物理情報システムの検証手法

制御と形式手法の相互理解，そして協働へ

蓮尾 一郎

国立情報学研究所 (NII)，総合研究大学院大学

JST ERATO 蓮尾メタ数理システムデザインプロジェクト

物理情報システムの検証手法

制御と形式手法の相互理解，そして協働へ

蓮尾 一郎

国立情報学研究所 (NII)，総合研究大学院大学

JST ERATO 蓮尾メタ数理システムデザインプロジェクト

- 専門： 理論計算機科学，論理学，
  計算機科学における代数的・圏論的構造，
  最近は制御理論も

Outline

* 制御理論 vs 形式手法・ソフトウェア科学
* 数学的相似・相互乗り入れ
  * 例1（相似）：確率的プログラムのマルチンゲールによる解析
    [Chakarov & Sankaranarayanan, CAV'13] [Takisaka, Oyabu, Urabe & Hasuo, ATVA'18]
  * 例2（乗り入れ）：近似双模倣による離散化
    [Girard & Pappas, IEEE TAC '07] [Kido, Sedwards & Hasuo, IFAC ADHS '18]
* 実システム応用に向けて
  * 機械学習・AIとの協働
  * ソフトウェア工学，現実的解決
* ERATO MMSD プロジェクトの取り組み

物理情報システム：制御理論と形式手法・ソフトウェア科学の協働

* 物理情報システム Cyber-Physical System (CPS)
  * “A mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users” (Wikipedia)
* 関連： embedded system, networked system, sensor network, robotics, systems of systems, Industrie 4.0, smart city, hybrid systems
* 連続的物理プラント + 離散的デジタル制御
* 米国： NSF Key Area of Research (2006-)

制御理論 vs 形式手法・ソフトウェア科学

制御理論		形式手法 ソフトウェア科学
連続空間・連続時間 （離散の場合も）	対象となる システム	離散空間・離散時間 （高々可算無限）
微分方程式	モデリング 形式	オートマトン（グラフ） プログラム
連続量最適化 LMI, SDP, mixed integer, …	最終的な 解き方	グラフアルゴリズム SATソルバ，SMTソルバ
機械，電気	主な 応用対象	ソフトウェア

・・・ 共通性？

* 対比の項目は同じ

制御理論 vs 形式手法・ソフトウェア科学

制御理論		形式手法 ソフトウェア科学
連続空間・連続時間 （離散の場合も）	対象となる システム	離散空間・離散時間 （高々可算無限）
微分方程式	モデリング 形式	オートマトン（グラフ） プログラム
連続量最適化 LMI, SDP, mixed integer, …	最終的な 解き方	グラフアルゴリズム SATソルバ，SMTソルバ
機械，電気	主な 応用対象	ソフトウェア

・・・ 共通性？

* 対比の項目は同じ

制御理論 vs 形式手法・ソフトウェア科学

制御理論		形式手法 ソフトウェア科学
連続空間・連続時間 （離散の場合も）	対象となる システム	離散空間・離散時間 （高々可算無限）
微分方程式	モデリング 形式	オートマトン（グラフ） プログラム
連続量最適化 LMI, SDP, mixed integer, …	最終的な 解き方	グラフアルゴリズム SATソルバ，SMTソルバ
機械，電気	主な 応用対象	ソフトウェア

*

ソフトウェア
検証問題

翻訳
- spec ↦ automaton
- model ↦ prop. formula
- …

制約充足問題
- SAT
- graph reachability
- …

制御問題

翻訳

最適化問題
- LMI
- SDP
- mixed integer
- stochastic optimization
- …

Outline

* 制御理論 vs 形式手法・ソフトウェア科学
* 数学的相似・相互乗り入れ
  * 例1（相似）：確率的プログラムのマルチンゲールによる解析
    [Chakarov & Sankaranarayanan, CAV'13] [Takisaka, Oyabu, Urabe & Hasuo, ATVA'18]
  * 例2（乗り入れ）：近似双模倣による離散化
    [Girard & Pappas, IEEE TAC '07] [Kido, Sedwards & Hasuo, IFAC ADHS '18]
* 実システム応用に向けて
  * 機械学習・AIとの協働
  * ソフトウェア工学，現実的解決
* ERATO MMSD プロジェクトの取り組み

Probabilistic Programs

* Programs with
  * random assignment

$$x := \mathbf{Gaussian}(0, 0.2)$$

  * probabilistic branching

$$\mathbf{if}\ \mathbf{prob}(0.2)$$

```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od
```

(say, $m = 16$ and $p = 0.2$)

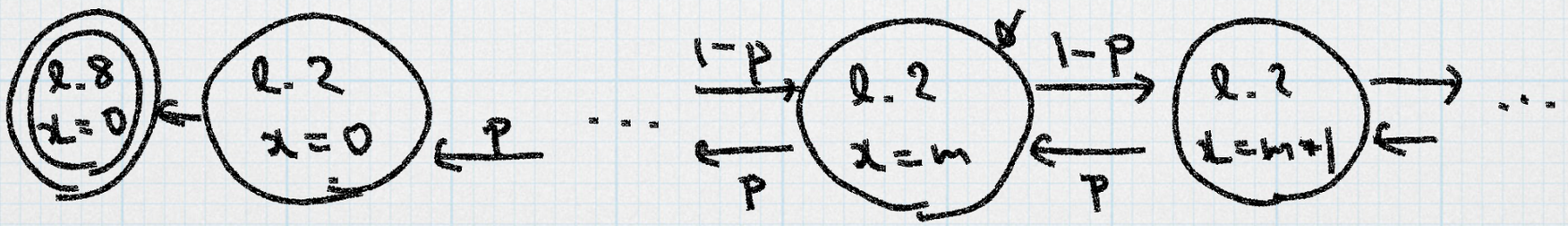
* Example: right (random walk)
* Disclaimer: we disregard the Bayesian aspects
  * observations, conditioning, priors/posteriors, etc.
  * See e.g. [Gordon+, FOSE'14]. Languages: Church, Anglican, Venture, …

Reachability Probabilities in PP

```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od
```

(say, $m = 16$ and $p = 0.2$)

* **Question** What is $\mathbf{Pr}(\text{the program terminates})$?
* How do we define it?
  * Configuration graph
    * A state is a pair (program location, memory state)
    * Transition by small-step operational semantics
    * ➜ MD (Markov chain) $\boldsymbol{M}$



* $$\mathbf{Pr}(\textbf{Termination}) \;=\; \mathbf{Pr}(M \text{ reaches } \circledcirc)$$

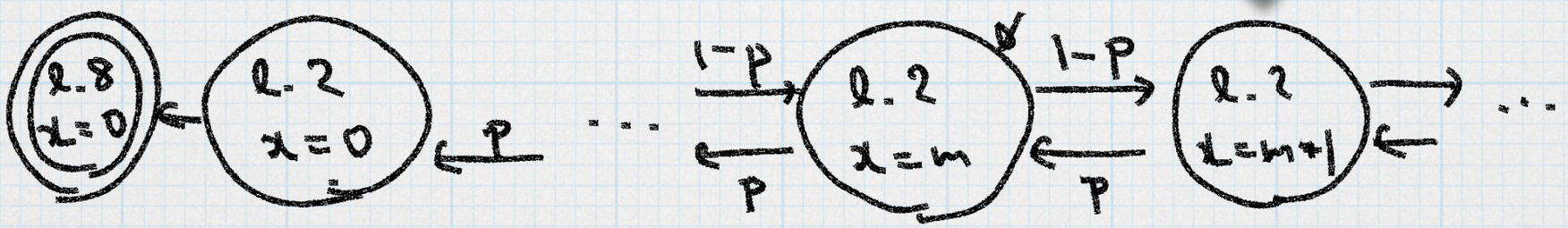
Reachability Probabilities in PP

* **Question** What is
  $\mathbf{Pr}(\text{the program terminates})$?

* How do we define it?
  * Configuration graph
  * A state is a pair (program l
  * Transition by small-step op
  * ➜ MD (Markov chain)

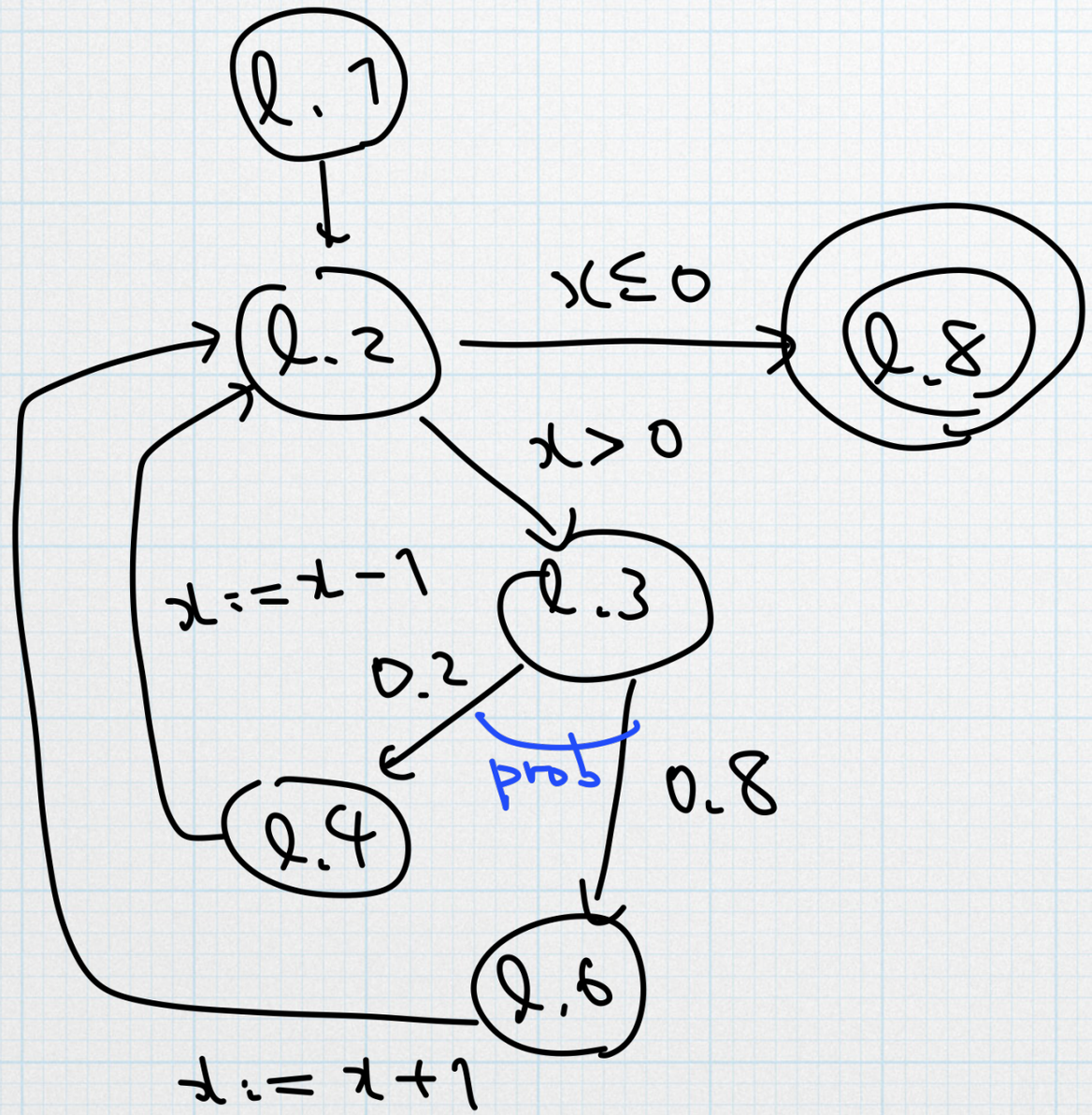
```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od

(say, m = 16 and p = 0.2)
```

real- and int- valued variables
➜ infinite states
➜ no “direct” automated analysis



* $$\mathbf{Pr}(\textbf{Termination}) \;=\; \mathbf{Pr}(M \text{ reaches } \circledcirc)$$

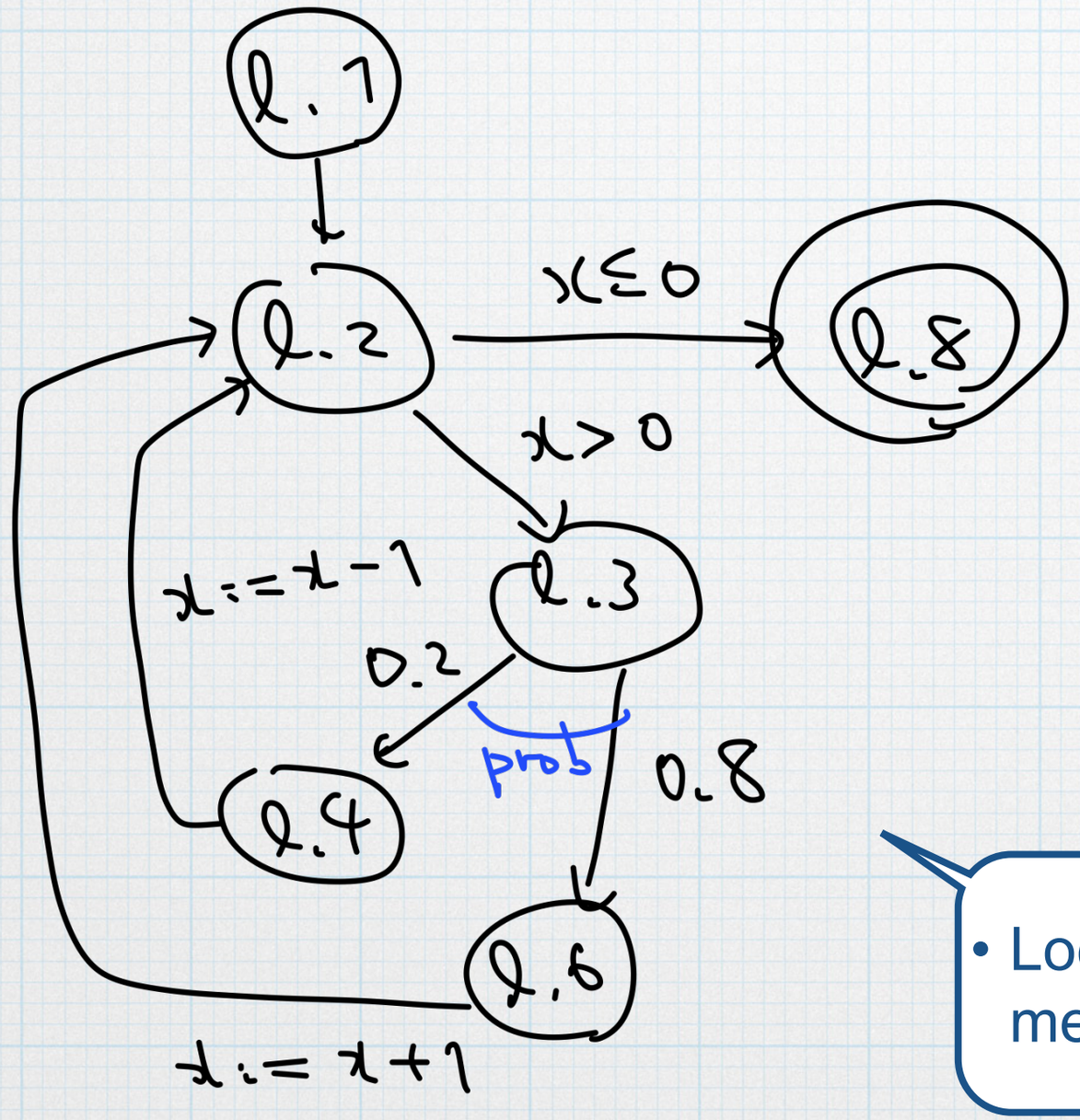
Probabilistic Control Flow Graph (pCFG) See e.g. [Chatterjee+, POPL'17]




```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od
```

(say, $m = 16$ and $p = 0.2$)

Probabilistic Control Flow Graph (pCFG) See e.g. [Chatterjee+, POPL'17]




```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od
```

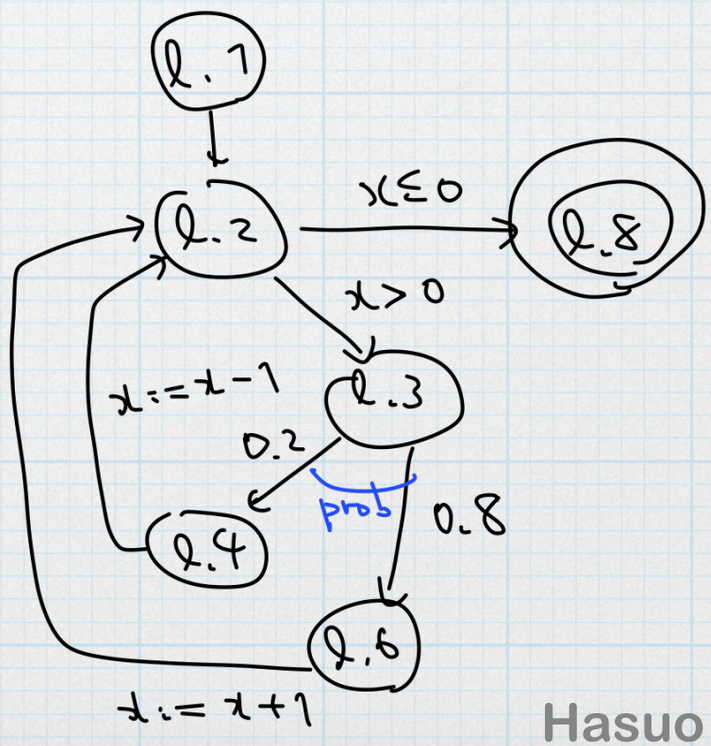
(say, $m = 16$ and $p = 0.2$)

- Locations + memory states (e.g. "x = 13")

Our Problem

* **Given**
  * a pCFG. n variables, state set L
  * $C \subseteq L \times \mathbb{R}^n$ (Lebesgue measurable) target region
  * $l_0 \in L,\ \vec{x}_0 \in \mathbb{R}^n$ initial configuration
* **Answer**

