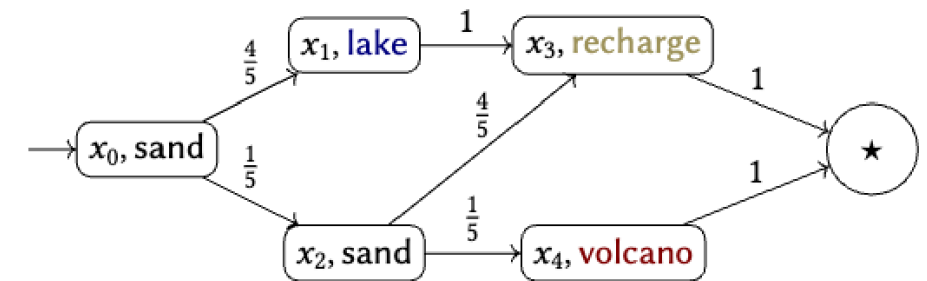
システム：マルコフ連鎖 $c: X \rightarrow \mathcal{D}_{\leq 1}(X) \times A$



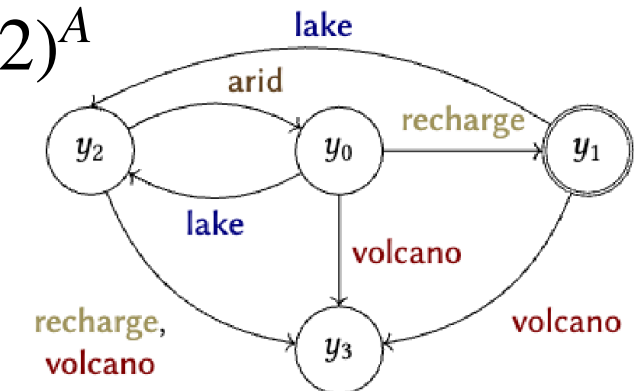
- $\tau_S(\sigma, a)$ は一文字目を a で取って二文字目以降 σ を使って定義される確率分布
- $[[c]]$ は $\tau_S \circ (\mathcal{D}_{\leq 1}(-) \times A) \circ c$ の最小不動点
- $[[c]](x)(w)$ は $x \in X$ から $w \in A^+$ を出力して止まる確率

例 | MCとDFAのモデル検査

- システム：マルコフ連鎖 $c: X \rightarrow \mathcal{D}_{\leq 1}(X) \times A$
 - $\llbracket c \rrbracket: X \rightarrow \mathcal{D}_{\leq 1}(A^+)$
 - $\llbracket c \rrbracket(x)(w)$ は x から w を出力して止まる確率



- 仕様：決定性有限オートマトン(DFA) $d: Y \rightarrow (Y \times 2)^A$
 - $\llbracket d \rrbracket: Y \rightarrow \mathcal{P}(A^+)$
 - $\llbracket d \rrbracket(y) \subseteq A^+$ は y から受理される言語



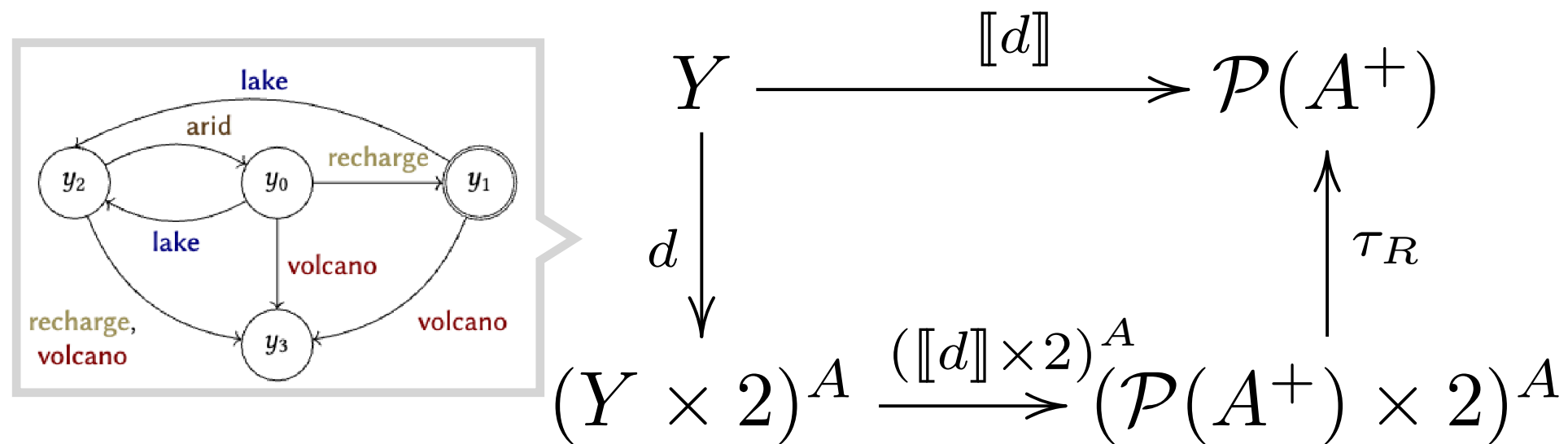
- モデル検査問題：仕様を満たす出力列 w の確率

(x, y) に対し $\sum_{w \in \llbracket d \rrbracket(y)} \llbracket c \rrbracket(x)(w)$ を計算

