ERATO MMSDプロジェクト紹介

高信頼物理情報システムのための包括的研究

蓮尾 一郎

国立情報学研究所 (NII) システム設計数理国際研究センター センター長・准教授

JST ERATO 蓮尾メタ数理システムデザインプロジェクト 研究総括

総合研究大学院大学 准教授

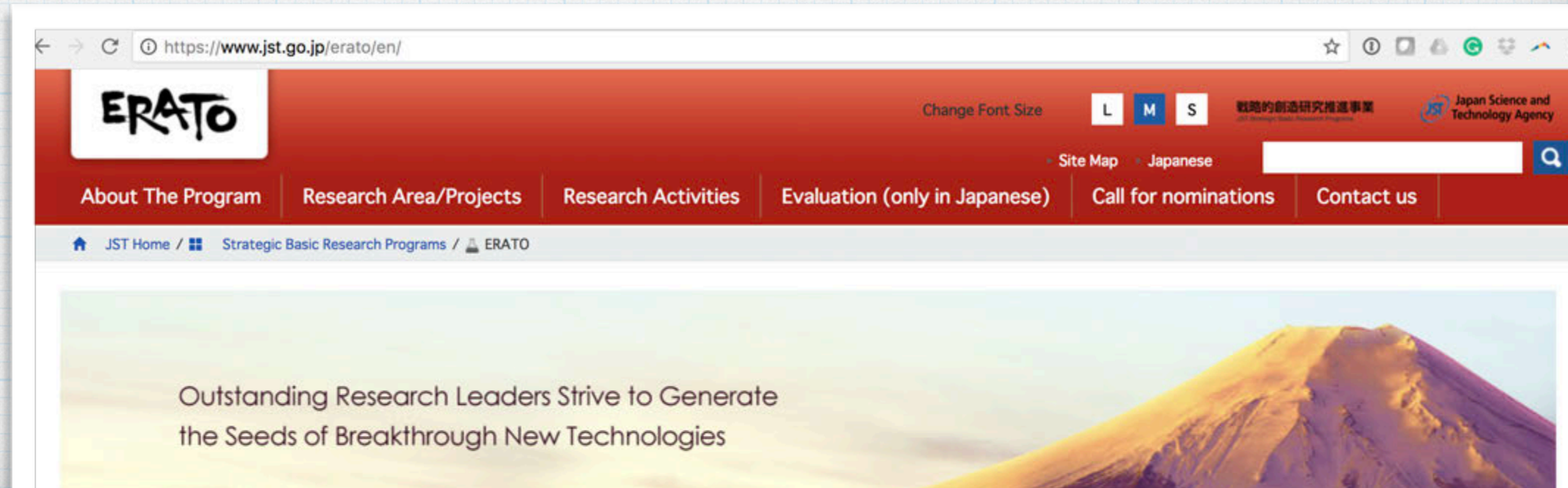
アウトライン

- ERATO MMSD プロジェクト概要
- 形式手法と物理情報システム
- プロジェクトの研究開発状況
- 技術紹介
  - 形式手法・テストによるシステム品質保証手法，特に
    - サーチベーステスト
    - 実行時監視
- 今後の協働に向けて

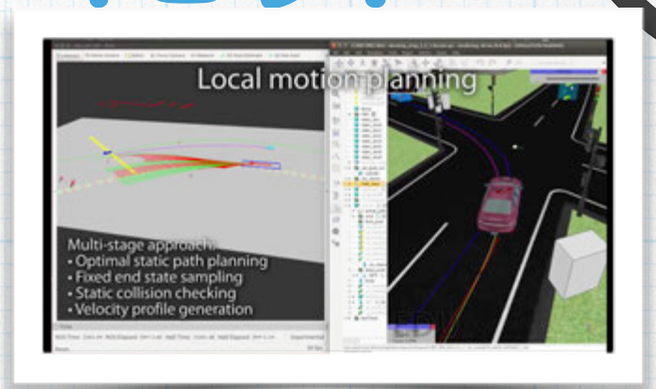
ERATO　蓮尾メタ数理システムデザインプロジェクト
ERATO Metamathematics for Systems Design Project
国立情報学研究所 & 科学技術振興機構　National Institute of Informatics & Japan Science and Technology Agency

ERATO とは

* 国立研究開発法人 科学技術振興機構（JST）の，
  戦略的創造研究推進事業プログラムの一つ
  * ERATO，CREST，さきがけ，ACT-I/ACT-X
* 規模の大きな研究費をもとに，既存の研究分野を超えた分野融合や
  新しいアプローチによって，挑戦的な基礎研究を推進
* 全ての学術分野から，毎年2-4件のプロジェクトを採択