$\mathbf{Pr}(\mathrm{Reach}_C)$



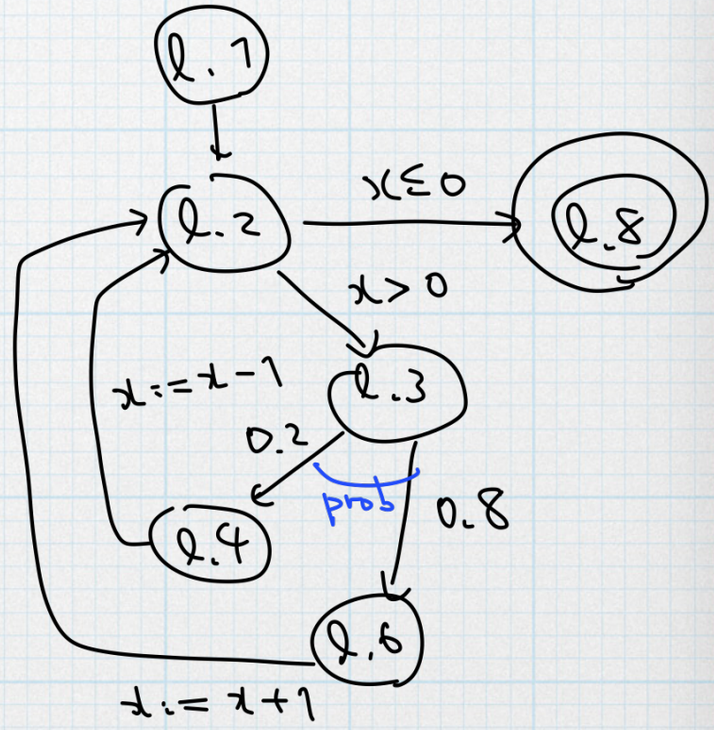
The Martingale-Based Approach

* Use **parametric certificates**, i.e. functions

$$\left(f_l : \mathbb{R}^n \to \mathbb{R} \right)_{l \in L}$$

to give *approximate* answers. Template-based synthesis

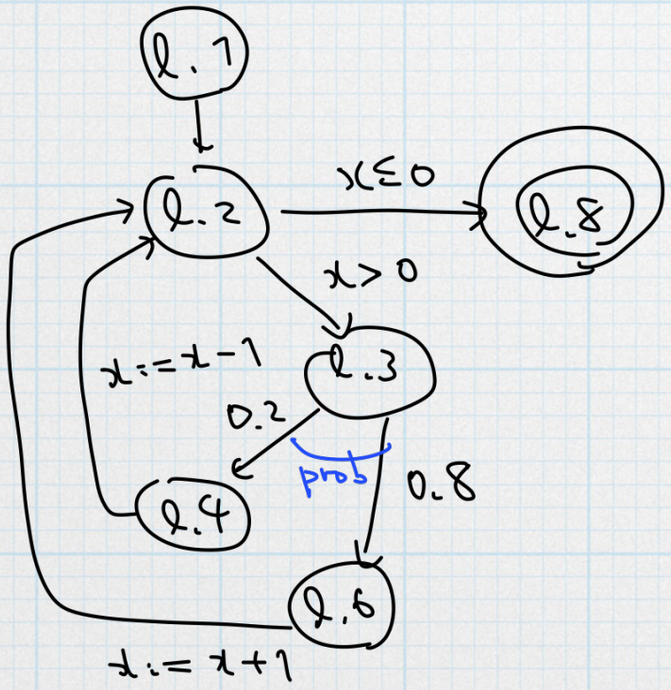
* Qualitative questions
  * $\mathbf{Pr}(\mathrm{Reach}_C) =^{?} 1$ (almost sure reachability)
  * $\mathbf{Pr}(\mathrm{Reach}_C) >=^{?} \alpha$ (threshold reachability)
* Quantitative questions
  * $\mathbf{Pr}(\mathrm{Reach}_C)$ >= ?? (lowerbound, “verification”)
  * $\mathbf{Pr}(\mathrm{Reach}_C)$ <= ?? (upperbound, “refutation”)
  * $\mathbf{Exp}(\mathrm{StepsToReach}_C)$, upperbound, lowerbound, …
  * “Concentration” [Chaterjee+, POPL’16]
    Find B s.t. $(x > B \rightarrow \mathbf{Pr}(\mathrm{StepsToReach}_C > x) < \alpha e^{-bx})$

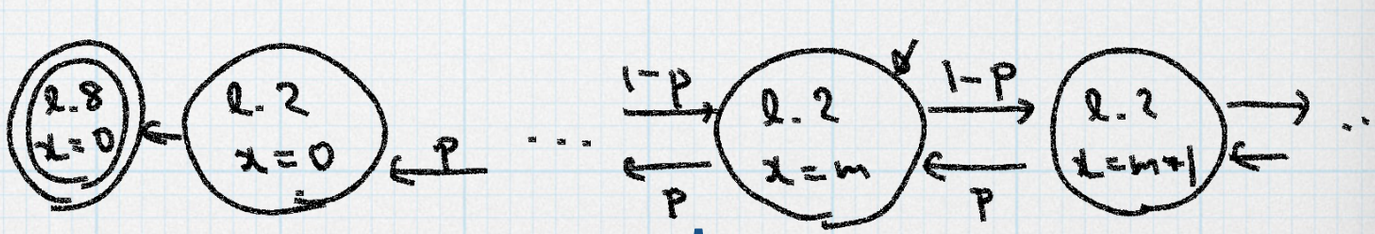


Disclaimer

* For the coming definitions, the setting is:

$$\text{A Markov chain } (S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S), \text{ and } C \subseteq S$$





- a **pCFG**:
  finite locations + memory states

- a **MC**:
  all the information as explicit states
  ➜ infinite states

Additive Ranking Supermartingale

[McIver+ PSSE'04] [Chakarov+ CAV'13]

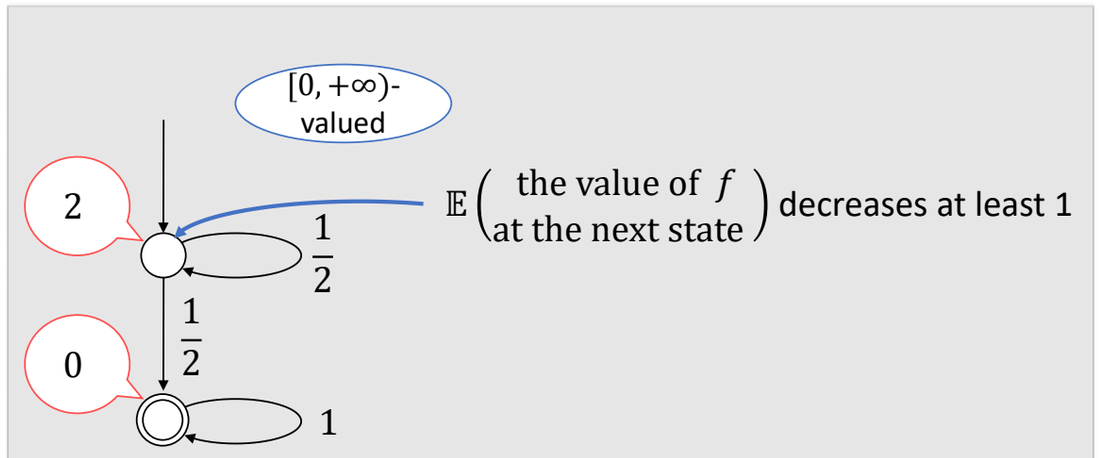
Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC,
$\eta\colon S \to \mathbb{R}$ be a function.

$\mathbb{X}\eta\colon S \to \mathbb{R}$ is defined by

$$
\begin{aligned}
(\mathbb{X}\eta)(s) &= \sum_{s'} \mathbf{tr}(s)(s') \cdot \eta(s') \\
&= \sum_{s'} \mathbf{Pr}(s \to s') \cdot \eta(s') \\
&= \mathbf{Exp}(\eta(s') \mid s \to s').
\end{aligned}
$$

* Overapprox.
  $\mathbf{Exp}(\text{Steps to } C)$



Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$.

$\eta\colon S \to \mathbb{R}_{\geq 0}$ is a *ranking supermartingale* for C if

- $\forall s \in S \setminus C. \quad \eta(s) \geq (\mathbb{X}\eta)(s) + 1.$
- $\eta(s) = 0$ implies $s \in C$

Additive Ranking Supermartingale

[McIver+ PSSE'04] [Chakarov+ CAV'13]

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC,
$\eta\colon S \to \mathbb{R}$ be a function.

$\mathbb{X}\eta\colon S \to \mathbb{R}$ is defined by

$$(\mathbb{X}\eta)(s) = \sum_{s'} \mathbf{tr}(s)$$
$$= \sum_{s'} \mathbf{Pr}(s$$
$$= \mathbf{Exp}(\eta(s$$

* Overapprox.
  $\mathbf{Exp}(\text{Steps to } C)$

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$.

$\eta\colon S \to \mathbb{R}_{\geq 0}$ is a *ranking supermartingale* for C if

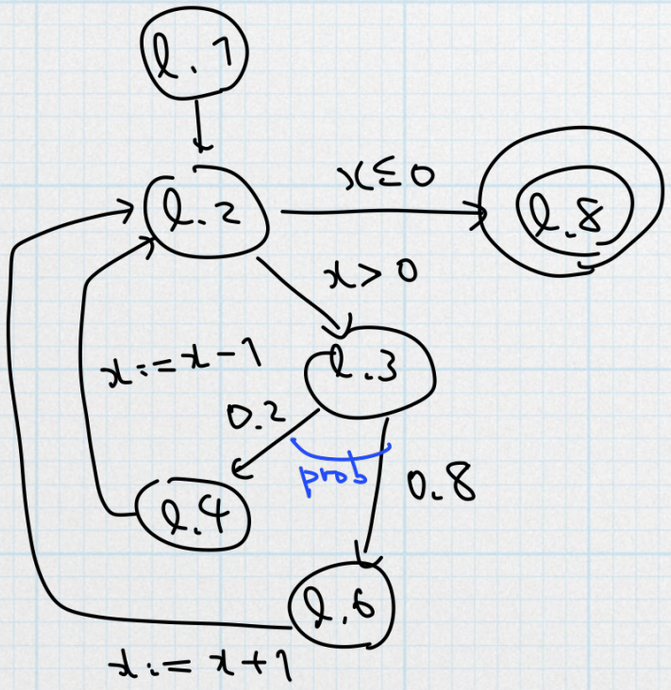
- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s) + 1.$
- $\eta(s) = 0$ implies $s \in C$

Thm.

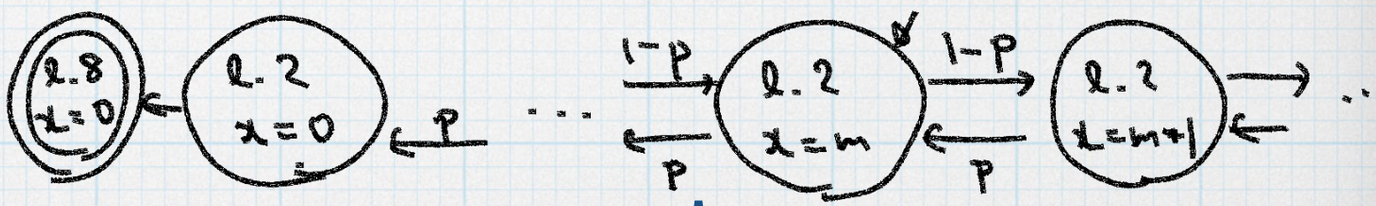
Let η be a ranking supermartingale for C. Then:

- $\mathbf{Pr}(\mathbf{Reach}_C) = 1$ (almost sure reachability)
- $\mathbf{Exp}(\text{Steps from } s \text{ to } C) \leq \eta(s)$

Towards Automated Reachability Analysis



- a **pCFG**:
  finite locations + memory states



- a **MC**:
  all the information as explicit states
  ➜ infinite states

The Martingale-Based Approach

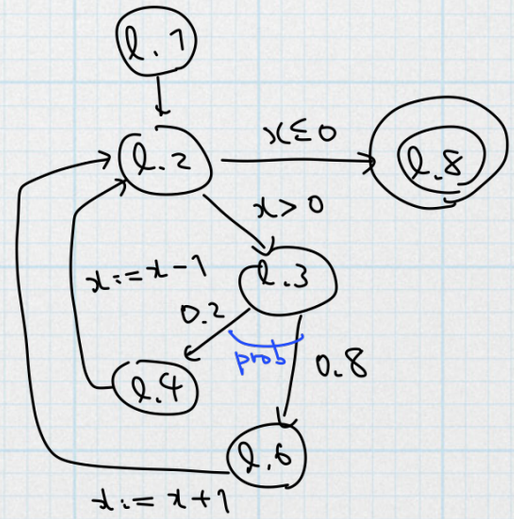
* Use **parametric certificates**, i.e. functions

$$\left(f_l : \mathbb{R}^n \to \mathbb{R} \right)_{l \in L}$$

to give *approximate* answers.

Def.
Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$.
$\eta : S \to \mathbb{R}_{\geq 0}$ is a *ranking supermartingale* for C if

- $\forall s \in S \setminus C. \quad \eta(s) \geq (\mathbb{X}\eta)(s) + 1.$
- $\eta(s) = 0$ implies $s \in C$



The Martingale-Based Approach

- Use **parametric certificates**, i.e. functions

$$\left(f_l : \mathbb{R}^n \to \mathbb{R} \right)_{l \in L}$$

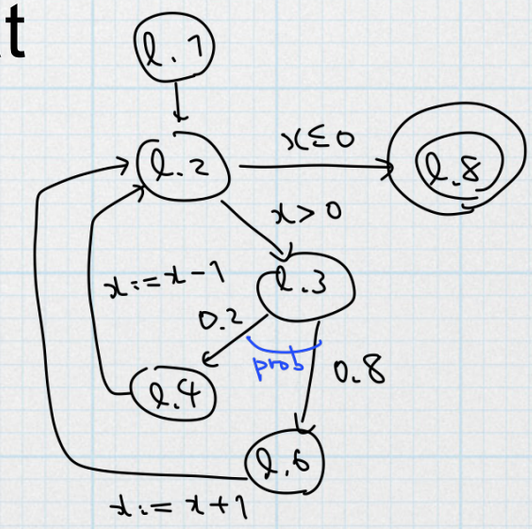
to give *approximate* answers.

- Template-based synthesis
  - Fix a **template**, e.g. "each f_l is a linear function" (Coefficients are parameters)
  - Generate **constraints** for the parameters, so that

$$\left(f_l : \mathbb{R}^n \to \mathbb{R} \right)_{l \in L}$$

is a supermartingale
  - Solve the constraints, by
    - LP (linear template, Farkas' Lemma),
    - SDP (polynomial template, Positivstellensatz), …

Def.
Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$.
$\eta : S \to \mathbb{R}_{\geq 0}$ is a *ranking supermartingale* for C if
- $\forall s \in S \setminus C. \quad \eta(s) \geq (\mathbb{X}\eta)(s) + 1.$
- $\eta(s) = 0$ implies $s \in C$



… 共通性？

* 対比の項目は同じ

制御理論 vs 形式手法・ソフトウェア科学

制御理論		形式手法 ソフトウェア科学
連続空間・連続時間 （離散の場合も）	対象となる システム	離散空間・離散時間 （高々可算無限）
微分方程式	モデリング 形式	オートマトン（グラフ） プログラム
連続量最適化 LMI, SDP, mixed integer, …	最終的な 解き方	グラフアルゴリズム SATソルバ，SMTソルバ
機械，電気	主な 応用対象	ソフトウェア

*

ソフトウェア
検証問題

翻訳
- spec ↦ automaton
- model ↦ prop. formula
- …

制約充足問題
- SAT
- graph reachability
- …

制御問題

翻訳

最適化問題
- LMI
- SDP
- mixed integer
- stochastic optimization
- …

ERATO 蓮尾メタ
ERATO Metamathem
国立情報学研究所 & 科学技術振興機構

・・・ 共通性？

* 対比の項目は同じ

• martingales for prob. programs

*

ソフトウェア
検証問題

• Lyapunov functions

制御問題

翻訳
- spec ↦ automaton
- model ↦ prop. formula
- …

翻訳

制約充足問題
- SAT
- graph reachability
- …

最適化問題
- LMI
- SDP
- mixed integer
- stochastic optimization
- …

制御理論 vs 形式手法・ソフトウェア科学

制御理論		形式手法 ソフトウェア科学
連続空間・連続時間 （離散の場合も）	対象となる システム	離散空間・離散時間 （高々可算無限）
微分方程式	モデリング 形式	オートマトン（グラフ） プログラム
連続量最適化 LMI, SDP, mixed integer, …	最終的な 解き方	グラフアルゴリズム SATソルバ，SMTソルバ
機械，電気	主な 応用対象	ソフトウェア

Outline

* 制御理論 vs 形式手法・ソフトウェア科学
* 数学的相似・相互乗り入れ
  * 例1（相似）：確率的プログラムのマルチンゲールによる解析
    [Chakarov & Sankaranarayanan, CAV'13] [Takisaka, Oyabu, Urabe & Hasuo, ATVA'18]
  * 例2（乗り入れ）：近似双模倣による離散化
    [Girard & Pappas, IEEE TAC '07] [Kido, Sedwards & Hasuo, IFAC ADHS '18]
* 実システム応用に向けて
  * 機械学習・AIとの協働
  * ソフトウェア工学，現実的解決
* ERATO MMSD プロジェクトの取り組み

Approximate Bisimulation

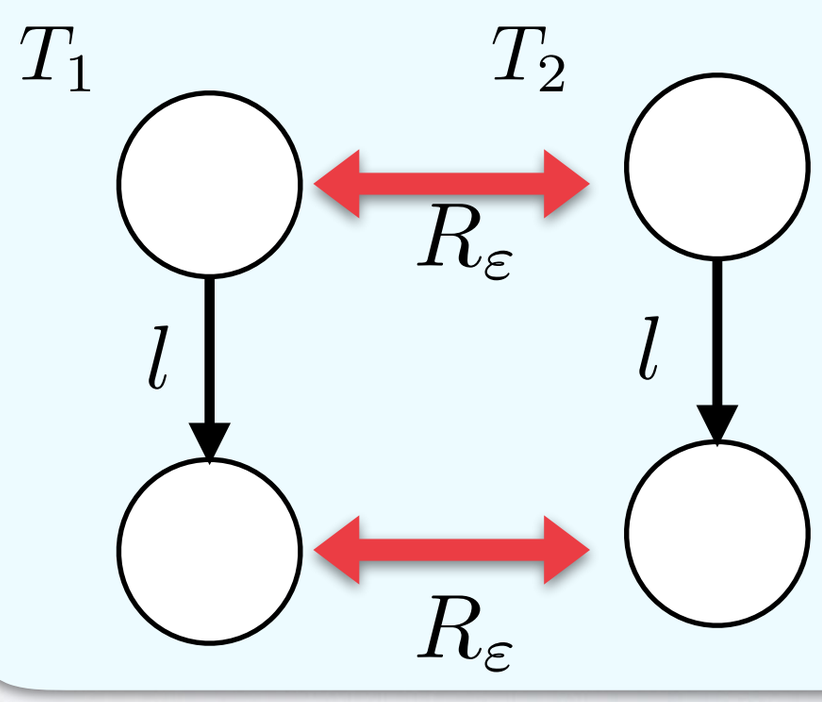
[Girard & Pappas, IEEE Transactions on Automatic Control'07]

$$T_i = (Q_i, L, \underset{i}{\longrightarrow}, O, H_i) \text{ for } i = 1, 2$$
$$(O \text{ equipped with a metric } d)$$

Def.

$R_\varepsilon \subseteq Q_1 \times Q_2$ is an **ε–approximate bisimulation** relation between T_1 and T_2 if for all $(q_1, q_2) \in R_\varepsilon$,

- $d(H_1(q_1), H_2(q_2)) \leq \epsilon$
- $\forall q_1 \xrightarrow[1]{l} q_1', \exists q_2 \xrightarrow[2]{l} q_2', \text{ s.t. } (q_1', q_2') \in R_\varepsilon$
- $\forall q_2 \xrightarrow[2]{l} q_2', \exists q_1 \xrightarrow[1]{l} q_1', \text{ s.t. } (q_1', q_2') \in R_\varepsilon$



Approximate Bisimulation

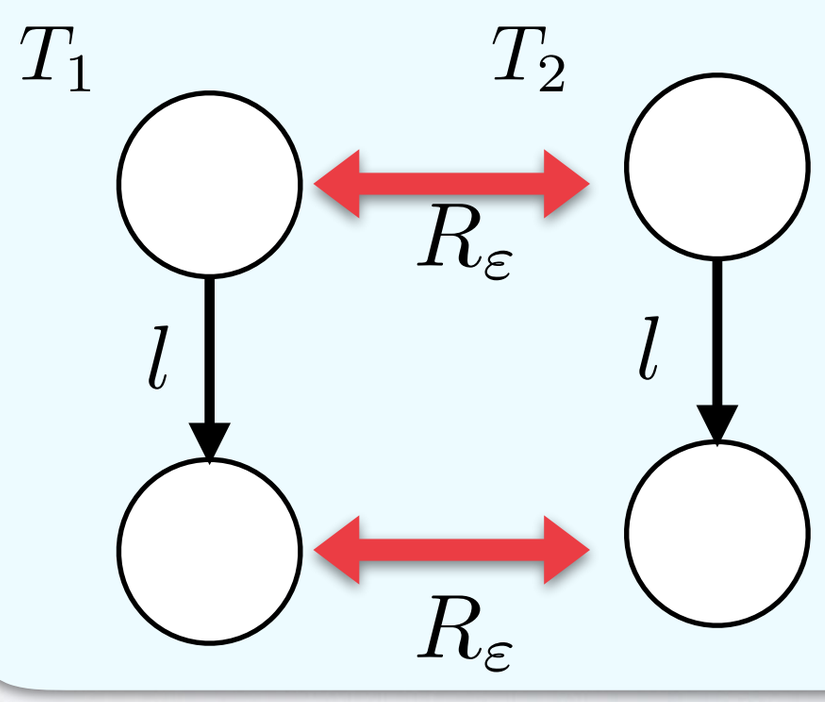
[Girard & Pappas, IEEE Transactions on Automatic Control'07]

$$T_i = (Q_i, L, \underset{i}{\longrightarrow}, O, H_i) \text{ for } i = 1, 2$$
$$(O \text{ equipped with a metric } d)$$

Def.