余代数的Product Construction

例 | MCとDFAのモデル検査

仕様：決定性有限オートマトン(DFA) $d: Y \rightarrow (Y \times 2)^A$

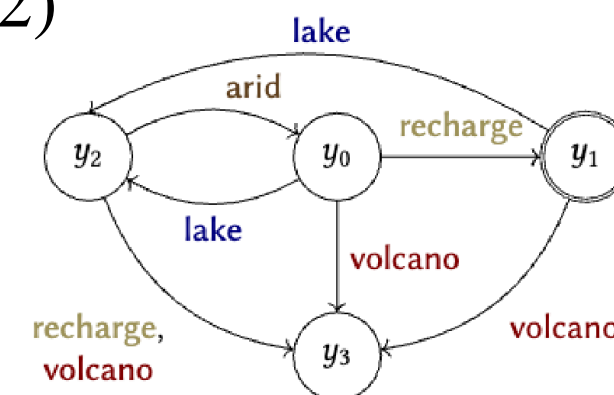
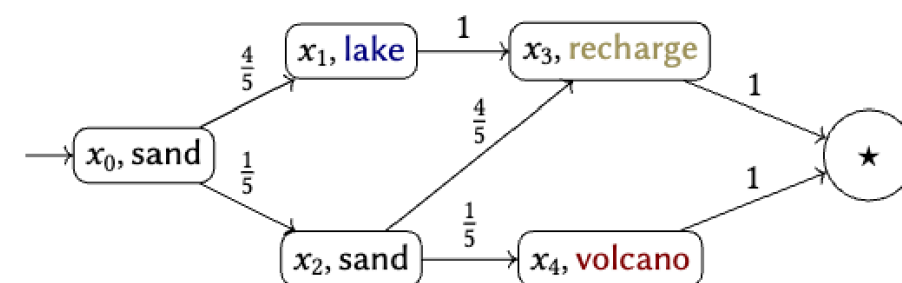


- $\tau_R(a) = \{a \mid \delta(a) = (-, \top)\} \cup \{a \cdot w \mid \delta(a) = (S, -), w \in S\}$
- $[[d]]$ は $\tau_R \circ ((-) \times 2)^A \circ d$ の最小不動点
- $[[d]](y) \subseteq A^+$ は y から受理される言語

例 | MCとDFAのモデル検査

- システム：マルコフ連鎖 $c: X \rightarrow \mathcal{D}_{\leq 1}(X) \times A$
 - $\llbracket c \rrbracket: X \rightarrow \mathcal{D}_{\leq 1}(A^+)$
 - $\llbracket c \rrbracket(x)(w)$ は x から w を出力して止まる確率
- 仕様：決定性有限オートマトン(DFA) $d: Y \rightarrow (Y \times 2)^A$
 - $\llbracket d \rrbracket: Y \rightarrow \mathcal{P}(A^+)$
 - $\llbracket d \rrbracket(y) \subseteq A^+$ は y から受理される言語
- モデル検査問題：仕様を満たす出力列 w の確率

(x, y) に対し $\sum_{w \in \llbracket d \rrbracket(y)} \llbracket c \rrbracket(x)(w)$ を計算



例 | MCとDFAのモデル検査

モデル検査問題：仕様を満たす出力列 w の確率

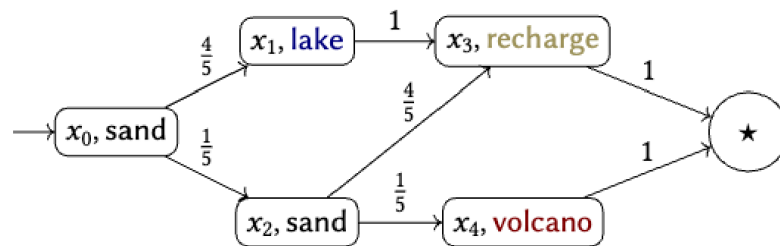
- $\llbracket c \rrbracket: X \rightarrow \mathcal{D}_{\leq 1}(A^+)$, $\llbracket c \rrbracket(x)(w)$ は x から w を出力して止まる確率
- $\llbracket d \rrbracket: Y \rightarrow \mathcal{P}(A^+)$, $\llbracket d \rrbracket(y) \subseteq A^+$ は y から受理される言語
- (x, y) に対し $\sum_{w \in \llbracket d \rrbracket(y)} \llbracket c \rrbracket(x)(w)$ を計算

$q: \mathcal{D}_{\leq 1}(A^+) \times \mathcal{P}(A^+) \rightarrow [0,1]$ を $q(\sigma, S) := \sum_{w \in S} \sigma(w)$ で定義すると、

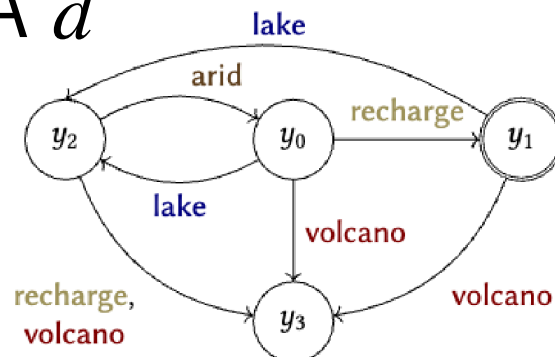
$q \circ (\llbracket c \rrbracket \times \llbracket d \rrbracket): X \times Y \rightarrow [0,1]$ が計算したい問題