ERATO MMSD 紹介



* JST ERATO プロジェクト
  * 2016/10-2022/03.
    総勢50名規模の基礎研究プロジェクト
* プロジェクト目標： 工業製品の設計サポート
  * 形式手法の拡張．ソフトウェアから物理情報システムへ
  * 安全性・信頼性，Verification & Validation．「システムが期待通り動作するか」
  * 特に自動運転を戦略的ターゲットに．U Waterloo と協働 www.autonomoose.net
* 研究体制
  * 国際的体制．4つのグループの1つは @ U Waterloo.
    雇用する研究員15名余のうち，外国人が半数以上
  * 先端的・包括的学術研究を実システムに応用
  * 学際的 "creative chaos" によるブレイクスルー
    * Waterloo・京大・阪大・九大のチームと協働しつつ，リソースの大部分を NII に集約
    * 多様な背景： 論理学・代数学から形式手法，制御理論，機械学習，ソフトウェア工学まで

Our Organization

International and multi-disciplinary. "creative chaos"

ERATO MMSD

Kyoto U IS Site:
Advanced Deductive Verification
Leader:
Kohei Suenaga

Kyoto U RIMS Site:
Categorical Infrastructure
Leader:
Masahito Hasegawa

Kyushu U Site:
Optimization for CPS V&V
Leader:
Hayato Waki

Osaka U Site:
Control Theory for CPS
Leader:
Toshimitsu Ushio

Group 0 @ NII:
Metatheoretical Integration
Leader: Shin-ya Katsumata

Topics:
Programming Languages, Formal Semantics, Categorical Models, Mathematical Logic, …

Group 3 @ NII:
Formal Methods and Intelligence
Leader: Fuyuki Ishikawa

Topics:
Software Engineering, Formal Modeling, Testing, Safe & Explainable AI

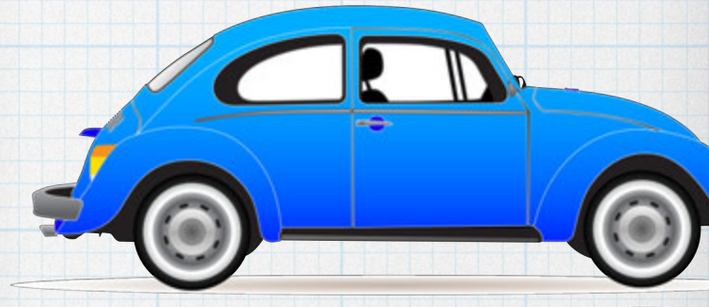
Group 1 @ NII:
Heterogeneous Formal Methods
Leader: Ichiro Hasuo
Subleader: Masako Kishida
Topics:
Automata Theory, Control Theory, Formal Verification, Proof Assistants, Automated Deduction, Runtime Verification