$R_\varepsilon \subseteq Q_1 \times Q_2$ is an **ε–approximate bisimulation** relation between T_1 and T_2 if for all $(q_1, q_2) \in R_\varepsilon$,

- $d(H_1(q_1), H_2(q_2)) \leq \epsilon$
- $\forall q_1 \xrightarrow[1]{l} q_1', \exists q_2 \xrightarrow[2]{l} q_2', \text{ s.t. } (q_1', q_2') \in R_\varepsilon$
- $\forall q_2 \xrightarrow[2]{l} q_2', \exists q_1 \xrightarrow[1]{l} q_1', \text{ s.t. } (q_1', q_2') \in R_\varepsilon$



Once in a relationship, always henceforth

Approximate Bisimulation

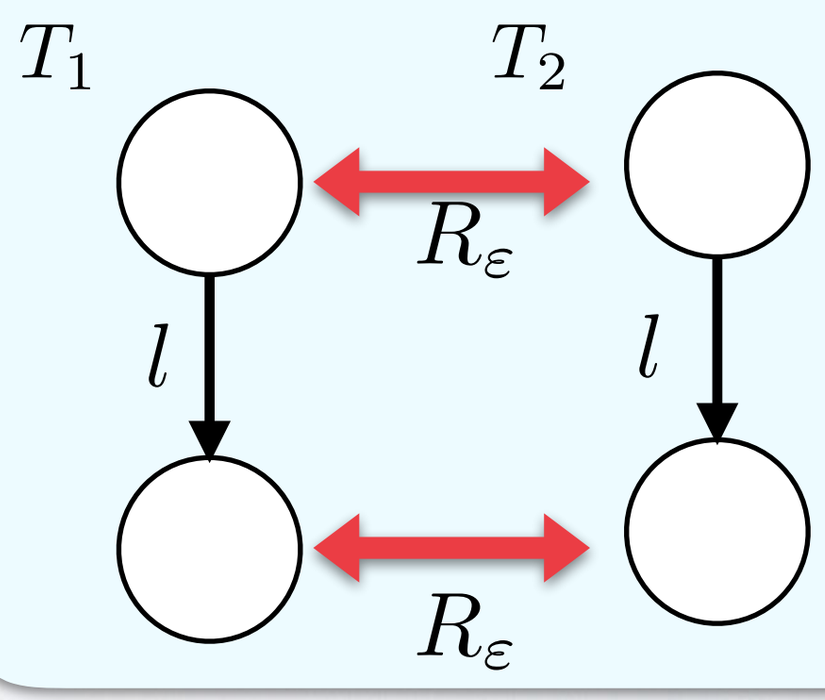
[Girard & Pappas, IEEE Transactions on Automatic Control'07]

$$T_i = (Q_i, L, \underset{i}{\longrightarrow}, O, H_i) \text{ for } i = 1, 2$$
$$(O \text{ equipped with a metric } d)$$

Def.

$R_\varepsilon \subseteq Q_1 \times Q_2$ is an ε–approximate bisimulation relation between T_1 and T_2 if for all $(q_1, q_2) \in R_\varepsilon$,

- $d(H_1(q_1), H_2(q_2)) \leq \epsilon$
- $\forall q_1 \xrightarrow[1]{l} q_1', \exists q_2 \xrightarrow[2]{l} q_2', \text{ s.t. } (q_1', q_2') \in R_\varepsilon$
- $\forall q_2 \xrightarrow[2]{l} q_2', \exists q_1 \xrightarrow[1]{l} q_1', \text{ s.t. } (q_1', q_2') \in R_\varepsilon$



Once in a relationship, always henceforth

Incremental Stability (δ-GUAS)

Incrementally **G**lobally **U**niformly **A**symptotically **S**table

Def. A dynamics is said to be δ-$\boldsymbol{GAS}$ if $\exists\ \mathcal{KL}$ function β s.t.

$$\left\| \mathbf{x}(x,t) - \mathbf{x}(y,t) \right\| \ \leq\ \beta\big(\|x-y\|, t \big)$$

where $\mathbf{x}(x,-)$ is the trajectory starting at x.

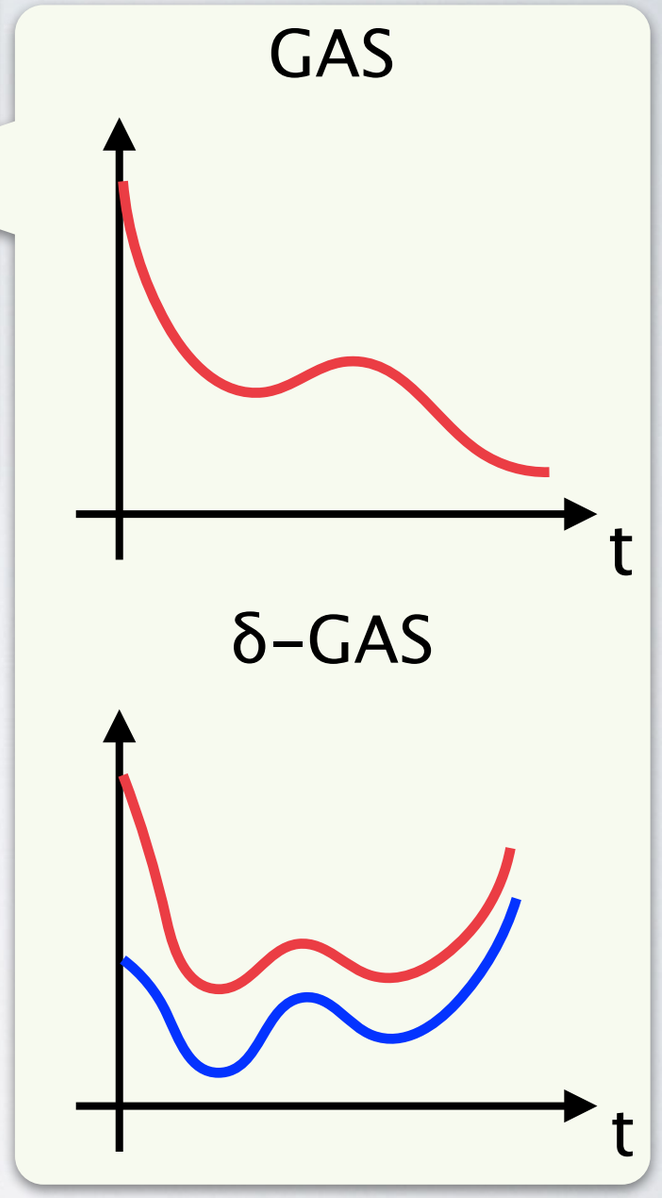
Incremental Stability (δ-GUAS)

Incrementally **G**lobally **U**niformly **A**symptotically **S**table

Def. A dynamics is said to be δ-$\boldsymbol{GAS}$ if $\exists\ \mathcal{KL}$ function β s.t.

$$\| \mathbf{x}(x,t) - \mathbf{x}(y,t) \| \ \leq\ \beta(\|x-y\|, t)$$

where $\mathbf{x}(x,-)$ is the trajectory starting at x.



- increasing in $\|x - y\|$
  - 0 if $\|x - y\| = 0$
  - $\to \infty$ if $\|x - y\| \to \infty$
- decreasing in t
  - $\to 0$ if $t \to \infty$

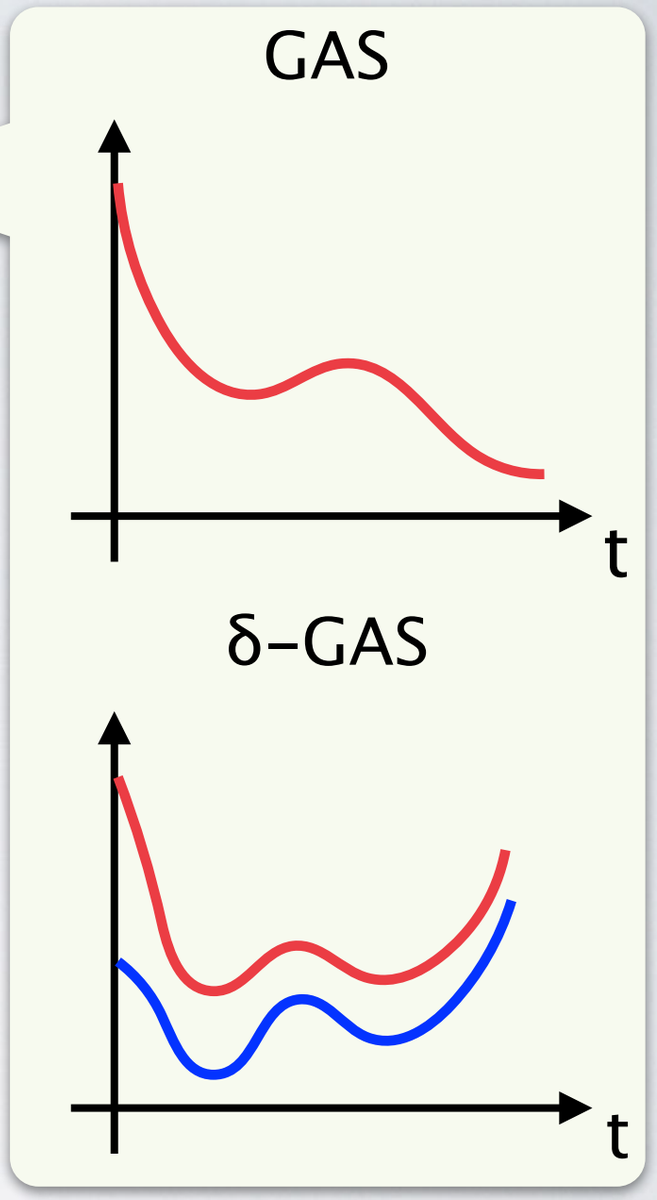
nental Stability (δ-GUAS)

nentally Globally Uniformly Asymptotically Stable

Def. A dynamics is said to be δ-$\boldsymbol{GAS}$ if $\exists\ \mathcal{KL}$ function β s.t.

$$\| \mathbf{x}(x,t) - \mathbf{x}(y,t) \| \ \leq\ \beta(\|x - y\|, t)$$

where $\mathbf{x}(x, -)$ is the trajectory starting at x.



- increasing in $\|x - y\|$
  - 0 if $\|x - y\| = 0$
  - $\to \infty$ if $\|x - y\| \to \infty$
- decreasing in t
  - $\to 0$ if $t \to \infty$

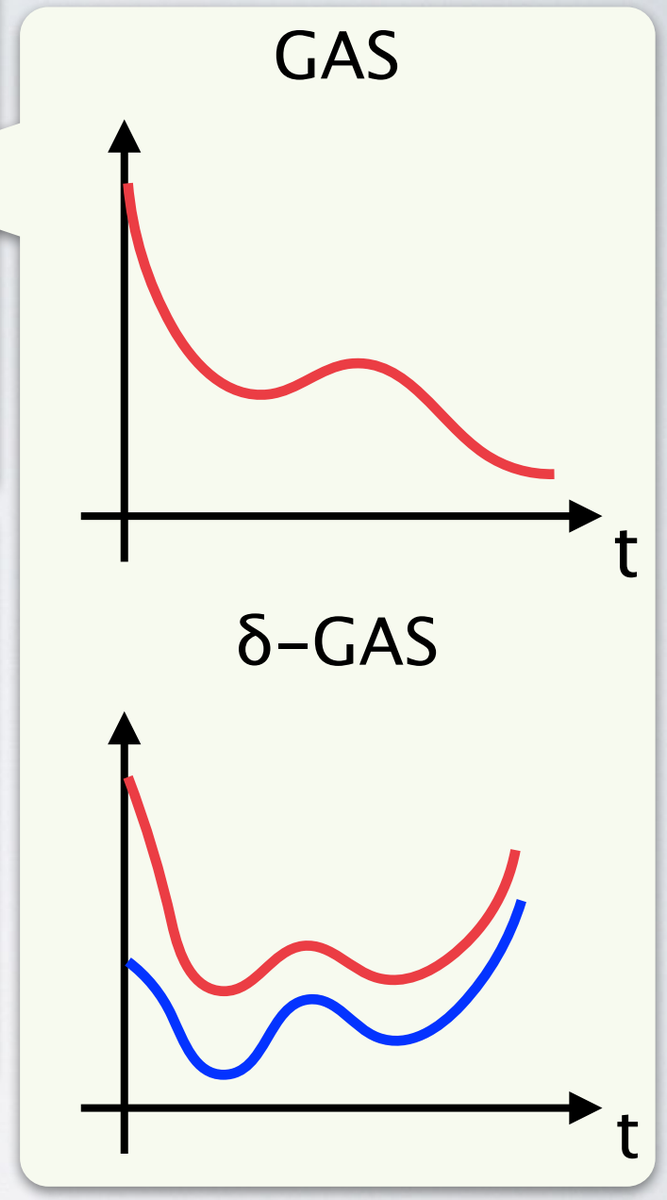
nental Stability (δ-GUAS)

nentally Globally Uniformly Asymptotically Stable

Def. A dynamics is said to be δ-$\boldsymbol{GAS}$ if $\exists\ \mathcal{KL}$ function β s.t.

$$\| \mathbf{x}(x,t) - \mathbf{x}(y,t) \| \ \leq\ \beta(\|x - y\|, t)$$

where $\mathbf{x}(x, -)$ is the trajectory starting at x.



Def. For a dynamics $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x})$ in $\mathbb{R}^{\boldsymbol{n}}$, a smooth function $\boldsymbol{V}: \mathbb{R}^{\boldsymbol{n}} \times \mathbb{R}^{\boldsymbol{n}} \to \mathbb{R}^{+}$ is a *common $\boldsymbol{\delta}$-GAS Lyapunov function* if there exist $\boldsymbol{\mathcal{K}_\infty}$ functions $\underline{\boldsymbol{\alpha}}$, $\overline{\boldsymbol{\alpha}}$ and $\boldsymbol{\kappa > 0}$ such that

$$\underline{\boldsymbol{\alpha}}(\|\boldsymbol{x} - \boldsymbol{y}\|) \ \leq\ \boldsymbol{V}(\boldsymbol{x}, \boldsymbol{y}) \ \leq\ \overline{\boldsymbol{\alpha}}(\|\boldsymbol{x} - \boldsymbol{y}\|)$$

$$\frac{\boldsymbol{\partial V}}{\boldsymbol{\partial x}}(\boldsymbol{x}, \boldsymbol{y})\boldsymbol{f}(\boldsymbol{x}) + \frac{\boldsymbol{\partial V}}{\boldsymbol{\partial y}}(\boldsymbol{x}, \boldsymbol{y})\boldsymbol{f}(\boldsymbol{y}) \ \leq\ -\boldsymbol{\kappa V}(\boldsymbol{x}, \boldsymbol{y})$$

- increasing in $\|x - y\|$
  - 0 if $\|x - y\| = 0$
  - $\to \infty$ if $\|x - y\| \to \infty$
- decreasing in t
  - $\to 0$ if $t \to \infty$

nental Stability (δ-GUAS)

nentally Globally Uniformly Asymptotically Stable

Def. A dynamics is said to be δ-$\boldsymbol{GAS}$ if $\exists\ \mathcal{KL}$ function β s.t.

$$\| \mathbf{x}(x,t) - \mathbf{x}(y,t) \| \ \leq\ \beta(\|x - y\|, t)$$

here $\mathbf{x}(x,-)$ is the trajectory starting at x.

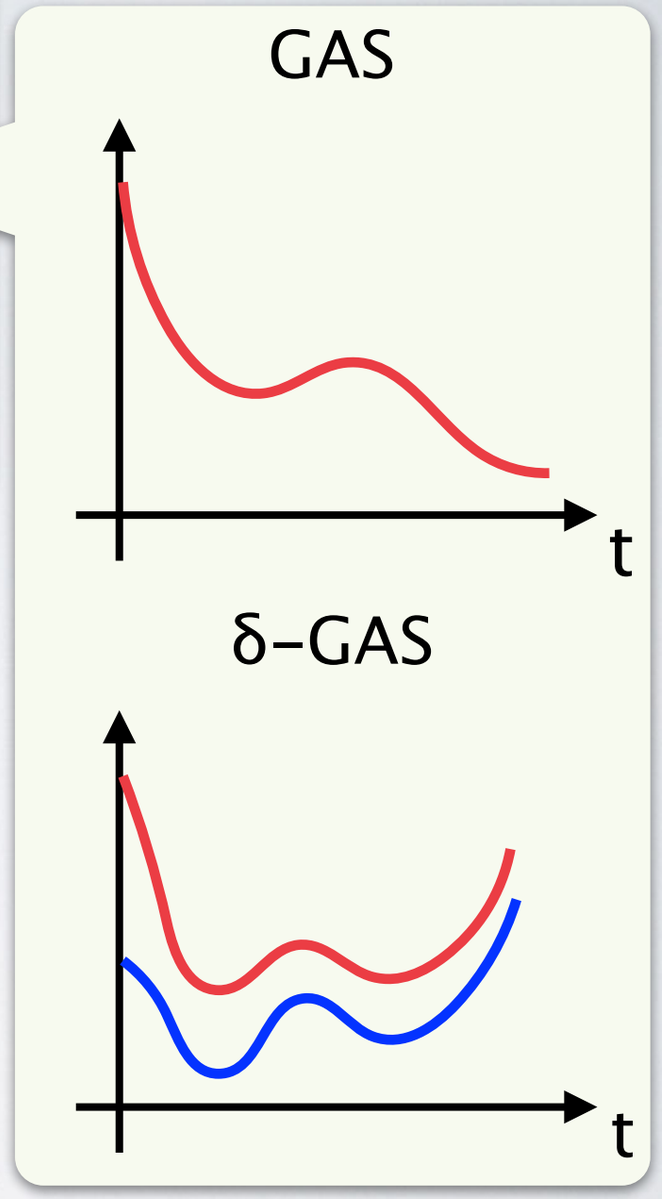
$V(x,y)$ is more or less $\| x - y \|$...

D For a dynamics $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x})$ in $\mathbb{R}^{\boldsymbol{n}}$, a smooth function $\boldsymbol{V}: \mathbb{R}^{\boldsymbol{n}} \times \mathbb{R}^{\boldsymbol{n}} \to \mathbb{R}^{+}$ is a *common* $\boldsymbol{\delta}$*-GAS Lyapunov function* if there exist $\mathcal{K}_{\infty}$ functions $\underline{\boldsymbol{\alpha}}$, $\overline{\boldsymbol{\alpha}}$ and $\boldsymbol{\kappa} > \mathbf{0}$ such that

$$\underline{\boldsymbol{\alpha}}(\|\boldsymbol{x} - \boldsymbol{y}\|) \ \leq\ \boldsymbol{V}(\boldsymbol{x},\boldsymbol{y}) \ \leq\ \overline{\boldsymbol{\alpha}}(\|\boldsymbol{x} - \boldsymbol{y}\|)$$

$$\frac{\boldsymbol{\partial V}}{\boldsymbol{\partial x}}(\boldsymbol{x},\boldsymbol{y})\boldsymbol{f}(\boldsymbol{x}) + \frac{\boldsymbol{\partial V}}{\boldsymbol{\partial y}}(\boldsymbol{x},\boldsymbol{y})\boldsymbol{f}(\boldsymbol{y}) \ \leq\ -\boldsymbol{\kappa V}(\boldsymbol{x},\boldsymbol{y})$$

that decreases along the dynamics



- increasing in $\|x - y\|$
  - 0 if $\|x - y\| = 0$
  - $\to \infty$ if $\|x - y\| \to \infty$
- decreasing in t
  - $\to 0$ if $t \to \infty$

nental Stability (δ-GUAS)

nentally Globally Uniformly Asymptotically Stable

Def. A dynamics is said to be δ-$\boldsymbol{GAS}$ if $\exists\ \mathcal{KL}$ function β s.t.

$$\| \mathbf{x}(x,t) - \mathbf{x}(y,t) \| \ \leq\ \beta(\|x - y\|, t)$$

here $\mathbf{x}(x,-)$ is the trajectory starting at x.