Product Construction

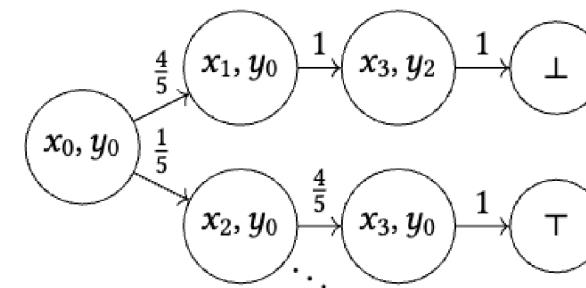
- $\llbracket c \rrbracket$, $\llbracket d \rrbracket$ をそれぞれ計算して $q \circ (\llbracket c \rrbracket \times \llbracket d \rrbracket)$ を得るのは計算コストが高い
 - c と d を同時に走らせるシステム $c \otimes d$ を作り、 $\llbracket c \otimes d \rrbracket (= q \circ (\llbracket c \rrbracket \times \llbracket d \rrbracket))$ を計算する
- マルコフ連鎖 c



DFA d



product マルコフ連鎖 $c \otimes d$



余代数的モデル検査

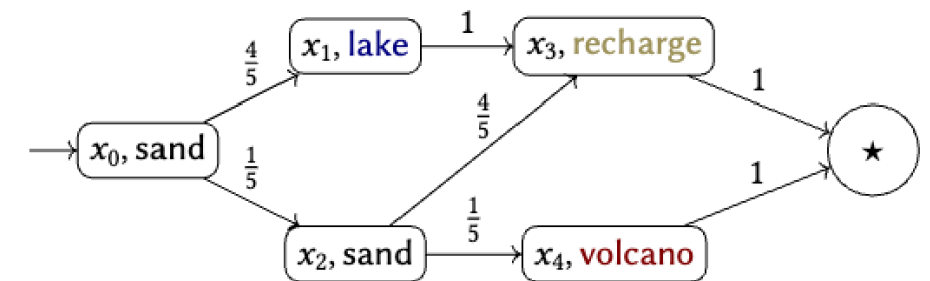
- システム：マルコフ連鎖 $c: X \rightarrow \mathcal{D}_{\leq 1}(X) \times A$

余代数 $c: X \rightarrow F_S(X)$

- $\llbracket c \rrbracket: X \rightarrow \mathcal{D}_{\leq 1}(A^+)$

代数 $\tau_S: F_S(\Omega_S) \rightarrow \Omega_S$
で定義した不動点

- $\llbracket c \rrbracket(x)(w)$ は x から w を出力して止まる確率



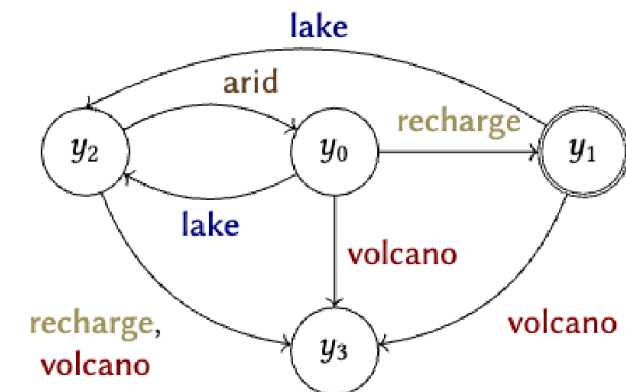
- 仕様：決定性有限オートマトン(DFA) $d: Y \rightarrow (Y \times 2)^A$

余代数 $d: Y \rightarrow F_R(Y)$

- $\llbracket d \rrbracket: Y \rightarrow \mathcal{P}(A^+)$

代数 $\tau_R: F_R(\Omega_R) \rightarrow \Omega_R$
で定義した不動点

- $\llbracket d \rrbracket(y) \subseteq A^+$ は y から受理される言語



- モデル検査問題：仕様を満たす出力列 w の確率

(x, y) に対し $\sum_{w \in \llbracket d \rrbracket(y)} \llbracket c \rrbracket(x)(w)$ を計算

$q: \Omega_S \times \Omega_R \rightarrow \Omega_{S \otimes R}$ で
 $q \circ (\llbracket c \rrbracket \times \llbracket d \rrbracket)$

余代数的Product Construction

Productは自然変換 $\{\lambda_{X,Y}: F_S X \times F_R Y \rightarrow F_{S \otimes R}(X \times Y)\}_{X,Y}$ で定義

- $\text{product } c \otimes_\lambda d := \lambda \circ (c \times d): X \times Y \rightarrow F_{S \otimes R}(X \times Y)$

productの意味 $\llbracket c \otimes_\lambda d \rrbracket$ 代数 $\tau_{c \otimes d}$ で定義した最小不動点

解きたいモデル検査問題がproductの意味を計算すれば解けるか？

- $\llbracket c \otimes_\lambda d \rrbracket = q \circ (\llbracket c \rrbracket \times \llbracket d \rrbracket)$

Prop.[Watanabe+, OOPSLA'25] q がstrict, omega-continuousかつ

$q \circ (\tau_S \times \tau_R) = \tau_{S \otimes R} \circ F_{S \otimes R}(q) \circ \lambda$ ならば $\llbracket c \otimes_\lambda d \rrbracket = q \circ (\llbracket c \rrbracket \times \llbracket d \rrbracket)$

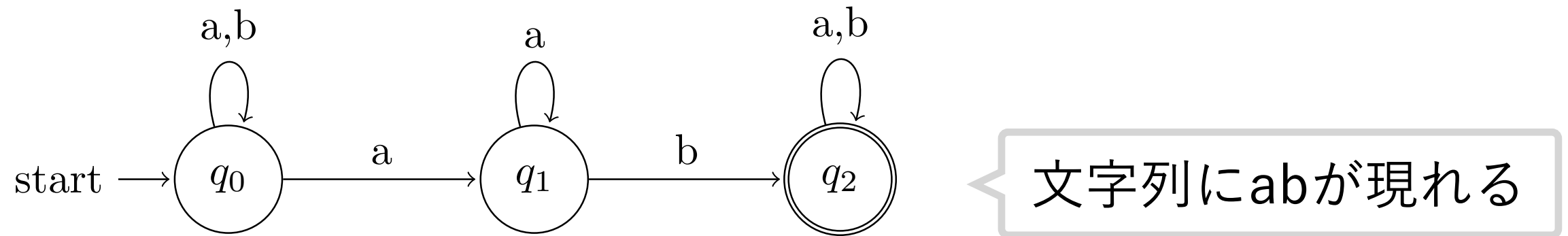
目次

1. 背景：モデル検査の余代数、不動点的枠組み
 - 余代数、不動点的意味論
 - 不動点と検証問題
2. **product constructionのno-go theorem**
 - 余代数的Product construction
 - **no-go theorem**
3. Recent work：大域的性質のための圏論的フレームワーク

No-go theorem for product construction

MCとNFAのproduct construction

- 非決定性有限オートマトン（NFA）：
入力に対し、とりうる遷移が複数個あり得る



- DFAもNFAも表現力は等価だが、DFAの方が状態数が爆発する
- MCとNFAでproduct constructionは（経験的）にできない
 - MCとunambiguousオートマトン（acceptするrunは高々一つ）ではできる[CouvreurSS, LPAR'03, Baier+, JCSC'23, ...]
- この話の形式的な証明を与えた

No-go theorem for product construction

Thm.

MCとNFAに対するモデル検査問題を解くためのproduct MCは存在しない(i.e. $q \circ (\tau_S \times \tau_R) = \tau_{S \otimes R} \circ F_{S \otimes R}(q) \circ \lambda$ を満たす λ は存在しない)

proof sketch. 自然変換 $\{\lambda_{X,Y}: \mathcal{D}_{\leq 1} X \times A \times \mathcal{P}(Y \times 1)^A \rightarrow \mathcal{D}_{\leq 1}(X \times Y + 1)\}_{X,Y}$ に対し、 $\mathcal{P} \Rightarrow \mathcal{D}_{\leq 1}$ がただ一つのみであることを使い、 λ のありうる形を制限する。そのうえで $q \circ (\tau_S \times \tau_R) = \tau_{S \otimes R} \circ F_{S \otimes R}(q) \circ \lambda$ を満たさないことを示す。

- MCとDFA, MFAには存在し、妥当な条件下で唯一
- これらを議論するために、
powerset functor $\mathcal{P}$, subdistribution functor $\mathcal{D}_{\leq 1}$,
multiset functor $\mathcal{M}$ などの間の自然変換を特徴づけた

No-go theorem for product construction

(脱線) モナドのno-go theorem

モナド T, S に対し、モナドの分配則 $\lambda: S \circ T \Rightarrow T \circ S$ があるとき
 $T \circ S$ はモナド $\rightarrow$ 2つの計算効果を合成して計算効果を作れる

no-go theorem: モナドの分配則 $\lambda: S \circ T \Rightarrow T \circ S$ が存在しない

- $\mathcal{D} \circ \mathcal{P} \Rightarrow \mathcal{P} \circ \mathcal{D}$ [VW06], $\mathcal{P} \circ \mathcal{P} \Rightarrow \mathcal{P} \circ \mathcal{P}$ [KS18], $\mathcal{P} \circ \mathcal{D} \Rightarrow \mathcal{D} \circ \mathcal{P}$ [Var03, without proof]
- no-go theoremの十分条件[Zwart22] (e.g. $\mathcal{D} \circ \mathcal{D} \Rightarrow \mathcal{D} \circ \mathcal{D}, \mathcal{L} \circ \mathcal{L} \Rightarrow \mathcal{L} \circ \mathcal{L}$)

モナドの構造と整合的な自然変換 $\lambda: S \circ T \Rightarrow T \circ S$ があるか？

$\rightarrow$ 今回：各関手に与えられた代数の構造と整合的な自然変換

$$\lambda: (\times) \circ (F_S \times F_R) \rightarrow F_{S \otimes R} \circ (\times) \text{ があるか？}$$

No-go theorem for product construction

可換モノイドで与える関手

CMonを可換モノイドの圏とする

Def. $F_{(-)}: \mathbf{CMon} \rightarrow [\mathbf{Set}, \mathbf{Set}]$ は以下で定義する。 $(A, +, 0)$ に、

$$F_A(X) := \{h: X \rightarrow A \mid \text{supp}(h) \text{ is finite}\}, F_A(f)(h) := \sum_{x \in f^{-1}(-)} h(x)$$

Example

- $F_{(\{\perp, \top\}, \vee, \perp)}$ はfinite powerset functor $\mathcal{P}$.