$V(x,y)$ is more or less $\| x - y \|$...

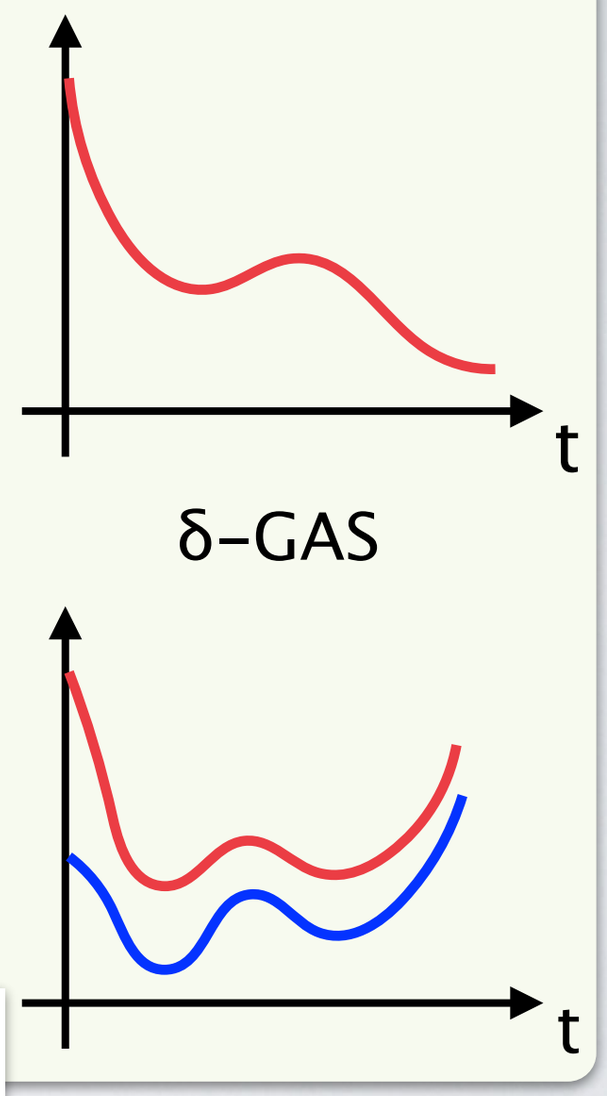
D For a dynamics $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x})$ in $\mathbb{R}^n$, a smooth function $\boldsymbol{V}: \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^+$ is a *common $\boldsymbol{\delta}$-GAS Lyapunov function* if there exist $\mathcal{K}_\infty$ functions $\underline{\boldsymbol{\alpha}}$, $\overline{\boldsymbol{\alpha}}$ and $\boldsymbol{\kappa} > \mathbf{0}$ such that

$$\underline{\boldsymbol{\alpha}}(\|\boldsymbol{x} - \boldsymbol{y}\|) \ \leq\ \boldsymbol{V}(\boldsymbol{x},\boldsymbol{y}) \ \leq\ \overline{\boldsymbol{\alpha}}(\|\boldsymbol{x} - \boldsymbol{y}\|)$$

$$\frac{\partial \boldsymbol{V}}{\partial \boldsymbol{x}}(\boldsymbol{x},\boldsymbol{y})\boldsymbol{f}(\boldsymbol{x}) + \frac{\partial \boldsymbol{V}}{\partial \boldsymbol{y}}(\boldsymbol{x},\boldsymbol{y})\boldsymbol{f}(\boldsymbol{y}) \ \leq\ -\boldsymbol{\kappa}\boldsymbol{V}(\boldsymbol{x},\boldsymbol{y})$$

that decreases along the dynamics

Thm. There is a $\boldsymbol{\delta}$-GAS Lyapunov function $\Longrightarrow$ incrementally stable ($\boldsymbol{\delta}$-GAS).



nental Stability (δ-GUAS)

nentally Globally Uniformly Asymptotically Stable

- increasing in $\|x-y\|$
  - 0 if $\|x-y\|=0$
  - $\to\infty$ if $\|x-y\|\to\infty$
- decreasing in t
  - $\to 0$ if $t\to\infty$

Def. A dynamics is said to be δ-$\boldsymbol{GAS}$ if $\exists\ \mathcal{KL}$ function β s.t.

$$\|\,\mathbf{x}(x,t)-\mathbf{x}(y,t)\,\| \;\le\; \beta(\,\|x-y\|,\,t\,)$$

here $\mathbf{x}(x,-)$ is the trajectory starting at x.

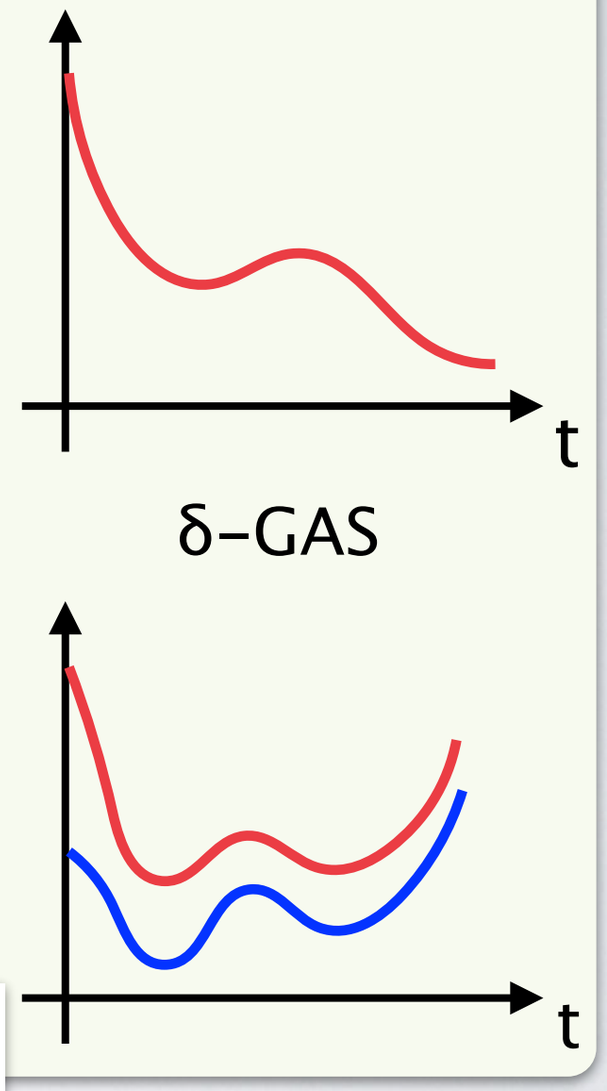
$\boldsymbol{V(x,y)}$ is more or less $\|\boldsymbol{x}-\boldsymbol{y}\|$...

D For a dynamics $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x})$ in $\mathbb{R}^{\boldsymbol{n}}$, a smooth function $\boldsymbol{V}: \mathbb{R}^{\boldsymbol{n}}\times\mathbb{R}^{\boldsymbol{n}}\to\mathbb{R}^{+}$ is a *common $\boldsymbol{\delta}$-GAS Lyapunov function* if there exist $\mathcal{K}_\infty$ functions $\underline{\boldsymbol{\alpha}}$, $\overline{\boldsymbol{\alpha}}$ and $\boldsymbol{\kappa}>\mathbf{0}$ such that

$$\underline{\boldsymbol{\alpha}}(\|\boldsymbol{x}-\boldsymbol{y}\|) \;\le\; \boldsymbol{V}(\boldsymbol{x},\boldsymbol{y}) \;\le\; \overline{\boldsymbol{\alpha}}(\|\boldsymbol{x}-\boldsymbol{y}\|)$$

$$\frac{\partial \boldsymbol{V}}{\partial \boldsymbol{x}}(\boldsymbol{x},\boldsymbol{y})\boldsymbol{f}(\boldsymbol{x}) + \frac{\partial \boldsymbol{V}}{\partial \boldsymbol{y}}(\boldsymbol{x},\boldsymbol{y})\boldsymbol{f}(\boldsymbol{y}) \;\le\; -\boldsymbol{\kappa}\boldsymbol{V}(\boldsymbol{x},\boldsymbol{y})$$

that decreases along the dynamics



Thm. There is a $\boldsymbol{\delta}$-GAS Lyapunov function $\Longrightarrow$ incrementally stable ($\boldsymbol{\delta}$-GAS).

Switched extension: δ-GUAS, common Lyapunov func.

[Girard, Pola, Tabuada, IEEE TAC '10]

Discrete Abstraction via Incremental Stability

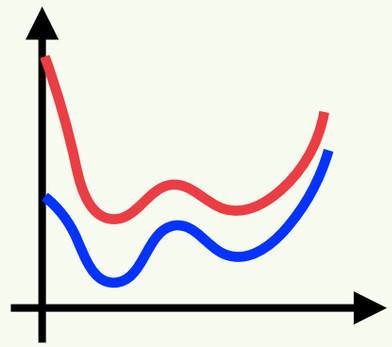
[Girard, Pola, Tabuada, IEEE TAC '10]

For a switched dynamics $\dot{x} = f_p(x)$ …

Common δ-GAS Lyapunov func. V

witnesses

Incremental stability (δ-GUAS)



Discrete Abstraction via Incremental Stability

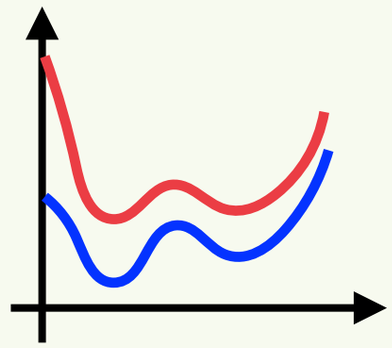
[Girard, Pola, Tabuada, IEEE TAC '10]

For a switched dynamics $\dot{x} = f_p(x)$ ...

Common δ-GAS Lyapunov func. V

witnesses

Incremental stability (δ-GUAS)



induces

Approximate bisimulation

Thm. Let V be a common δ-GAS Lyapunov func. lower-bounded by $\underline{\alpha}$. Then

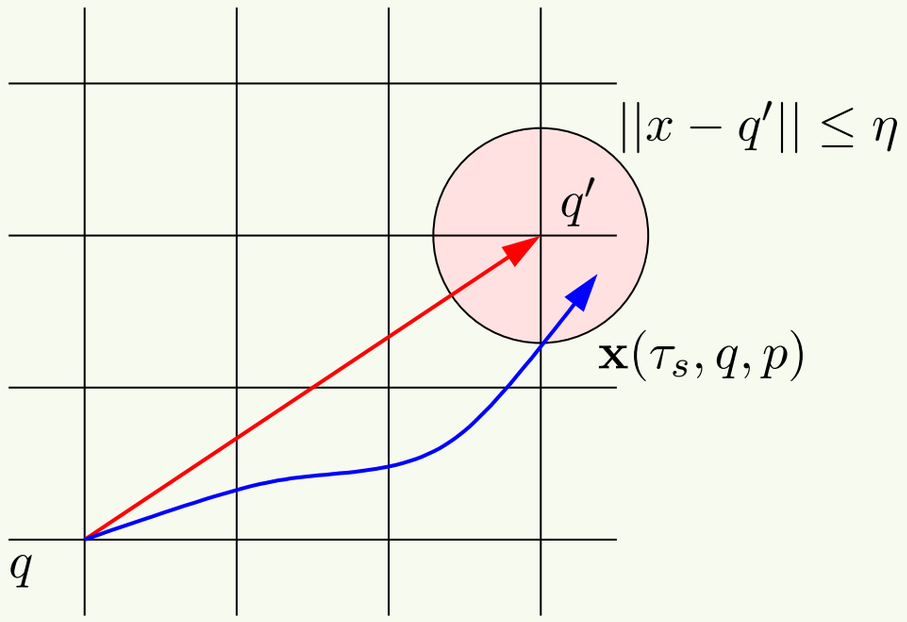
$$(x, y) \in R \quad \overset{\text{def}}{\Longleftrightarrow} \quad V(x, y) \leq \underline{\alpha}(\varepsilon)$$

yields an ε-approximate bisimulation.

correctness guarantee

Statespace abstraction

(Fig. from [GirardPT'10])



Discrete Abstraction via Incremental Stability

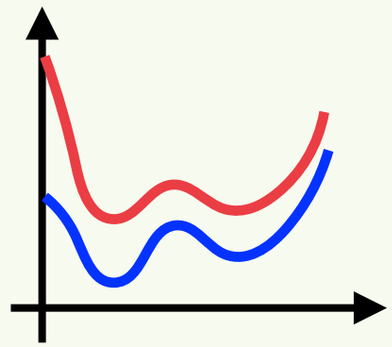
[Girard, Pola, Tabuada, IEEE TAC '10]

For a switched dynamics $\dot{x} = f_p(x)$ …

Common δ-GAS Lyapunov func. V

witnesses

Incremental stability (δ-GUAS)



Discrete verification, synthesis, supervisory control, …

induces

Approximate bisimulation

Thm. Let V be a common δ-GAS Lyapunov func. lower-bounded by $\underline{\alpha}$. Then

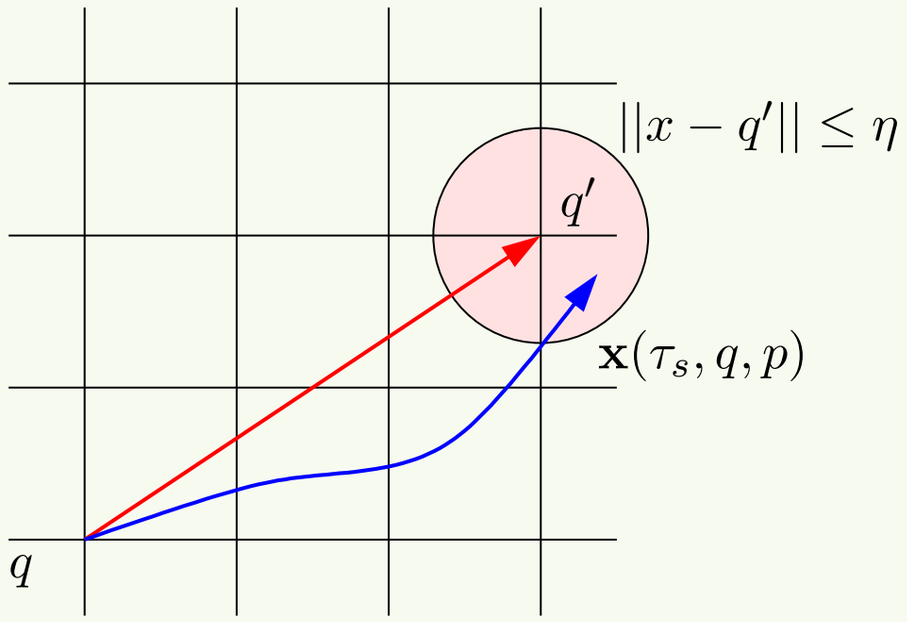
$$(x, y) \in R \quad \overset{\text{def}}{\Longleftrightarrow} \quad V(x, y) \leq \underline{\alpha}(\varepsilon)$$

yields an ε-approximate bisimulation.

correctness guarantee

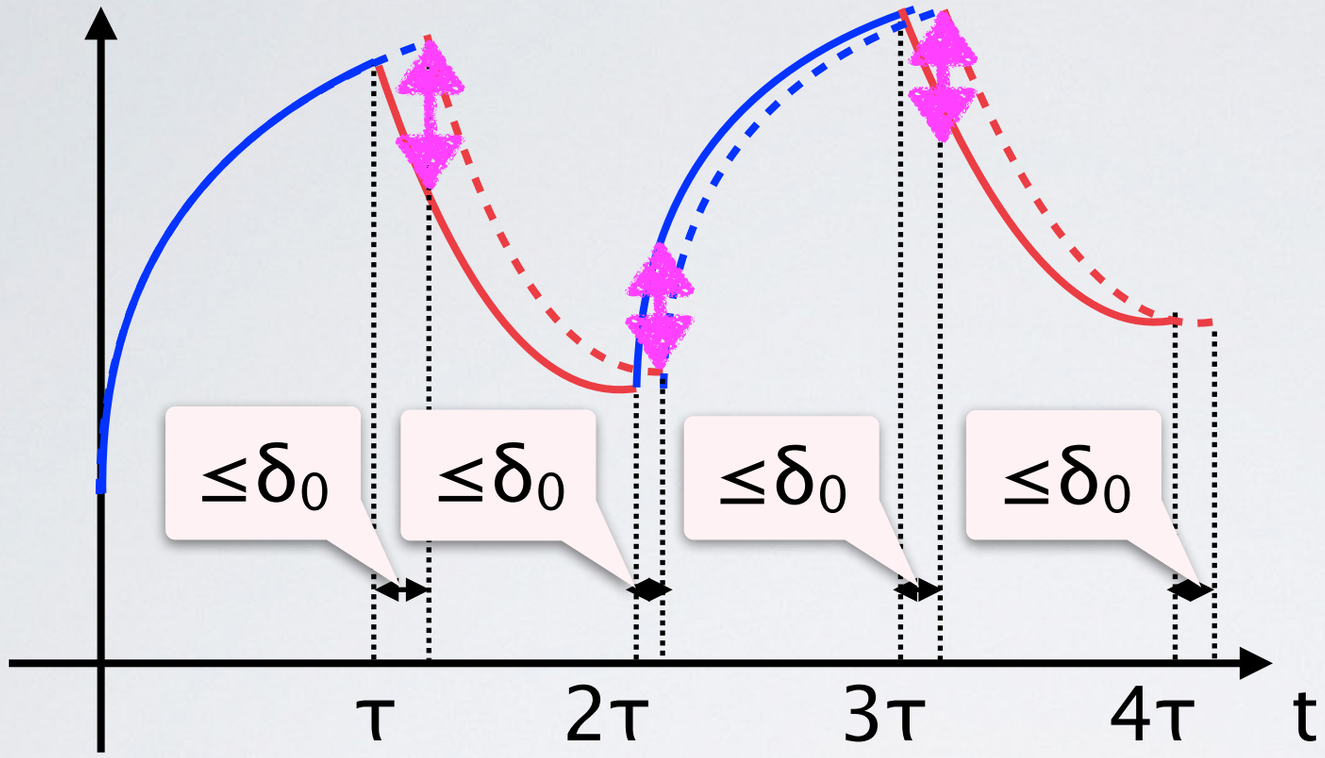
Statespace abstraction

(Fig. from [GirardPT'10])



Bounding Errors by Switching Delays

[Kido, Sedwards & Hasuo, IFAC ADHS '18]