$$F_{(\{\perp, \top\}, \vee, \perp)}(X) \cong \{H \mid H \subseteq X \text{ and } H \text{ is finite}\} = \mathcal{P}(X),$$

$$F_{(\{\perp, \top\}, \vee, \perp)}(f)(H) = \bigvee_{x \in f^{-1}(_)} H(x) \cong \{f(x) \mid x \in H\} = \mathcal{P}(f)$$

- $F_{(\mathbb{N}, +, 0)}$ はmultiset functor $\mathcal{M}$. $R_{\geq 0}^+ := F_{(\mathbb{R}_{\geq 0}, +, 0)}$, $R_{\geq 0}^\times := F_{(\mathbb{R}_{\geq 0}, \times, 1)}$

No-go theorem for product construction

自然変換 $\lambda: F_A \Rightarrow F_B$ の特徴づけ

自然変換 λ の集まり $\text{Nat}(F_A, F_B)$ は集合をなす。この特徴づけを行った

$\text{Nat}(F_A, F_B)$ と同型な集合:

$F_A \setminus F_B$	$\mathcal{P}_f$	$\mathcal{M}$	$\mathcal{R}_{\geq 0}^+$	$\mathcal{R}_{\geq 0}^\times$
$\mathcal{P}_f$	2	1	1	2
$\mathcal{M}$	$2^{\mathbb{N}_{\geq 1}}$	$\mathbb{N}^{\mathbb{N}_{\geq 1}}$	$\mathbb{R}_{\geq 0}^{\mathbb{N}_{\geq 1}}$	$\mathbb{R}_{\geq 0}^{\mathbb{N}_{\geq 1}}$
$\mathcal{R}_{\geq 0}^+$	$2^{\mathbb{R}_{>0}}$	1	$\mathbb{R}_{\geq 0}^{\mathbb{R}_{>0}}$	?

(Non-gray entries are our new results)

No-go theoremのために数だけでなく形まで決定している

► **Corollary 1** (from Proposition 21). *There is an isomorphism $\lambda(_): [0, 1]^{\mathbb{N}_{\geq 1}} \rightarrow \text{Nat}(\mathcal{M}, \mathcal{D}_{\leq 1})$ defined by*

$$\lambda_X^b(f)(x) = \begin{cases} \frac{f(x)}{\sum_{x \in X} f(x)} \cdot b(\sum_{x \in X} f(x)) & \text{if } \sum_{x \in X} f(x) > 0, \\ 0 & \text{if } \sum_{x \in X} f(x) = 0. \end{cases}$$

No-go theorem for product construction

自然変換 $\lambda: F_A \Rightarrow F_B$ の特徴づけ

自然変換 λ の集まり $\text{Nat}(F_A, F_B)$ は集合をなす。この特徴づけを行った $\text{Nat}(F_A, F_B)$ と同型な集合:

$F_A \setminus F_B$	$\mathcal{P}_f$	$\mathcal{M}$	$\mathcal{R}_{\geq 0}^+$	$\mathcal{R}_{\geq 0}^\times$
$\mathcal{P}_f$	2	1	1	2
$\mathcal{M}$	$2^{\mathbb{N}_{\geq 1}}$	$\mathbb{N}^{\mathbb{N}_{\geq 1}}$	$\mathbb{R}_{\geq 0}^{\mathbb{N}_{\geq 1}}$	$\mathbb{R}_{\geq 0}^{\mathbb{N}_{\geq 1}}$
$\mathcal{R}_{\geq 0}^+$	$2^{\mathbb{R}_{>0}}$	1	$\mathbb{R}_{\geq 0}^{\mathbb{R}_{>0}}$	?

(Non-gray entries are our new results)

Remark: $F_{(_)}$ は faithful だが full ではない

- **CMon** の任意の射 $i: (\mathbb{N}, +, 0) \rightarrow (2, \vee, \perp)$ は $i(n) = i(1)$ を満たす。
よって $\mathbf{CMon}((\mathbb{N}, +, 0), (2, \vee, \perp)) \cong 2$
- $\text{Nat}(F_{\mathbb{N}}, F_2) \cong \text{Nat}(\mathcal{M}, \mathcal{P}_f) \cong 2^{\mathbb{N}_{\geq 1}}$ が成り立つ

No-go theorem for product construction

自然変換 $\lambda: F_A \Rightarrow F_B$ の特徴づけ

主に 2 つの場合を考えた

1. A が一元生成のとき (e.g. $\mathcal{P} = F_{(\{\perp, \top\}, \vee, \perp)}$, $\mathcal{M} = F_{(\mathbb{N}, +, 0)}$)

- $\mathcal{P} \Rightarrow \mathcal{D}_{\leq 1}$ が唯一 $\rightarrow$ MC と NFA の no-go
- $\mathcal{M} \Rightarrow \mathcal{R}_{\geq 0}^+$ が $b: \mathbb{N}_{\geq 1} \rightarrow \mathbb{R}_{\geq 0}$ で決まる $\rightarrow$ MC と MFA の唯一性

2. $F_A = \mathcal{R}_{\geq 0}^+$ のとき ($A = (\mathbb{R}_{\geq 0}, +, 0)$)

- $\mathcal{D}_{\leq 1} \Rightarrow \mathcal{R}_{\geq 0}^+$ が $b: [0, 1] \rightarrow \mathbb{R}_{\geq 0}$ で決まる $\rightarrow$ MC と MFA の唯一性

No-go theorem for product construction

$\lambda: F_A \Rightarrow F_B$ の性質

Lem. $n \cdot f(x) = f(x) \Rightarrow n \cdot \lambda_X(f)(x) = \lambda_X(f)(x)$, for each $f \in F_A(X)$, $n \in \mathbb{N}$, $x \in X$.

- $n = 0$ を考えると、 $f(x) = 0 \Rightarrow \lambda_X(f)(x) = 0$
- $n = 2$ を考えると、 $f(x)$ がidempotent $\Rightarrow \lambda_X(f)(x)$ もidempotent

► **Lemma 16.** Let A and B be commutative monoids, and $\lambda: F_A \Rightarrow F_B$ be a natural transformation. For each $f \in F_A(X)$, $x \in X$, $a \in A$, $n, m \in \mathbb{N}$, and $\triangleright_1, \triangleright_2 \in \{=, \geq\}$, we assume that

$$f(x) \triangleright_1 n \cdot a, \quad \text{and} \quad \sum_{x' \in X \setminus \{x\}} f(x') \triangleright_2 m \cdot a.$$

Then there are $a_1, a_2 \in A$ such that $f(x) = n \cdot a + a_1$ and $\sum_{x' \in X \setminus \{x\}} f(x') = m \cdot a + a_2$ by definition of $\triangleright_1$ and $\triangleright_2$. For these a_1 and a_2 , the following relations hold:

$$\lambda_X(f)(x) \triangleright_1 n \cdot \lambda_{\mathbf{n}+\mathbf{m}+\mathbf{2}}(f')(1), \quad \sum_{x' \in X \setminus \{x\}} \lambda_X(f)(x') \triangleright_2 m \cdot \lambda_{\mathbf{n}+\mathbf{m}+\mathbf{2}}(f')(1),$$

where $f' \in F_A(\mathbf{n} + \mathbf{m} + \mathbf{2})$ is defined by $f'(n + m + 1) := a_1$, $f'(n + m + 2) := a_2$, and $f'(i) := a$ for each $i \in \mathbf{n} + \mathbf{m}$.

$$a \leq a' \\ \text{iff } \exists a'' . a + a'' = a'$$

- $f(x)$ の $\sum_x f(x)$ に対する (有理数による) 割合は $\lambda_X(f)(x)$ の $\sum_x \lambda_X(f)(x)$ に対する割合と一致

Characterisation of natural trans

Aが一元生成のとき

Case 1: $A = (\perp \rightarrow a \rightarrow 2 \cdot a \rightarrow \dots)$

There exists an isomorphism $\lambda^{(-)}: \{b \in B^{\mathbb{N}} \mid b(0) = 0\} \rightarrow \text{Nat}(F_A, F_B)$:

$$\lambda_X^b(f)(x) := N(f(x)) \cdot b\left(\sum_{x \in X} N(f(x))\right).$$

- e.g. $\mathcal{M} \Rightarrow \mathcal{R}_{\geq 0}^+$ is determined by $b: \mathbb{N}_{\geq 1} \rightarrow \mathbb{R}_{\geq 0}$

Case 2: $A = (\perp \rightarrow a \rightarrow \dots \rightarrow (n-1) \cdot a)$

Let n be the least natural number such that $n > 1$ and $n \cdot a = a$. There exists an isomorphism $\lambda^{(-)}: \{c \in B \mid n \cdot c = c\}^{\{0, \dots, n-2\}} \rightarrow \text{Nat}(F_A, F_B)$ given by

$$\lambda_X^b(f)(x) := N(f(x)) \cdot b\left(\left[\sum_{x \in X} N(f(x))\right]\right),$$

where $[l]$ is the remainder of l modulo $n-1$.

- e.g. $\mathcal{P}_f \Rightarrow \mathcal{R}_{\geq 0}^+$ is unique. $(\{c \mid c^2 = c\}^0 \cong 1)$

Characterisation of natural trans

Aが一元生成のとき

Subfunctorに対しても特徴づけられる

Prop.

- No natural trans $\mathcal{P}_f \Rightarrow \mathcal{D}$ exists.
- There exists a unique $\mathcal{P}_f \Rightarrow \mathcal{D}_{\leq 1}$.
- No natural trans $\mathcal{M} \Rightarrow \mathcal{D}$ exists.
- There is an isom $\lambda^{(-)}: [0,1]^{\mathbb{N}_{\geq 1}} \rightarrow \text{Nat}(\mathcal{M}, \mathcal{D}_{\leq 1})$ defined by

$$\lambda_X^b(f)(x) = \begin{cases} \frac{f(x)}{\sum_{x \in X} f(x)} \cdot b\left(\sum_{x \in X} f(x)\right) & \text{if } \sum_{x \in X} f(x) > 0, \\ 0 & \text{if } \sum_{x \in X} f(x) = 0. \end{cases}$$

$\mathcal{P}_f \Rightarrow \mathcal{R}_{\geq 0}^+$ is unique, and is Δ_0 .
 Δ_0 in $\mathcal{D}_{\leq 1}X$ but not in $\mathcal{D}X$

No-go theorem for product construction

まとめ・その他の結果

- product construction:
モデルと仕様を表すシステムたちのproduct $c \otimes d$ の意味を計算し、
効率的にモデル検査問題を解く手法
- 余代数的product constructionの枠組みで、以下を示した
 - MCとNFAのproduct constructionのNo-go theorem
 - MCとMFAのproduct constructionの唯一性
- MCとMFAのproduct constructionを新手法として提案
 - MFAのpolynomial ambiguityのもとでpolynomial timeで解ける