$\dot{x} = f_1(x)$

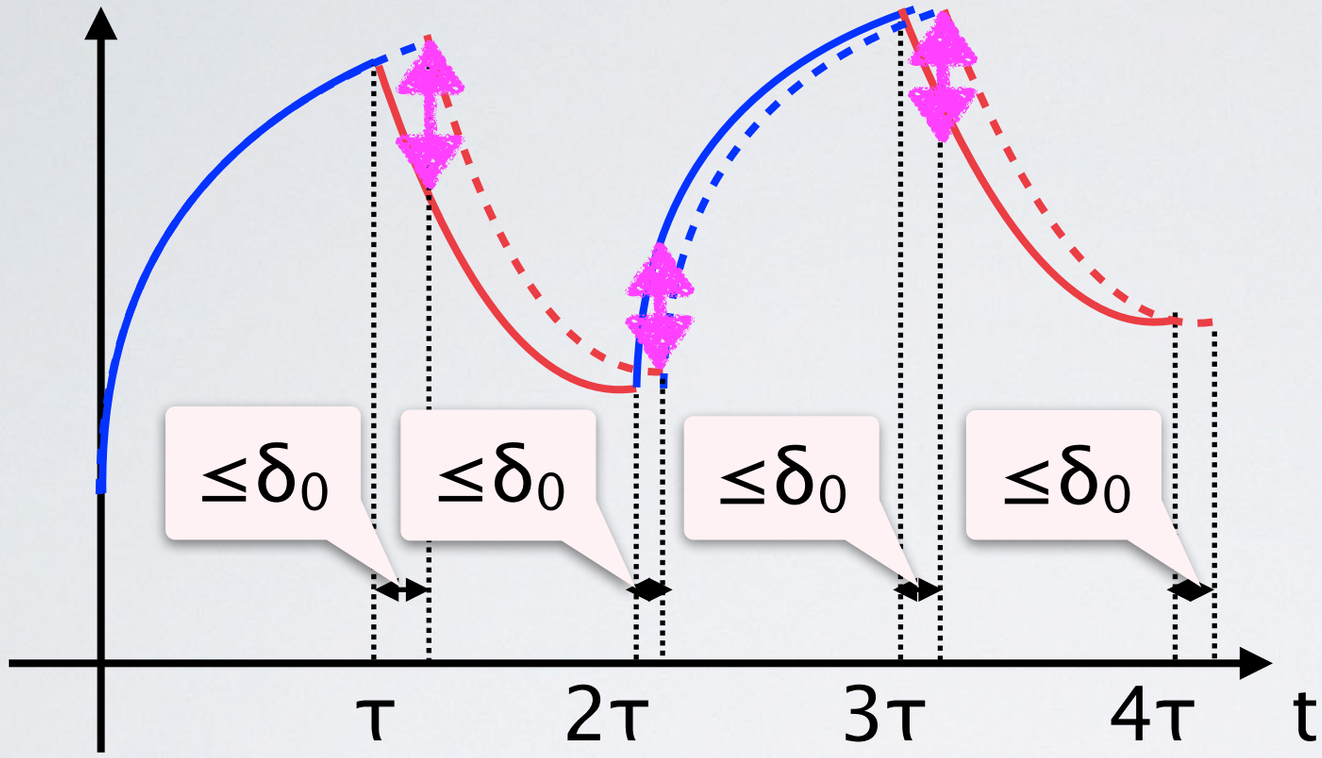
$\dot{x} = f_2(x)$

Ideal, without delay

Actual, with delay

Bounding Errors by Switching Delays

[Kido, Sedwards & Hasuo, IFAC ADHS '18]



$$\dot{x} = f_1(x)$$

$$\dot{x} = f_2(x)$$

Ideal, without delay

Actual, with delay

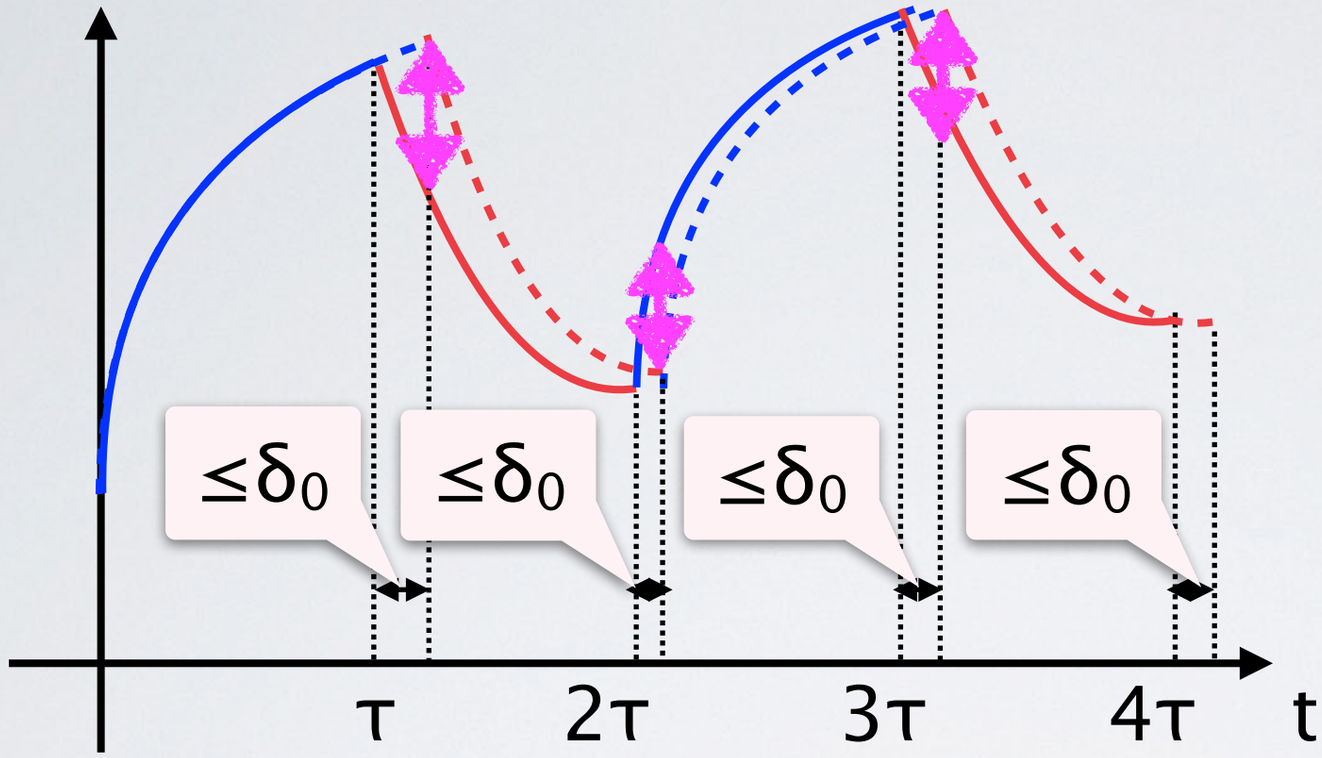
Thm. If the switched system has a common δ-GAS Lyapunov function V, then the gap (L∞ dist., ↕) is bounded by

$$\underline{\alpha}^{-1}\left(\frac{\nu\delta_0}{1-e^{-\kappa(\tau-\delta_0)}}\right)$$

Here $\underline{\alpha}$, $\varkappa$, ν are param's of the dynamics and V.

Bounding Errors by Switching Delays

[Kido, Sedwards & Hasuo, IFAC ADHS '18]



$$\dot{x} = f_1(x)$$

$$\dot{x} = f_2(x)$$

Ideal, without delay

Actual, with delay

Thm. If the switched system has a common δ-GAS Lyapunov function V, then the gap (L∞ dist., ↕) is bounded by

$$\underline{\alpha}^{-1}\left(\frac{\nu\delta_0}{1-e^{-\kappa(\tau-\delta_0)}}\right)$$

Here $\underline{\alpha}$, κ, ν are param's of the dynamics and V.

No accumulation of ↕

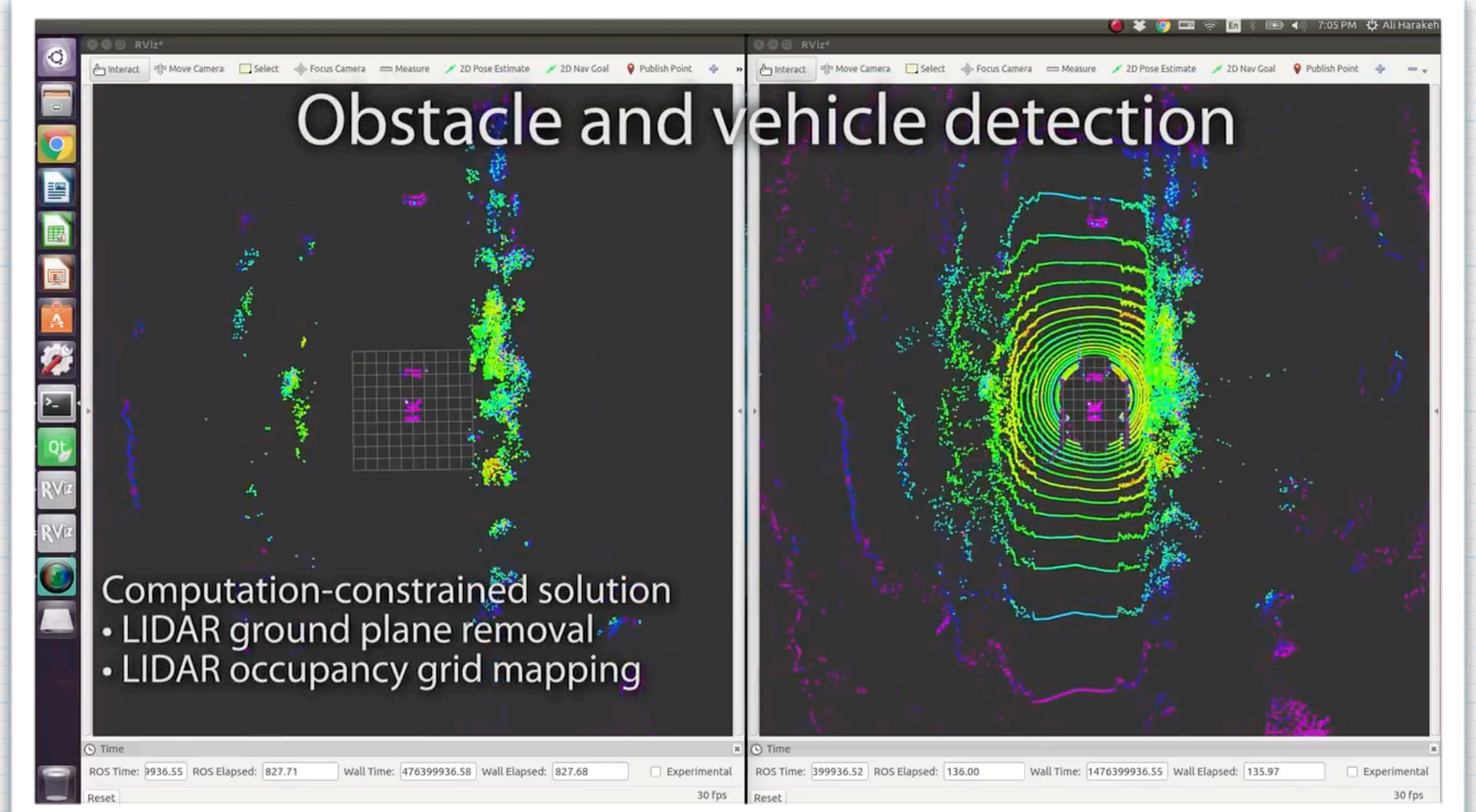
Outline

* 制御理論 vs 形式手法・ソフトウェア科学
* 数学的相似・相互乗り入れ
  * 例1（相似）：確率的プログラムのマルチンゲールによる解析
    [Chakarov & Sankaranarayanan, CAV'13] [Takisaka, Oyabu, Urabe & Hasuo, ATVA'18]
  * 例2（乗り入れ）：近似双模倣による離散化
    [Girard & Pappas, IEEE TAC '07] [Kido, Sedwards & Hasuo, IFAC ADHS '18]
* 実システム応用に向けて
  * 機械学習・AIとの協働
  * ソフトウェア工学，現実的解決
* ERATO MMSD プロジェクトの取り組み

実システム応用に向けて

* 自動運転を例に.

センシング ➔ 物体認識 ➔ 経路計画 ➔ 経路トレース

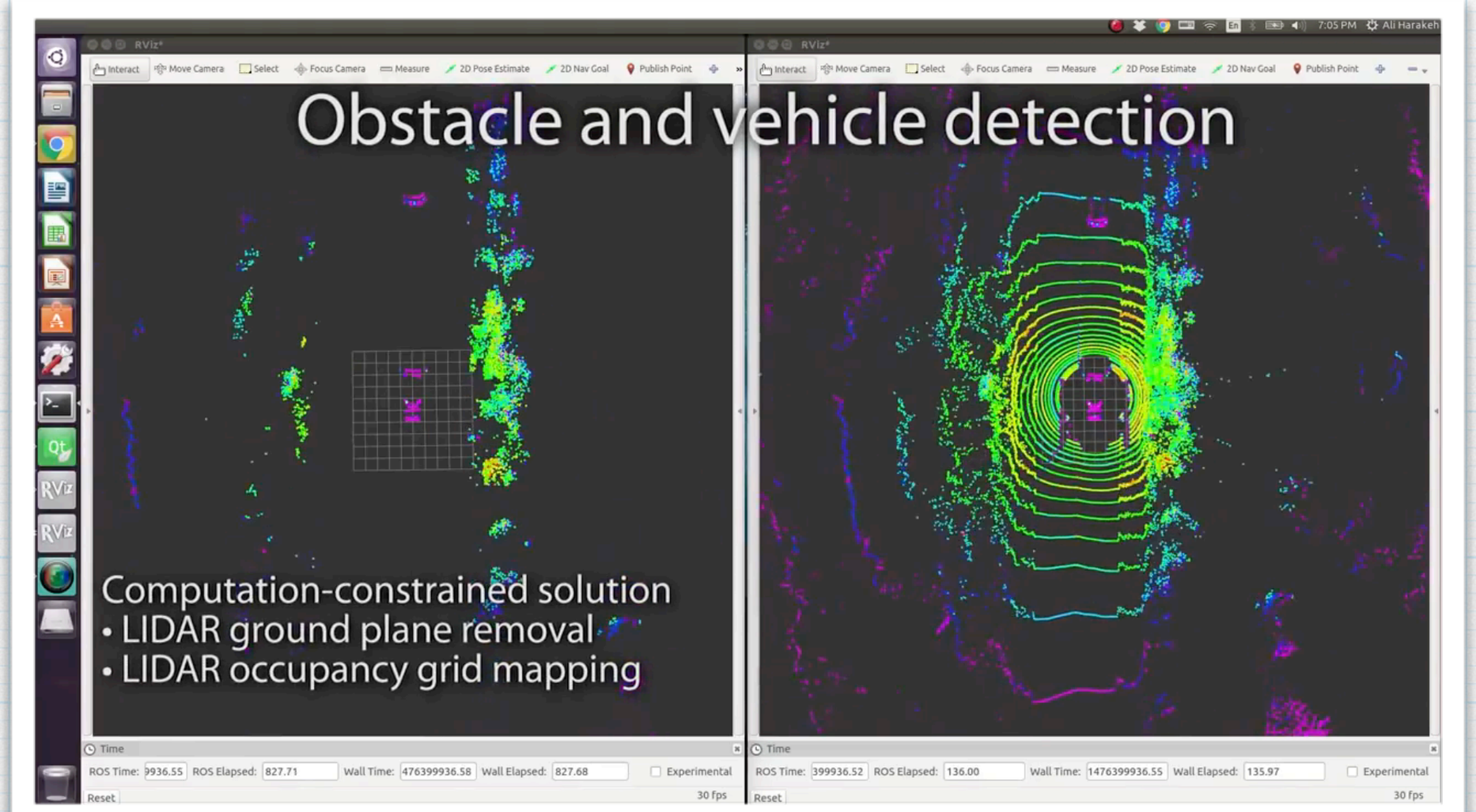


Autonomoose Project, U. Waterloo
www.autonomoose.net

実システム応用に向けて

* 自動運転を例に.

センシング ➔ 物体認識 ➔ 経路計画 ➔ 経路トレース

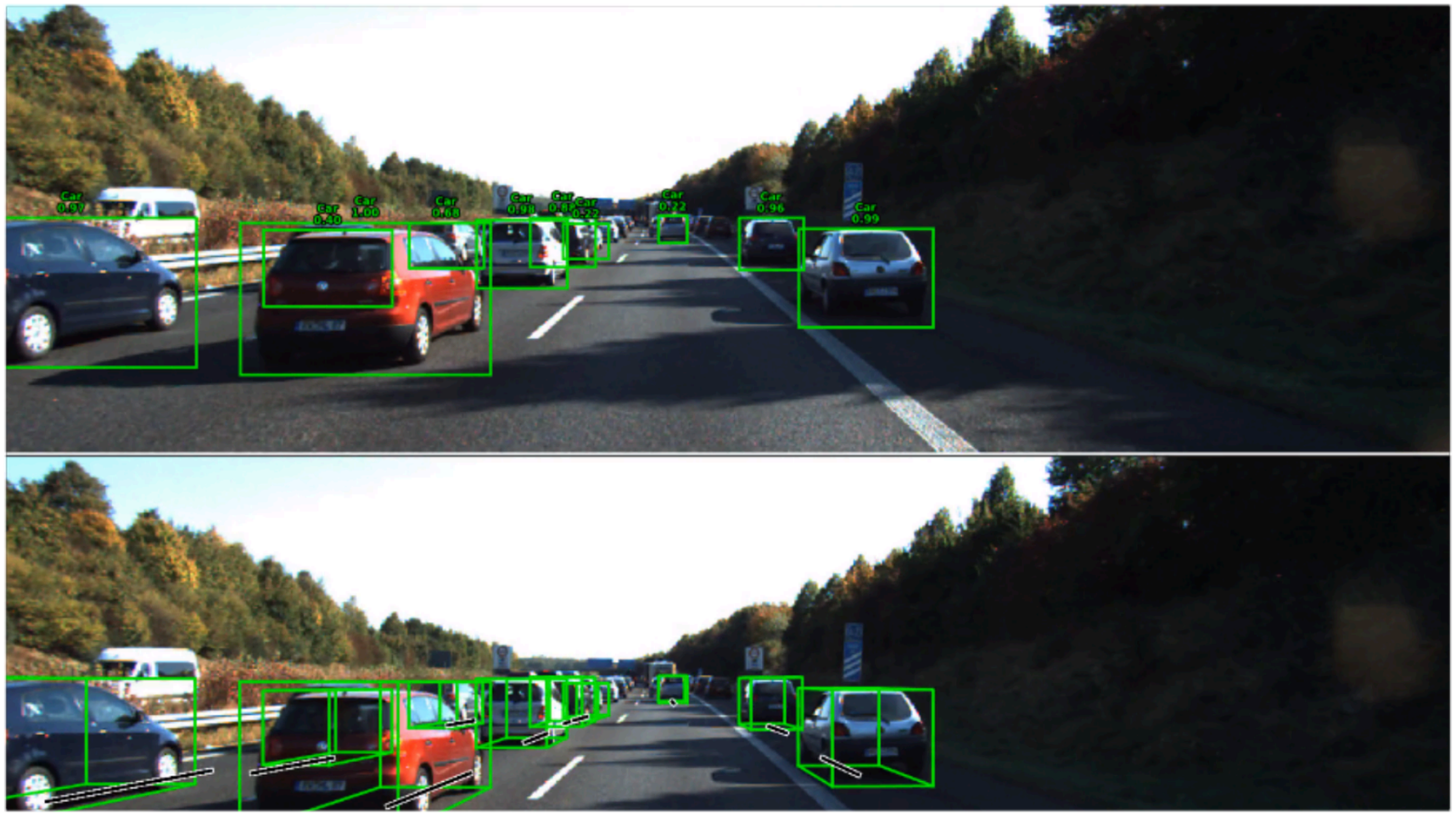


Autonomoose Project, U. Waterloo
www.autonomoose.net

実システム応用に向けて

* 自動運転を例に.