目次

1. 背景：モデル検査の余代数、不動点的枠組み
 - 余代数、不動点的意味論
 - 不動点と検証問題
2. product constructionのno-go theorem
 - 余代数的Product construction
 - no-go theorem
3. **Recent work：大域的性質のための圏論的フレームワーク**

(関手的)圏論的意味論

syntaxの圏

semanticsの圏

$$\llbracket - \rrbracket : \mathbb{C} \rightarrow \mathbb{D}$$

- $\mathbb{C}$ は意味論を与えたいもの(e.g. プログラム)を表す
- $\llbracket . \rrbracket$ は $\mathbb{C}$ の構造を保つ (e.g. $\llbracket f \circ g \rrbracket = \llbracket f \rrbracket \circ \llbracket g \rrbracket$)
→ プログラム全体の意味を各部分の意味を組み合わせて表せる
- 不動点の扱い方: initial algebra, final coalgebra, trace in monoidal cat, ...
- 局所的な(各部分でチェックすれば十分な)性質を扱うのは得意
→ 大域的な性質は?

大域的な性質で唯一存在する不動点

例

- 遷移システム $c: S \rightarrow \mathcal{P}S$, $a: \mathcal{P}A \rightarrow A$
- $f(s) = a(\{f(s') \mid s' \in c(s)\})$ を満たす不動点 $f: S \rightarrow A$
- c がwell-foundedなら f は唯一

c のグラフが整礎 iff c が再帰余代数 (iff c が整礎余代数) [Osirus, J. Pure Appl. Alg.'74], [Taylor'95-96, '99], [AdamekMM, FoSSaCS'20]

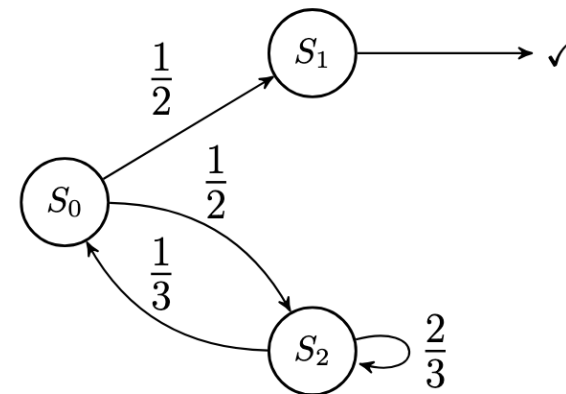
c が再帰余代数
iff 任意の a に $f: c \rightarrow a$ が唯一

$$\begin{array}{ccc} S & \xrightarrow{\quad f \quad} & A \\ c \downarrow & & \uparrow a \\ \mathcal{P}S & \xrightarrow{\quad \mathcal{P}f \quad} & \mathcal{P}A \end{array}$$

大域的性質による2つの不動点の一致

マルコフ連鎖の完全・部分期待報酬

- マルコフ連鎖



$$\text{rew}(S_i) = 1,$$

- 完全期待報酬：すべてのパスについての期待報酬($\mu\Psi$)

$$\Psi: [S, [0, \infty]] \rightarrow [S, [0, \infty]]$$

$$k \mapsto (s \mapsto \text{rew}(s) + \sum_{s'} P(s, s') \cdot k(s'))$$

- 部分期待報酬：✓に到達するパスについての期待報酬($\mu\Phi$)

$$\Phi: [S, [0, 1] \times [0, \infty]] \rightarrow [S, [0, 1] \times [0, \infty]]$$

$$k \mapsto (s \mapsto (p, r))$$

計算が複雑

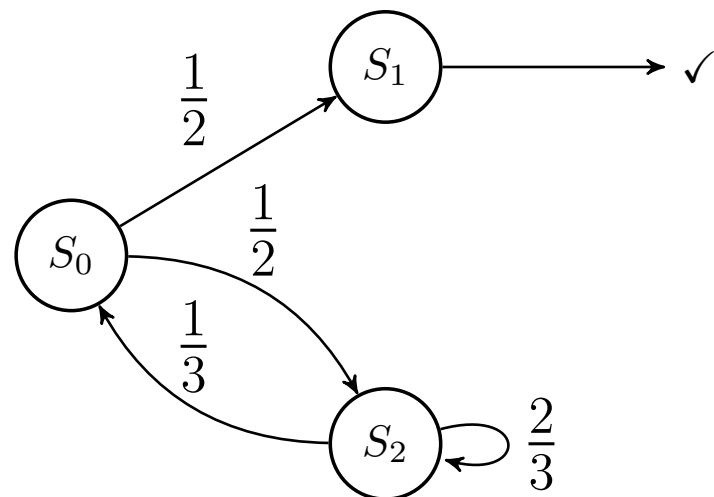
where $p := P(s, \checkmark) + \sum_{s' \in S} P(s, s') \cdot \pi_1 k(s')$

$$r := \text{rew}(s) \cdot P(s, \checkmark) + \sum_{s' \in S} P(s, s') \cdot (\pi_2 k(s') + \text{rew}(s) \cdot \pi_1 k(s'))$$

大域的性質による2つの不動点の一致

完全・部分期待報酬の一致

Prop. マルコフ連鎖がほぼ確実に到達可能($\forall s \in S. \Pr(s, \checkmark) = 1$)
のとき完全期待報酬 $\mu\Psi$ と部分期待報酬 $\mu\Phi$ は一致する