センシング ➜ 物体認識 ➜ 経路計画 ➜ 経路トレース

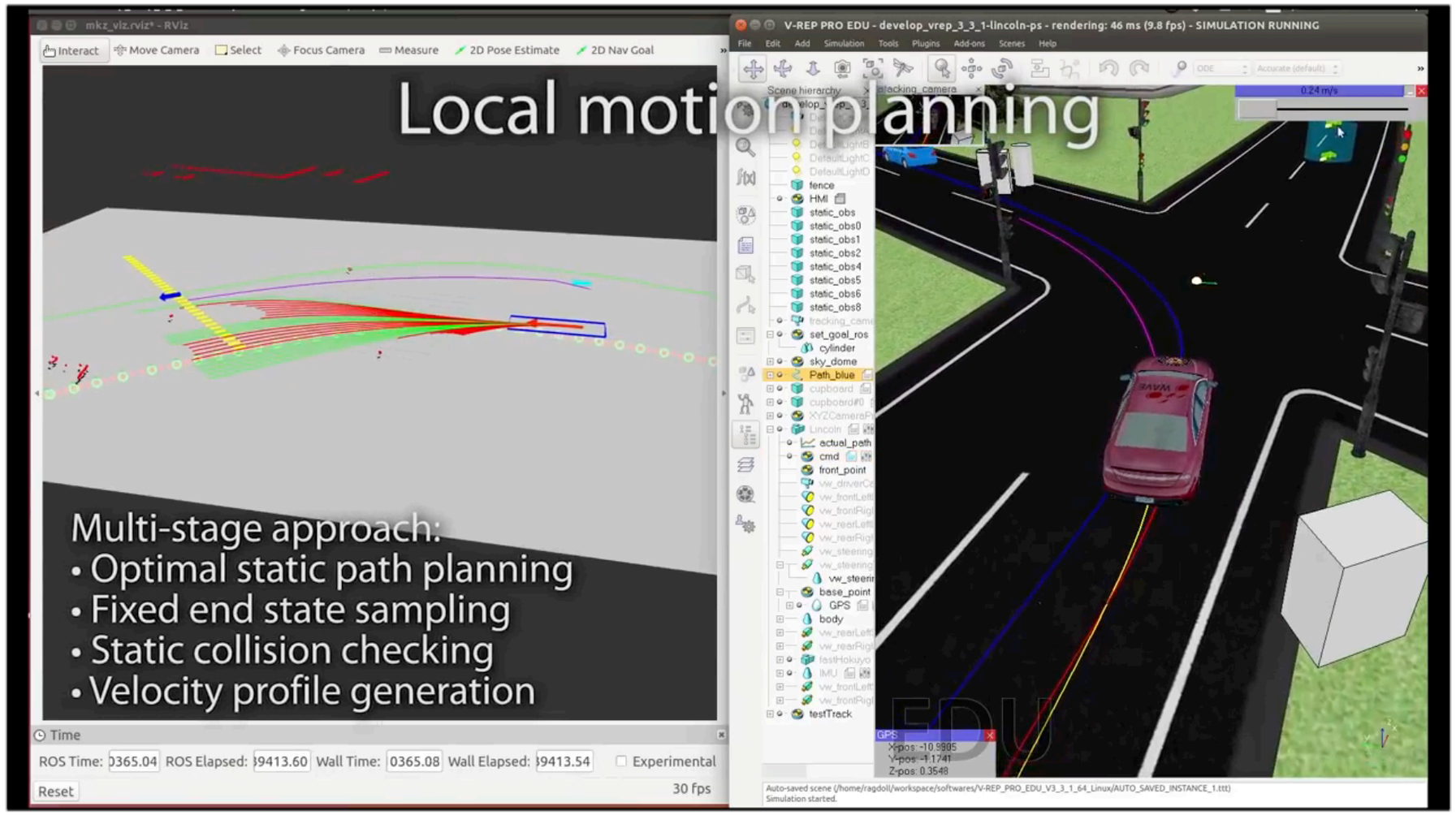


Autonomoose Project, U. Waterloo
www.autonomoose.net

実システム応用に向けて

* 自動運転を例に.

センシング ➔ 物体認識 ➔ 経路計画 ➔ 経路トレース

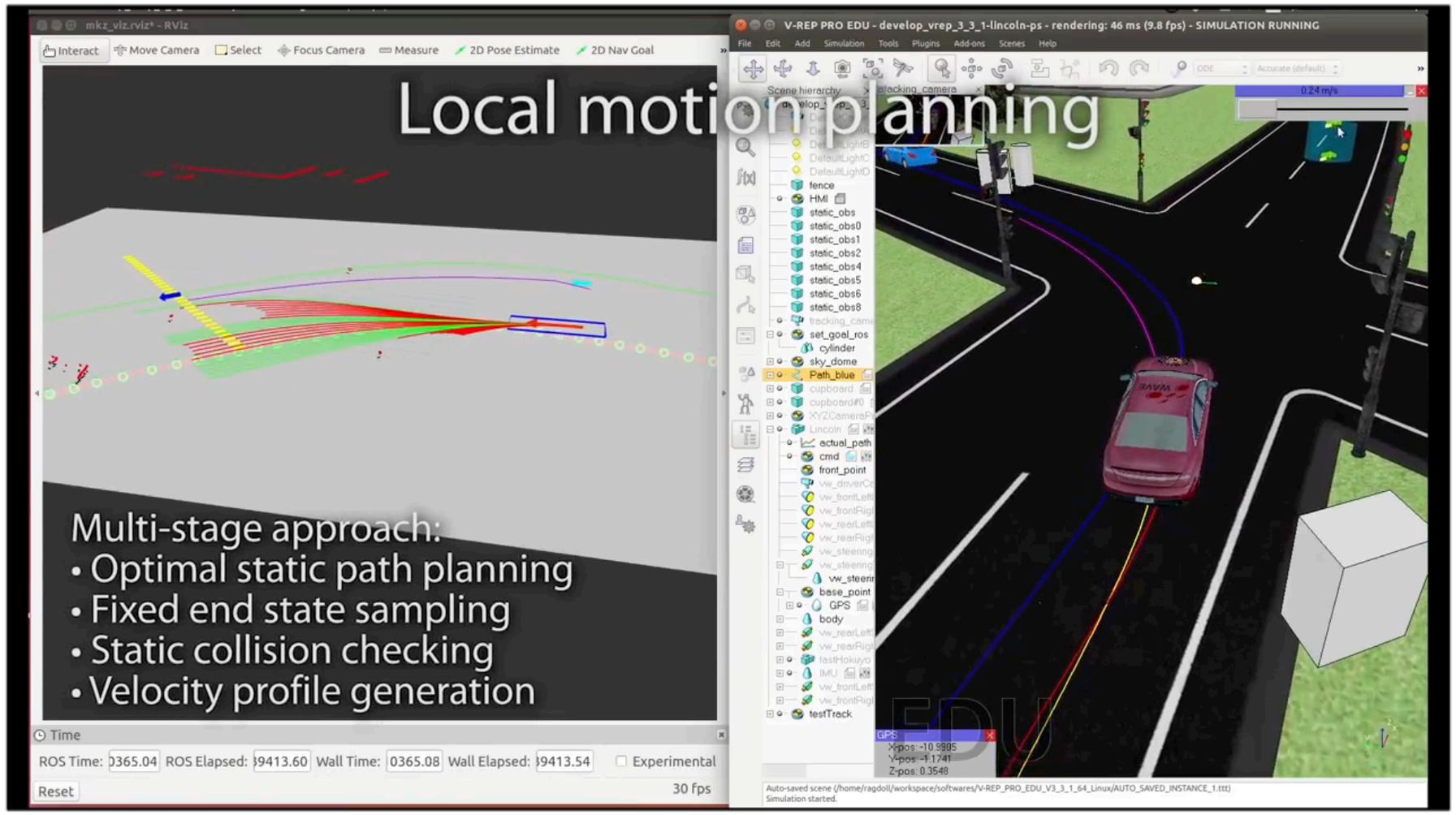


Autonomoose Project, U. Waterloo
www.autonomoose.net

実システム応用に向けて

* 自動運転を例に.

センシング ➔ 物体認識 ➔ 経路計画 ➔ 経路トレース



Autonomoose Project, U. Waterloo
www.autonomoose.net

実システム応用に向けて

* 自動運転を例に.

センシング ➔ 物体認識 ➔ 経路計画 ➔ 経路トレース

Autonomoose Project, U. Waterloo
www.autonomoose.net

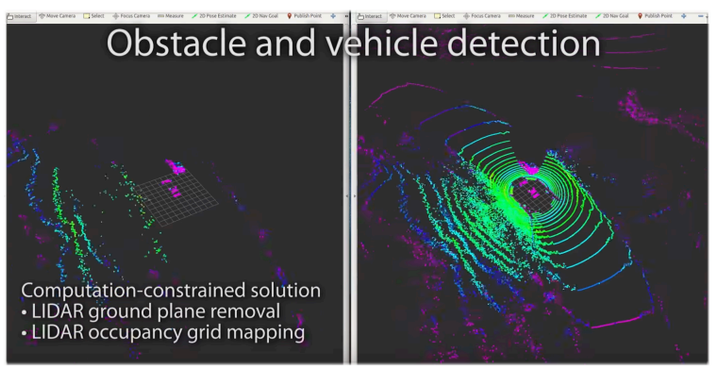
実システム応用に向けて

* 自動運転を例に.

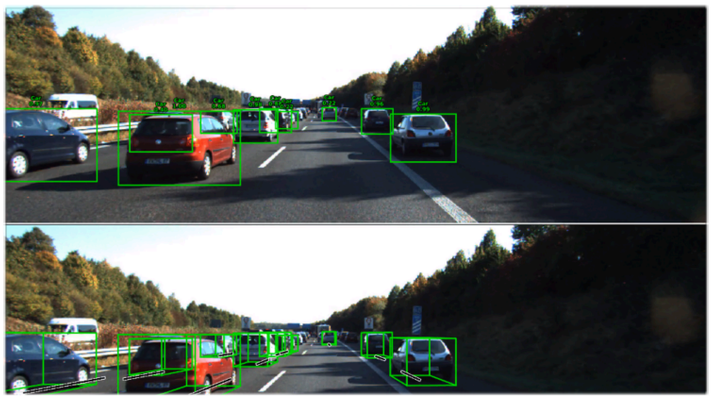
センシング ➔ 物体認識 ➔ 経路計画 ➔ 経路トレース

Autonomoose Project, U. Waterloo
www.autonomoose.net

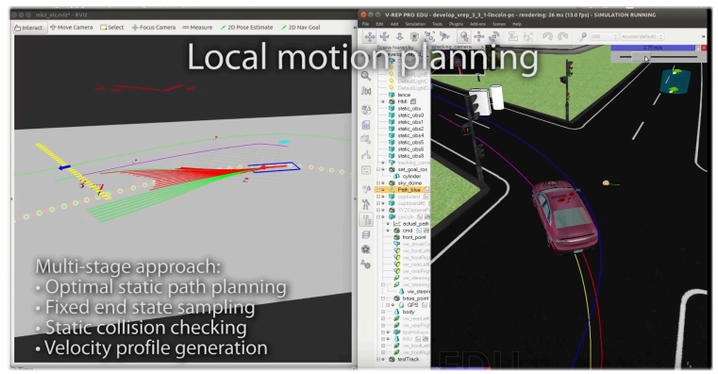
機械学習コンポーネントと，品質保証・説明責任



センシング



物体認識

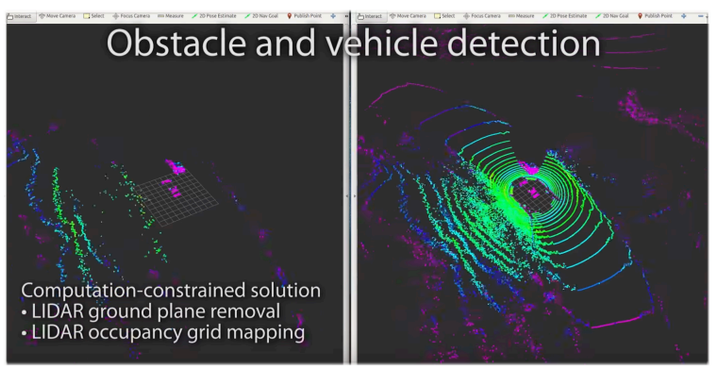


経路計画

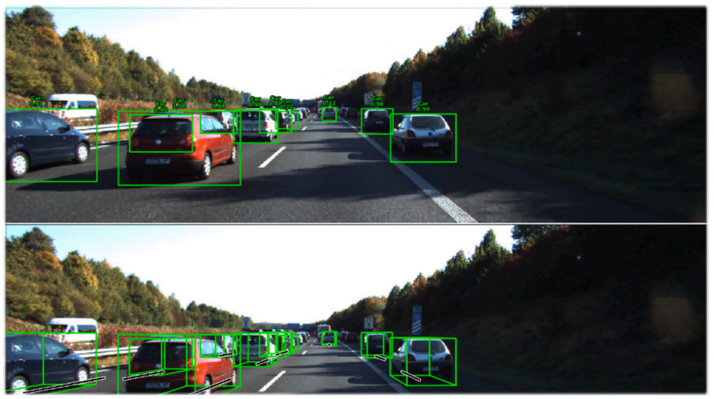
経路トレース

gtspirit.com
moralmachine.mit.edu

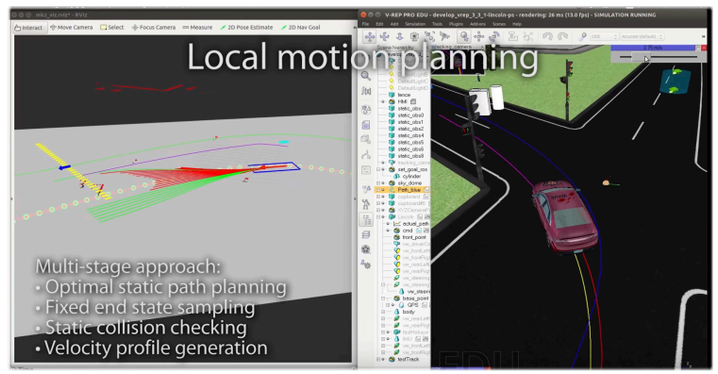
機械学習コンポーネントと，品質保証・説明責任



センシング



物体認識

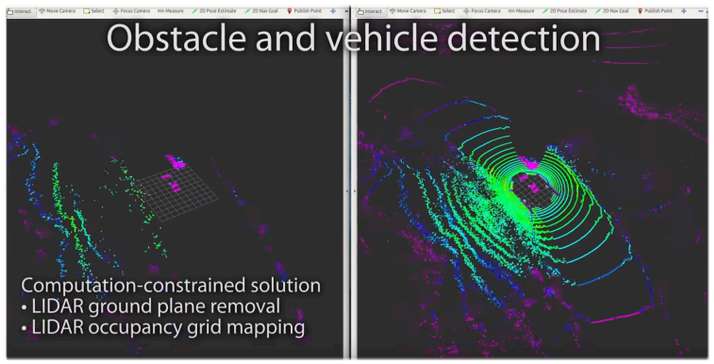


経路計画

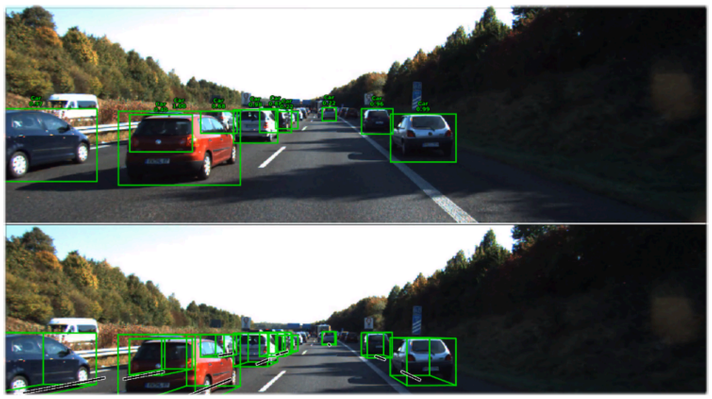
経路トレース

gtspirit.com
moralmachine.mit.edu

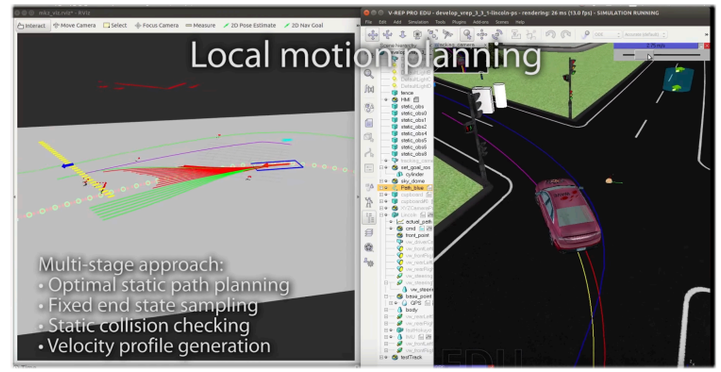
機械学習コンポーネントと，品質保証・説明責任



センシング

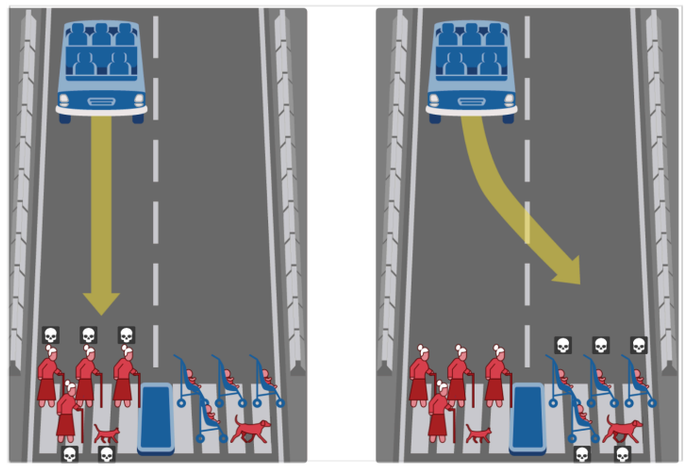


物体認識



経路計画

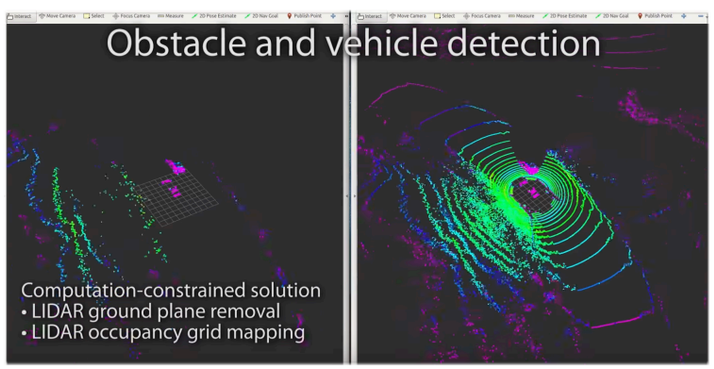
経路トレース



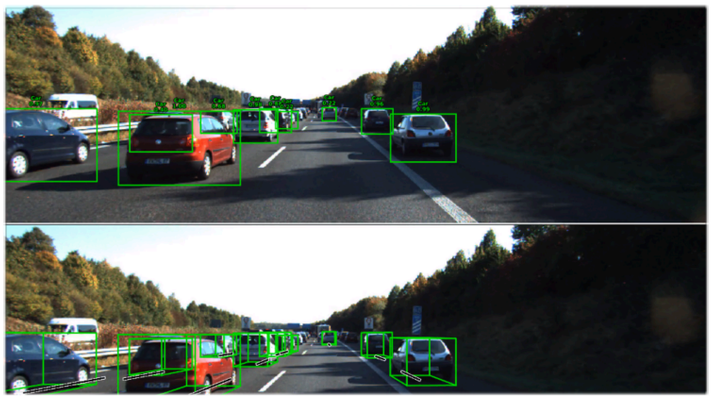
事故 & 原因解明 & 社会に対する説明

gtspirit.com
moralmachine.mit.edu

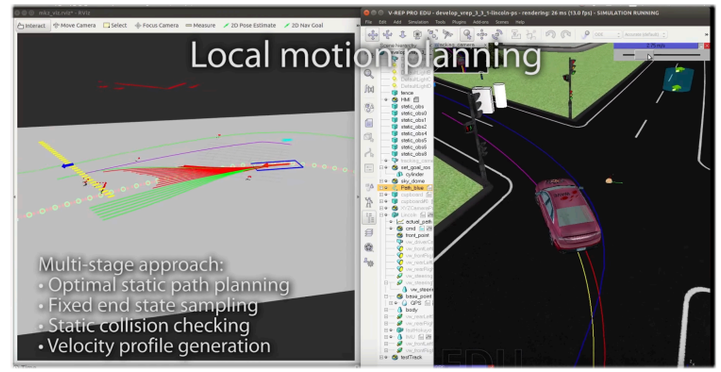
機械学習コンポーネントと，品質保証・説明責任



センシング

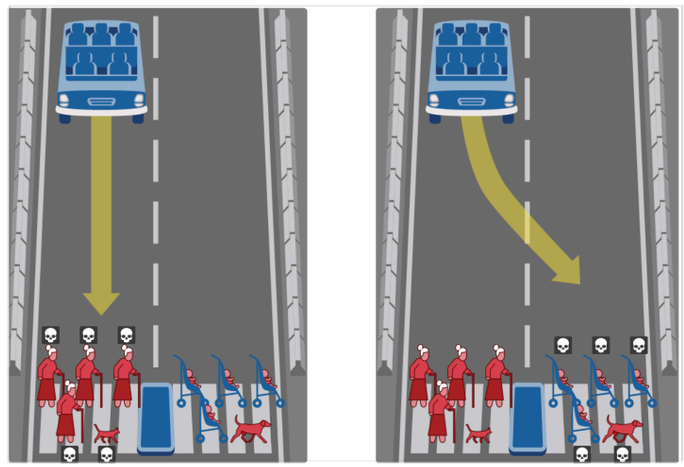


物体認識



経路計画

経路トレース



事故 & 原因解明 & 社会に対する説明

ニューラルネットは
ほぼブラックボックス…

gtspirit.com
moralmachine.mit.edu

統計的機械学習との協働

*

統計的機械学習	帰納的（データから学ぶ）	不確かさ（データのノイズ）	ブラックボックス
制御理論・形式手法	演繹的（証明）	数学的・論理的厳密性	ホワイトボックス

統計的機械学習との協働

*

統計的機械学習	帰納的（データから学ぶ）	不確かさ（データのノイズ）	ブラックボックス
制御理論・形式手法	演繹的（証明）	数学的・論理的厳密性	ホワイトボックス

統計的機械学習との協働

*

統計的機械学習	帰納的（データから学ぶ）	不確かさ（データのノイズ）	ブラックボックス
制御理論・形式手法	演繹的（証明）	数学的・論理的厳密性	ホワイトボックス

*

制御理論・形式手法

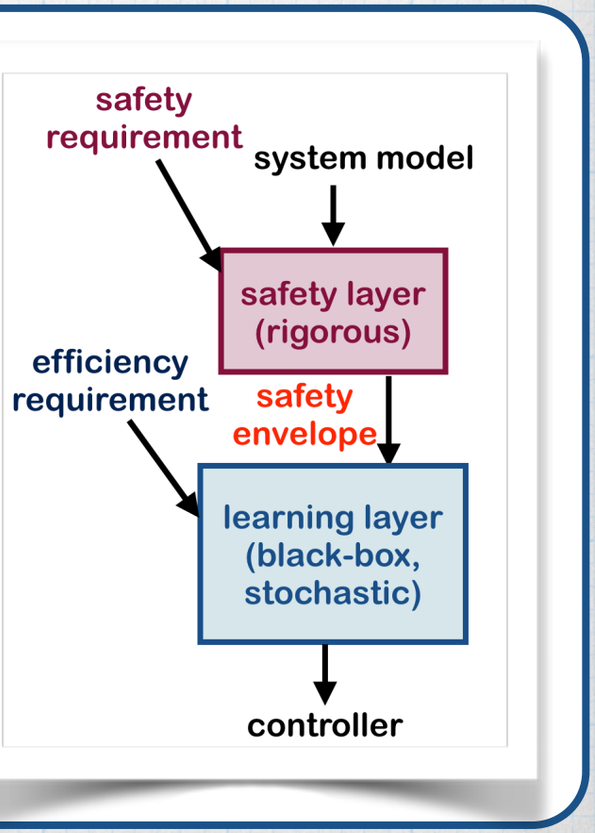
統計的機械学習

統計的機械学習との協働

統計的機械学習	帰納的（データから学ぶ）	不確かさ（データのノイズ）	ブラックボックス
制御理論・形式手法	演繹的（証明）	数学的・論理的厳密性	ホワイトボックス

制御理論・形式手法 → 統計的機械学習

* 不確かな機械学習コンポーネントを包み込む “safety envelope”
* 例： 自動運転の経路計画．safety envelope の中で最適化



ERATO 蓮
ERATO Metan
国立情報学研究所 & 科学技術振

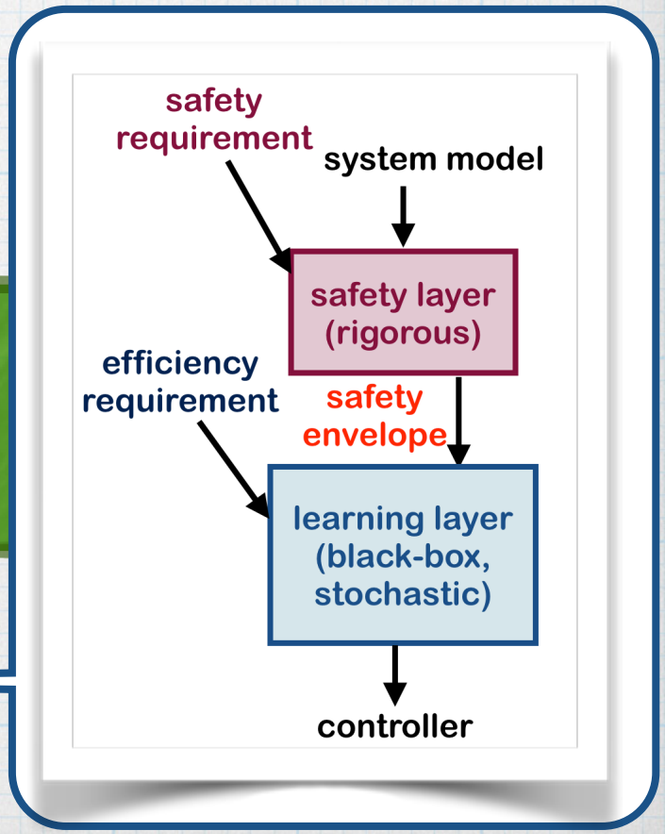
Key: 論理と統計的学習の間で,
システムレベルのタスク切り分けと構造化

統計的機械学習との協働

統計的機械学習	帰納的（データから学ぶ）	不確かさ（データのノイズ）	ブラックボックス
制御理論・形式手法	演繹的（証明）	数学的・論理的厳密性	ホワイトボックス

制御理論・形式手法 → 統計的機械学習

* 不確かな機械学習コンポーネントを包み込む “safety envelope”
* 例： 自動運転の経路計画．safety envelope の中で最適化



ERATO 蓮
ERATO Metan
国立情報学研究所 & 科学技術振

Key: 論理と統計的学習の間で,
システムレベルのタスク切り分けと構造化

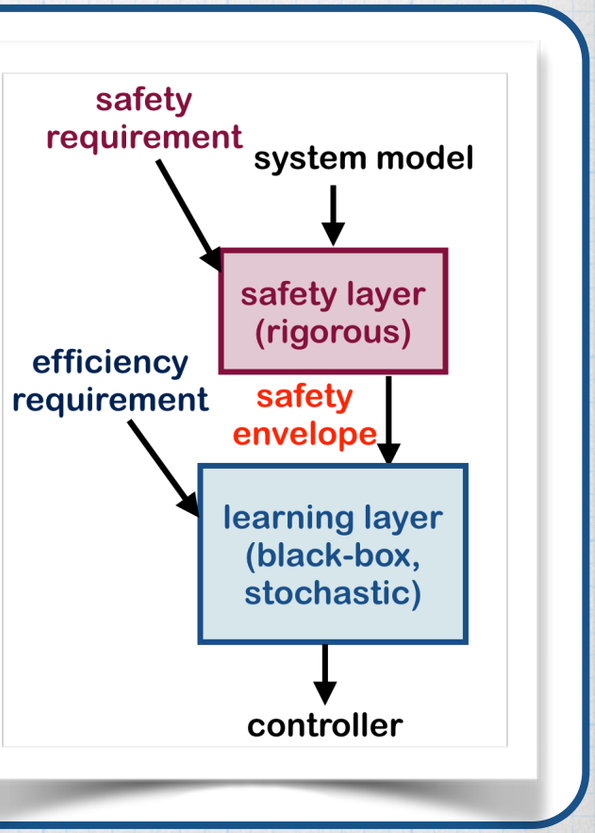
統計的機械学習との協働

統計的機械学習	帰納的（データから学ぶ）	不確かさ（データのノイズ）	ブラックボックス
制御理論・形式手法	演繹的（証明）	数学的・論理的厳密性	ホワイトボックス

* 総当たり探索の代わりに，データから傾向を読み取り高速に証明や補題を探索

制御理論・形式手法 ⇄ 統計的機械学習

* 不確かな機械学習コンポーネントを包み込む “safety envelope”
* 例： 自動運転の経路計画．safety envelope の中で最適化



ソフトウェア検証問題

翻訳

- spec ↦ automaton
- model ↦ prop. formula
- …

制約充足問題

- SAT
- graph reachability
- …

制御問題

翻訳

最適化問題

- LMI
- SDP
- mixed integer
- stochastic optimization
- …

ソフトウェア検証問題

制御問題

翻訳

- spec ↦ automaton
- model ↦ prop. formula
- …

翻訳

確率的最適化
機械学習

ソフトウェア検証問題

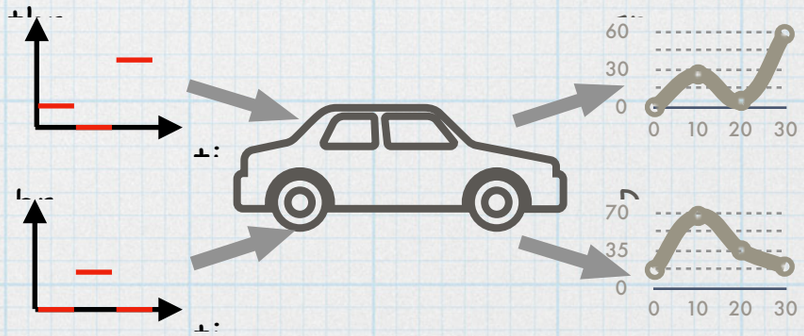
制御問題

翻訳
- spec ↦ automaton
- model ↦ prop. formula
- …

翻訳

確率的最適化
機械学習

- 例：
  - Simulink モデルと時相論理式仕様に対する
    サーチベーステスト，反例生成
    [Zhang, Ernst, Sedwards, Arcaini & Hasuo, EMSOFT'18]
    - 確率的最適化による
      ブラックボックスアプローチ
    - Cf. S-TaLiRo, BREACH, …



$\square_{[0,30]}(speed < 120)$

制御理論・形式手法のソフトウェア工学的応用

* 困難
  * スケーラビリティ
  * システムの「定義」（＝ホワイトボックス・モデル）が必要
    * 実システムではむずかしい（自動車部品，NNなど）
* 産業応用における証明の意義．「労力の割にありがたがられない」
  * 環境への仮定に依存 ➜ 仮定の正しさをどう担保する？

制御理論・形式手法のソフトウェア工学的応用

* 困難
  * スケーラビリティ
  * システムの「定義」（＝ホワイトボックス・モデル）が必要
    * 実システムではむずかしい（自動車部品，NNなど）
  * 産業応用における証明の意義．「労力の割にありがたがられない」
    * 環境への仮定に依存 ➜ 仮定の正しさをどう担保する？
* ➜ 現行の帰納的品質保証手段（＝テスト）のサポートに注力
  * ソフトウェア工学の考え方．テスト，実行時検証
  * 形式手法の演繹的推論が決定的に有効
    （サーチベーステストのスコア定義，テスト空間の削減，…）
  * テストの有効性の数学的議論 ➜ 品質保証の業界標準，国際規格，…

制御理論・形式手法のソフトウェア工学的応用

* 困難
  * スケーラビリティ
  * システムの「定義」（＝ホワイトボックス・モデル）が必要
    * 実システムではむずかしい（自動車部品，NNなど）
  * 産業応用における証明の意義．「労力の割にありがたがられない」
    * 環境への仮定に依存 ➜ 仮定の正しさをどう担保する？
* ➜ 現行の帰納的品質保証手段（＝テスト）のサポートに注力
  * ソフトウェア工学の考え方．テスト，実行時検証
  * 形式手法の演繹的推論が決定的に有効
    （サーチベーステストのスコア定義，テスト空間の削減，…）
  * テストの有効性の数学的議論 ➜ 品質保証の業界標準，国際規格，…

「〇〇の範囲にバグはない」ことを証明
➜ 〇〇の範囲をテストする必要はない

制御理論・形式手法のソフトウェア工学的応用

* 困難
  * スケーラビリティ
  * システムの「定義」（＝ホワイトボックス・モデル）が必要
    * 実システムではむずかしい（自動車部品，NNなど）
  * 産業応用における証明の意義．「労力の割にありがたがられない」
    * 環境への仮定に依存 ➜ 仮定の正しさをどう担保する？
* ➜ 現行の帰納的品質保証手段（＝テスト）のサポートに注力
  * ソフトウェア工学の考え方．テスト，実行時検証
  * 形式手法の演繹的推論が決定的に有効
    （サーチベーステストのスコア定義，テスト空間の削減，…）
  * テストの有効性の数学的議論 ➜ 品質保証の業界標準，国際規格，…

「〇〇の範囲にバグはない」ことを証明
➜ 〇〇の範囲をテストする必要はない

「何をチェックすれば十分と認められるのか」の工学的見極め

Outline

* 制御理論 vs 形式手法・ソフトウェア科学
* 数学的相似・相互乗り入れ
  * 例1（相似）：確率的プログラムのマルチンゲールによる解析
    [Chakarov & Sankaranarayanan, CAV'13] [Takisaka, Oyabu, Urabe & Hasuo, ATVA'18]
  * 例2（乗り入れ）：近似双模倣による離散化
    [Girard & Pappas, IEEE TAC '07] [Kido, Sedwards & Hasuo, IFAC ADHS '18]
* 実システム応用に向けて
  * 機械学習・AIとの協働
  * ソフトウェア工学，現実的解決
* ERATO MMSD プロジェクトの取り組み

ERATO 蓮尾メタ数理システムデザインプロジェクト
ERATO Metamathematics for Systems Design Project
国立情報学研究所 & 科学技術振興機構 National Institute of Informatics & Japan Science and Technology Agency

プロジェクト紹介

* プロジェクト目標： 工業製品の設計サポート
  * 形式手法をソフトウェアから物理情報システムへ
  * 工業製品の品質保証をサポート，省力化

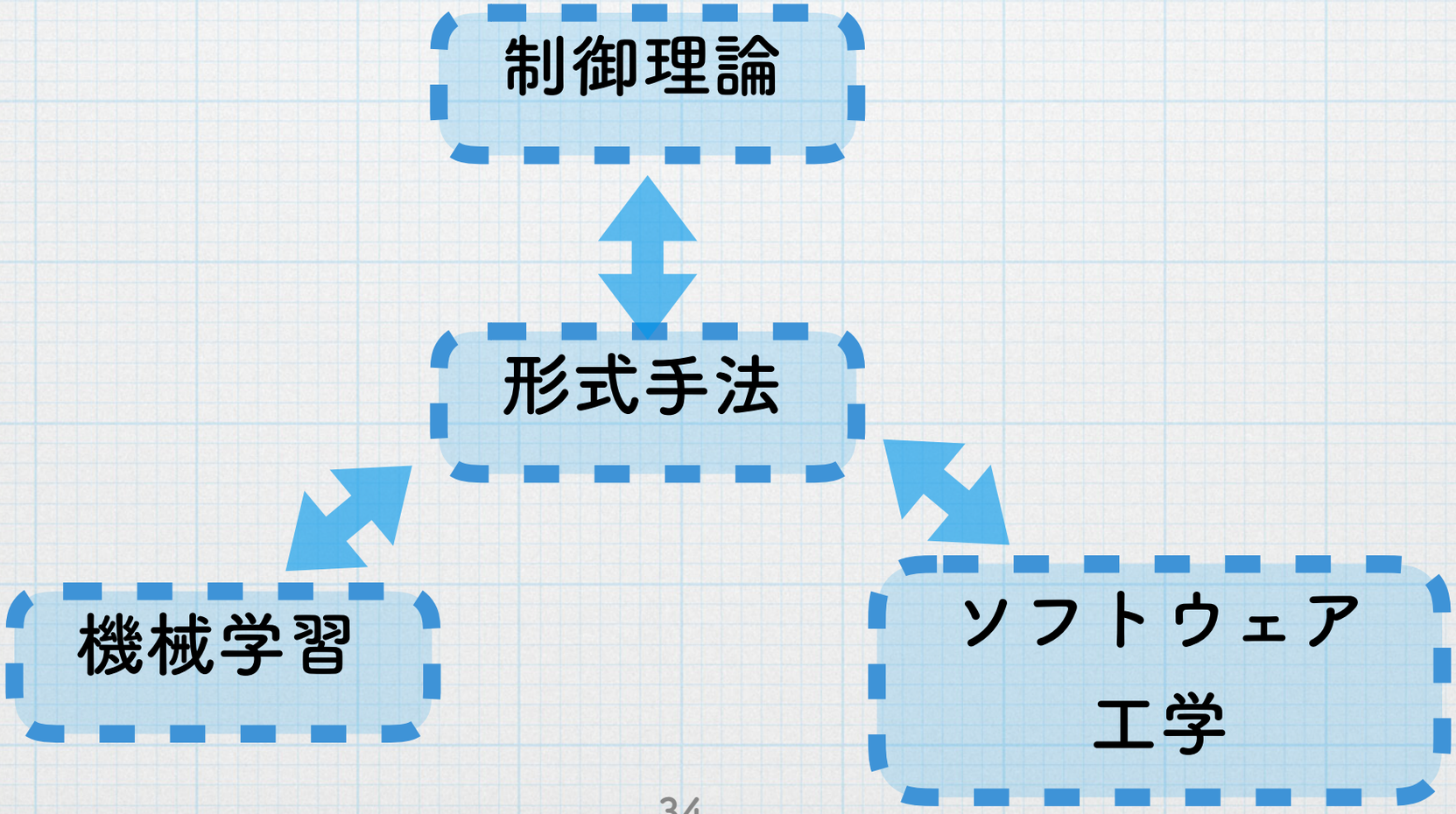
* Challenge: 関連分野の多様性
  * 計算機科学，制御理論，ソフトウェア工学，機械学習，etc.
* 方法論： 圏論・代数学的メタ理論による統合
* > 10 名の特任教員・研究員を含む 50 名体制で理論研究を推進.
* 国内製造業企業（自動車関連），U Waterloo 自動運転プロジェクトと協働，社会応用
* 特任教員・特任研究員募集中 (-2022). https://group-mmm.org/eratommsd/openpositions/