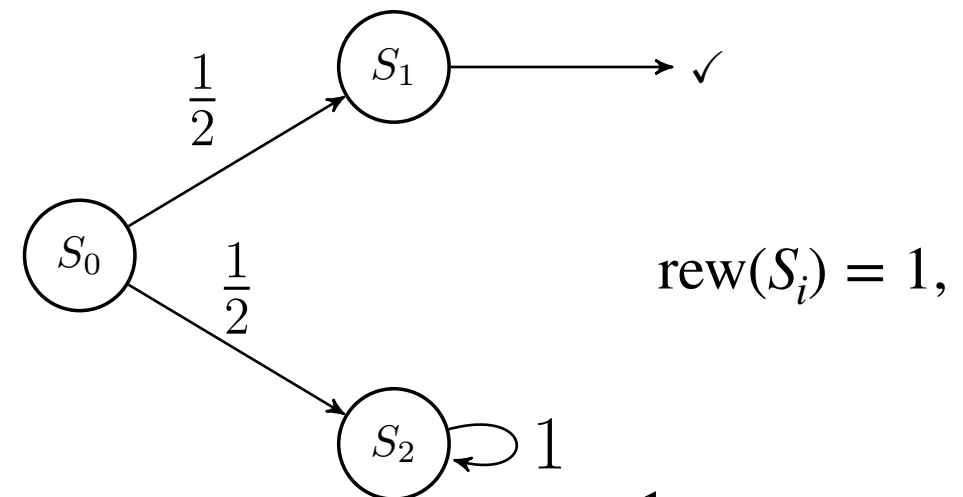
$$\mu\Psi(S_0) = 6, \mu\Phi(S_0) = (1, 6)$$

$$\mu\Psi(S_1) = 1, \mu\Phi(S_1) = (1, 1)$$

$$\mu\Psi(S_2) = 9, \mu\Phi(S_2) = (1, 9)$$

ほぼ確実に到達可能

$$(1, \mu\Psi) = \mu\Phi$$



$$\text{rew}(S_i) = 1,$$

$$\mu\Psi(S_0) = \infty, \mu\Phi(S_0) = (\frac{1}{2}, 1)$$

$$\mu\Psi(S_1) = 1, \mu\Phi(S_1) = (1, 1)$$

$$\mu\Psi(S_2) = \infty, \mu\Phi(S_2) = (0, 0)$$

ほぼ確実に到達可能でない

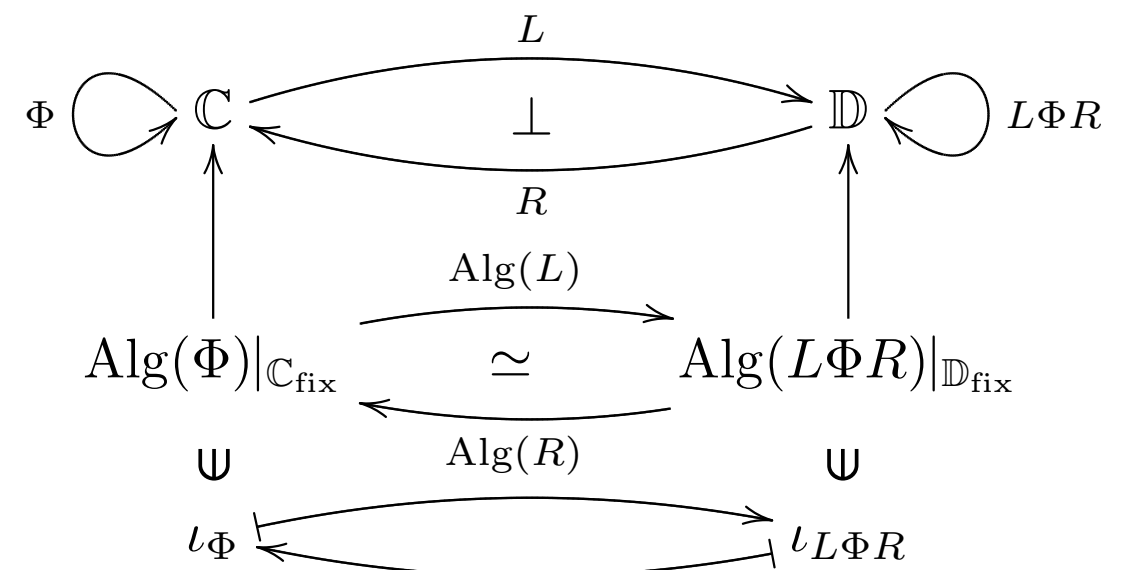
$$(1, \mu\Psi) \neq \mu\Phi$$

大域的性質による2つの不動点の一致

到達可能性条件下での始代数の対応

大域的な条件下での2つの不動点意味論の対応を抽象化[KoriWJ, LICS'25]

- 2つの不動点意味論 $\rightarrow$ 始代数 $\iota_\Phi, \iota_{L\Phi R}$
- 大域的な条件
 $\rightarrow$ 不動点がどこにいるか
($\iota_\Phi \in \text{Alg}(\Phi)|_{\mathbb{C}_{\text{fix}}}$ 不動点の唯一性と等価)



例：マルコフ連鎖・マルコフ決定過程の部分・完全期待報酬の一致、NFAのunambiguityのもとでの意味論の一致

- マルコフ決定過程では一般に知られている条件より弱い条件が得られる