私達の取り組み： ３つの柱

* 連続量を扱う形式手法：
* 統計的機械学習と協働する形式手法
* 演繹的手法のソフトウェア工学的応用

私達の取り組み： ３つの柱

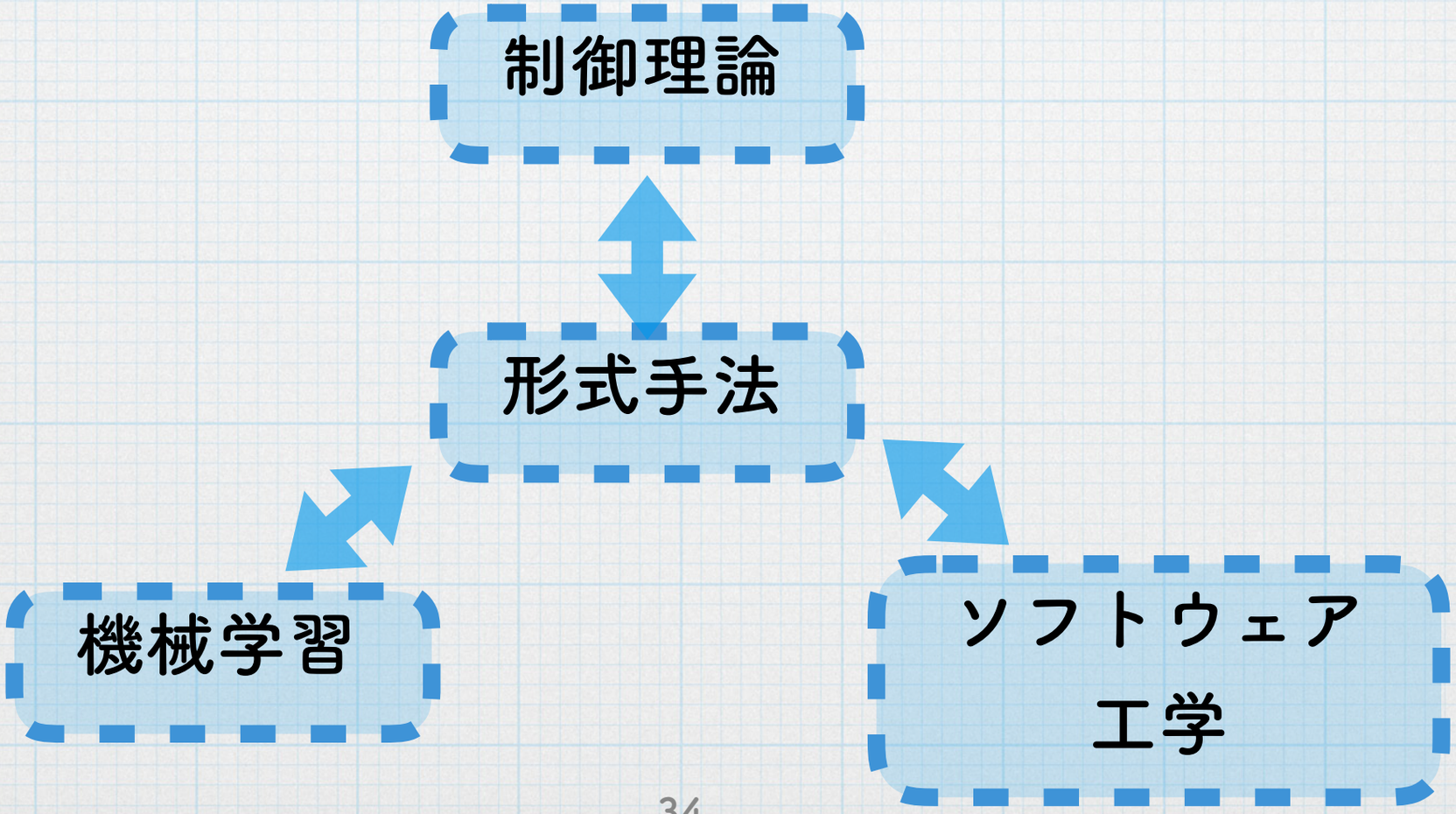
* 連続量を扱う形式手法：
* 統計的機械学習と協働する形式手法
* 演繹的手法のソフトウェア工学的応用



私達の取り組み：３つの柱

* 連続量を扱う形式手法：
* 統計的機械学習と協働する形式手法
* 演繹的手法のソフトウェア工学的応用

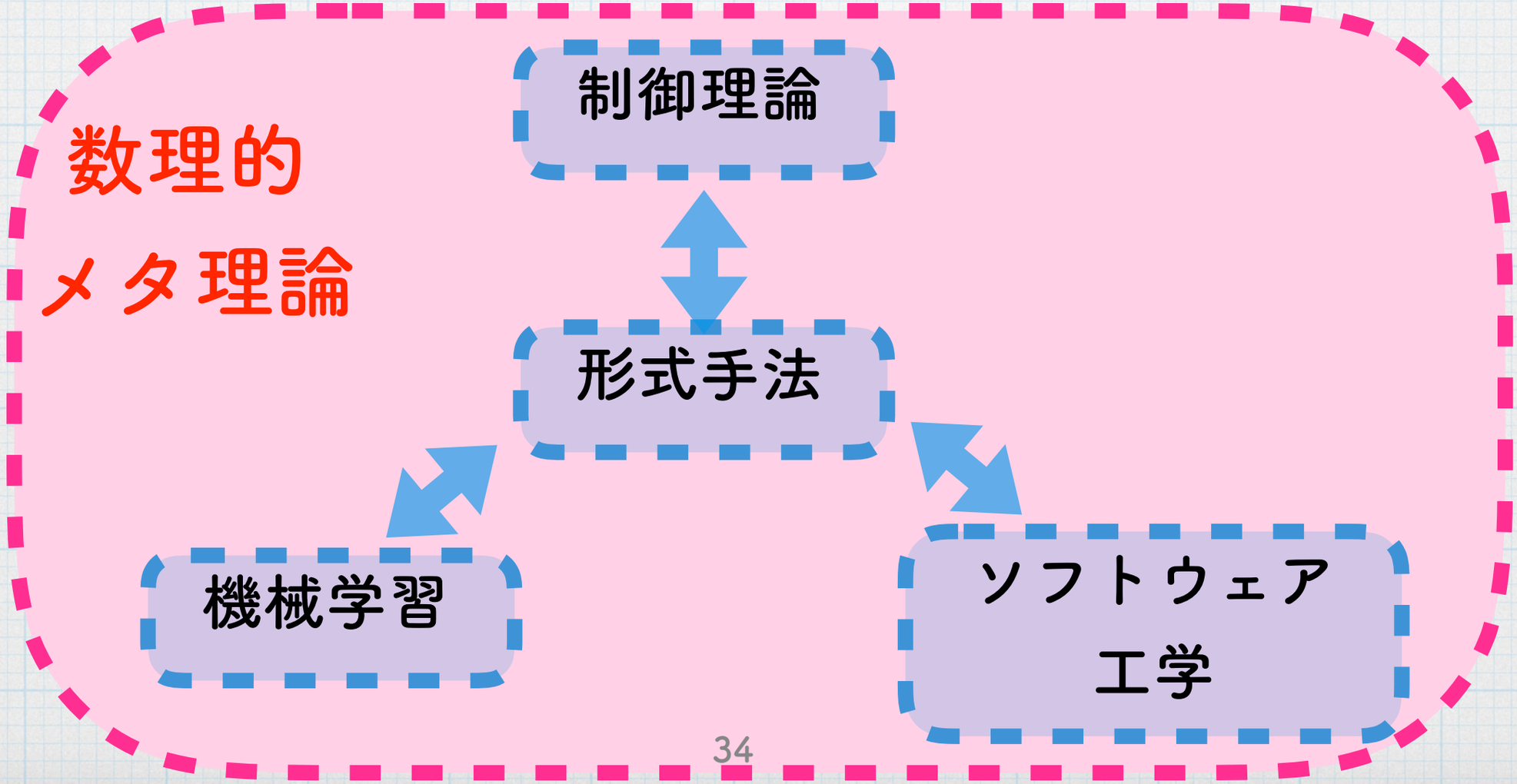
制御理論との協働.
潮俊光（阪大），岸田昌子（NII），
脇隼人（九大）



私達の取り組み：３つの柱

* 連続量を扱う形式手法：
* 統計的機械学習と協働する形式手法
* 演繹的手法のソフトウェア工学的応用

制御理論との協働.
潮俊光（阪大），岸田昌子（NII），
脇隼人（九大）



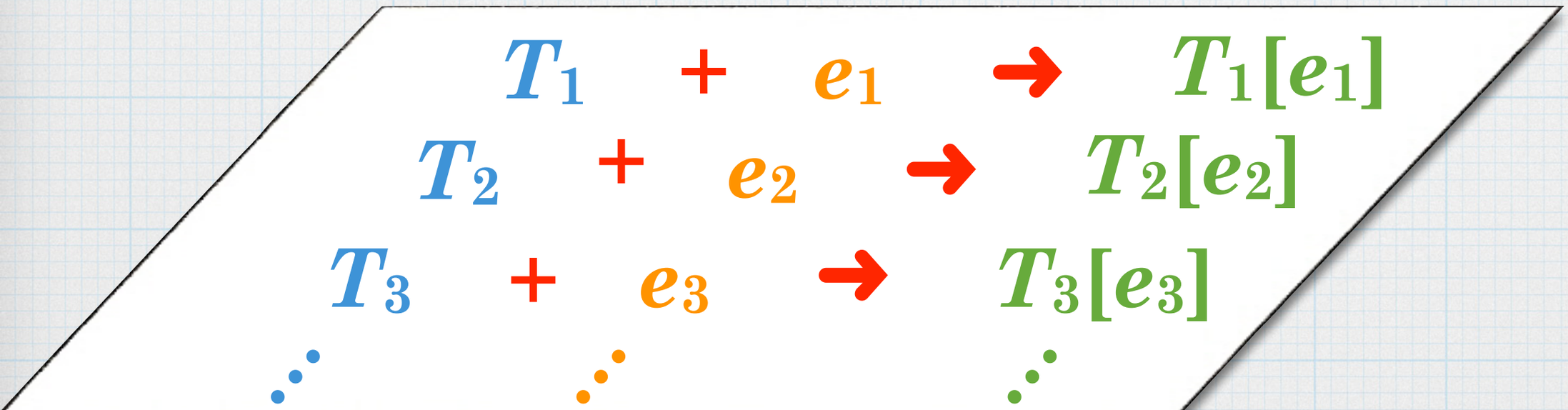
ＥＲＡＴＯ　蓮尾メタ数理システムデザインプロジェクト
ERATO Metamathematics for Systems Design Project

国立情報学研究所 & 科学技術振興機構　National Institute of Informatics & Japan Science and Technology Agency

ＥＲＡＴＯ　蓮尾メタ数理システムデザインプロジェクト
ERATO Metamathematics for Systems Design Project

国立情報学研究所 & 科学技術振興機構　National Institute of Informatics & Japan Science and Technology Agency

独自の方法論：
メタ理論による移転

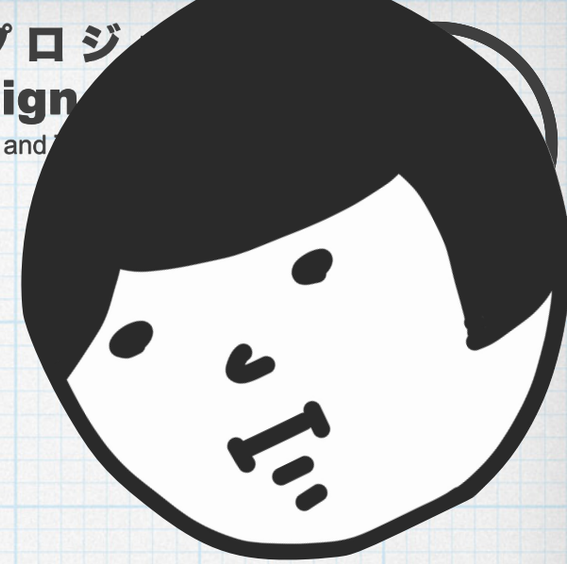


ソフトウェアの
ための形式手法

新たな関心事
連続量，不確かさ，…

物理情報システム
のための形式手法

独自の方法論：
メタ理論による移転



メタ理論家

論理学，
代数学，圏論，
…

$T_1 + e_1 \rightarrow T_1[e_1]$

$T_2 + e_2 \rightarrow T_2[e_2]$

$T_3 + e_3 \rightarrow T_3[e_3]$

$\vdots \quad \vdots \quad \vdots$

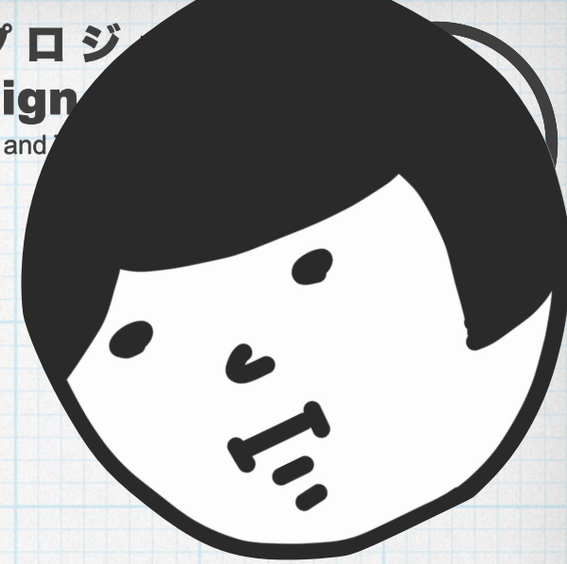
ソフトウェアの
ための形式手法

新たな関心事
連続量，不確かさ，…

物理情報システム
のための形式手法

独自の方法論：
メタ理論による移転

理論拡張のプロセス
自体を理論的に解析



メタ理論家

論理学，
代数学，圏論，
…

$T_1 + e_1 \rightarrow T_1[e_1]$

$T_2 + e_2 \rightarrow T_2[e_2]$

$T_3 + e_3 \rightarrow T_3[e_3]$

$\vdots \quad \vdots \quad \vdots$

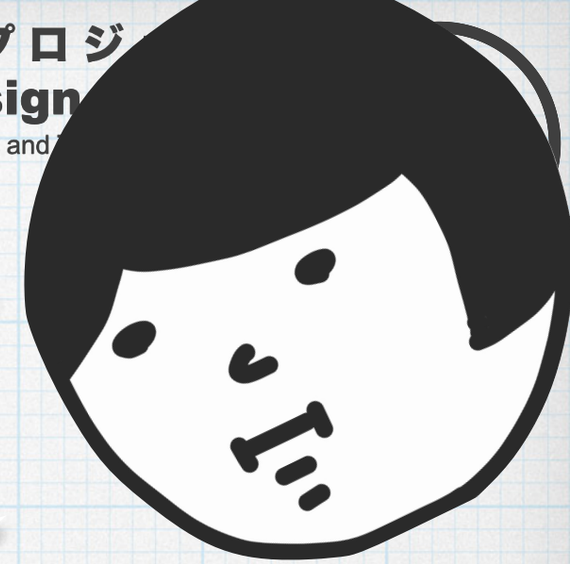
ソフトウェアの
ための形式手法

新たな関心事
連続量，不確かさ，…

物理情報システム
のための形式手法

独自の方法論：
メタ理論による移転

理論拡張のプロセス
自体を理論的に解析



メタ理論家

論理学，
代数学，圏論，
…

… $T + e \rightarrow T[e]$
の包括的な一般論を構築
（さまざまな T と e に一挙に適用可能）

$T_1 + e_1 \rightarrow T_1[e_1]$
$T_2 + e_2 \rightarrow T_2[e_2]$
$T_3 + e_3 \rightarrow T_3[e_3]$
⋮　⋮　⋮

ソフトウェアの
ための形式手法

新たな関心事
連続量，不確かさ，…

物理情報システム
のための形式手法

Existing Technique

T_1

Abstract Technique

$T[\_]$

Identify
"mathematical
essense"

Existing Technique

T_1

Abstract Technique

$T[\_]$

Identify "mathematical essense"

Choose parameter e_1

Existing Technique

$T_1 = T[e_1]$

Abstract Technique

$T[\_]$

Identify "mathematical essense"

Choose parameter e_1

Choose parameter e_2

Existing Technique

$T_1 = T[e_1]$

Novel Technique

$T[e_2]$

論理学,
代数学, 圏論,
…

ERATO MSD

Abstract Technique

$T[\_]$

$$A ::= \texttt{true} \mid \texttt{false} \mid A_1 \wedge A_2 \mid \neg A \mid a_1 < a_2 \mid \forall x \in {}^*\mathbb{N}.\, A \mid \forall x \in {}^*\mathbb{R}.\, A$$

$$\begin{array}{ccc} FX & \xrightarrow{F\mathbf{beh}_c} & FZ \\ {\scriptstyle c}\uparrow & & \uparrow{\scriptstyle \text{final}} \\ X & \xrightarrow[\mathbf{beh}_c]{} & Z \end{array}$$
system behavior

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & FY \\ {\scriptstyle c}\uparrow & \sqsupseteq & \uparrow{\scriptstyle d} \\ X & \xrightarrow[f]{} & Y \end{array}$$
simulation

Identify "mathematical essense"

Choose parameter e_1

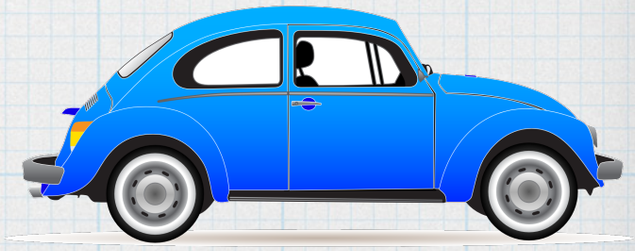
Choose parameter e_2

Existing Technique

$T_1 = T[e_1]$

Novel Technique

$T[e_2]$



ERATO 蓮尾メタ数理システムデザ
ERATO Metamathematics for Syste
国立情報学研究所 & 科学技術振興機構 National Institute of Informatics

論理学,
代数学, 圏論,
…

ERATO MSD

Abstract Technique

$$T[\_]$$

$$A ::= \texttt{true} \mid \texttt{false} \mid A_1 \wedge A_2 \mid \neg A \mid a_1 < a_2 \mid \forall x \in {}^*\mathbb{N}.\, A \mid \forall x \in {}^*\mathbb{R}.\, A$$

$$\begin{array}{ccc} FX & \xrightarrow{F\mathbf{beh}_c} & FZ \\ {\scriptstyle c}\uparrow & & \uparrow{\scriptstyle \text{final}} \\ X & \xrightarrow[\mathbf{beh}_c]{} & Z \end{array}$$
system behavior

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & FY \\ {\scriptstyle c}\uparrow & \sqsupseteq & \uparrow{\scriptstyle d} \\ X & \xrightarrow[f]{} & Y \end{array}$$
simulation

Identify "mathematical essense"

Choose parameter e_1

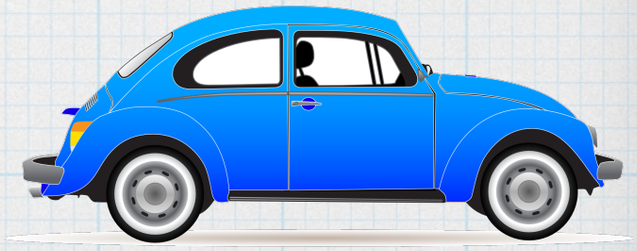
Choose parameter e_2

Existing Technique

$$T_1 = T[e_1]$$

Novel Technique

$$T[e_2]$$



- 物理情報システムの多様な応用に即応
- 産業界（製造業）のニーズに根ざした理論展開
- 現代数学の抽象性から生まれる応用

まとめ

* 制御理論 vs 形式手法・ソフトウェア科学
* 数学的相似・相互乗り入れ
  * 例1（相似）：確率的プログラムのマルチンゲールによる解析
    [Chakarov & Sankaranarayanan, CAV'13] [Takisaka, Oyabu, Urabe & Hasuo, ATVA'18]
  * 例2（乗り入れ）：近似双模倣による離散化
    [Girard & Pappas, IEEE TAC '07] [Kido, Sedwards & Hasuo, IFAC ADHS '18]
* 実システム応用に向けて
  * 機械学習・AIとの協働
  * ソフトウェア工学，現実的解決
* ERATO MMSD プロジェクトの取り組み