Group 2 @ U Waterloo:
Formal Methods in Industry
Leader: Krzysztof Czarnecki

Topics:
Automated Driving, Software Engineering, Machine Learning

ERATO MMSD: プロジェクト目標

* 数理的技法を用いた
  工業製品設計の支援



* 形式手法の拡張：
  ソフトウェアから
  物理情報システムへ

機械などの物理ダイナミクス
（連続，アナログ）
＋
計算機制御，ネットワーク
（離散，デジタル）

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

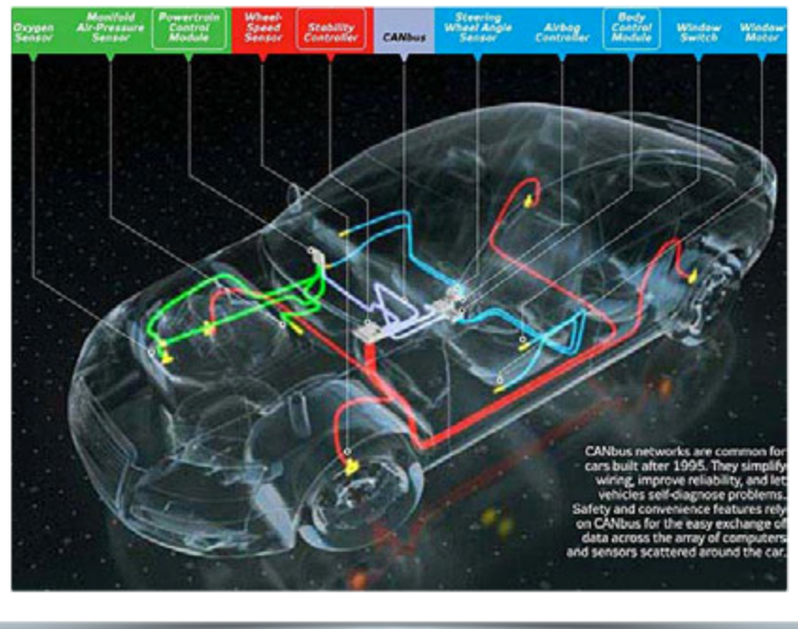
$$\begin{array}{ccc} FX & \xrightarrow{F\mathbf{beh}_c} & FZ \\ {\scriptstyle c}\uparrow & & \uparrow{\scriptstyle \text{final}} \\ X & \xrightarrow[\mathbf{beh}_c]{} & Z \end{array} \qquad \begin{array}{ccc} FX & \xrightarrow{Ff} & FY \\ {\scriptstyle c}\uparrow & \sqsupseteq & \uparrow{\scriptstyle d} \\ X & \xrightarrow[f]{} & Y \end{array}$$

system behavior　　simulation

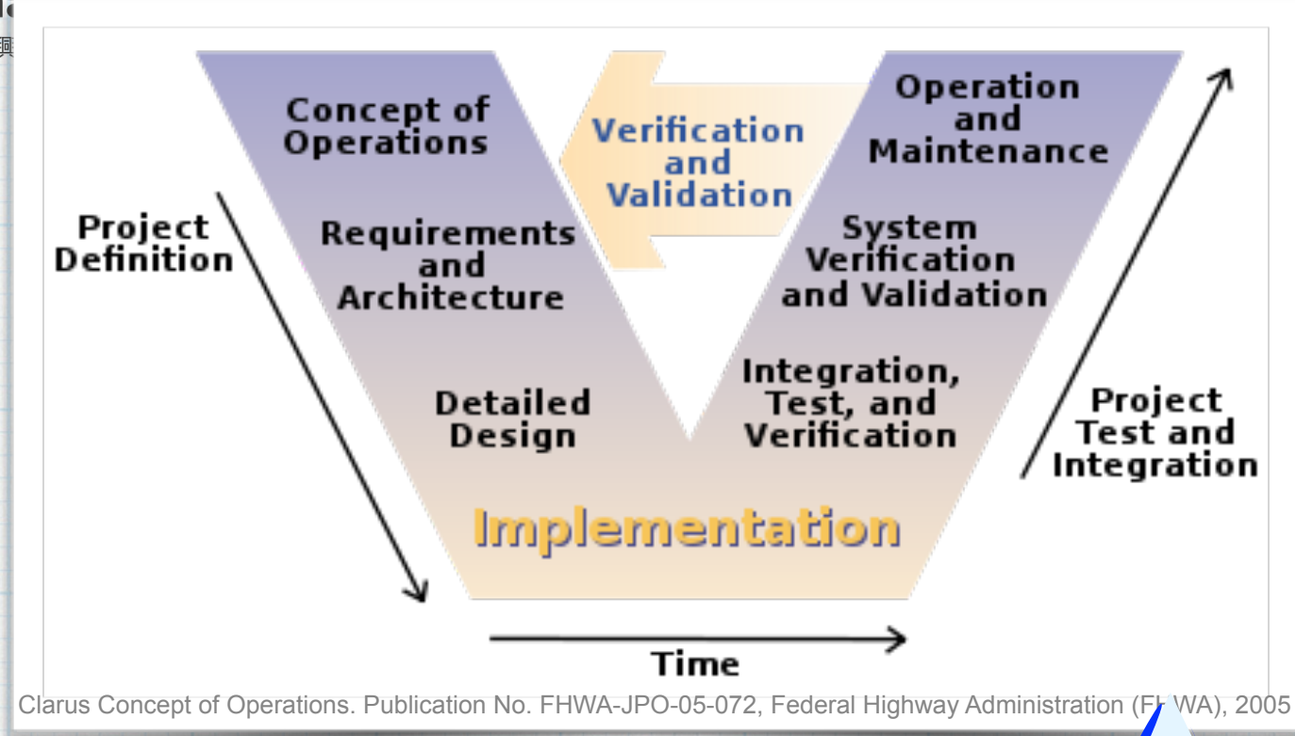
今日の製造業における挑戦

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

複雑さの爆発

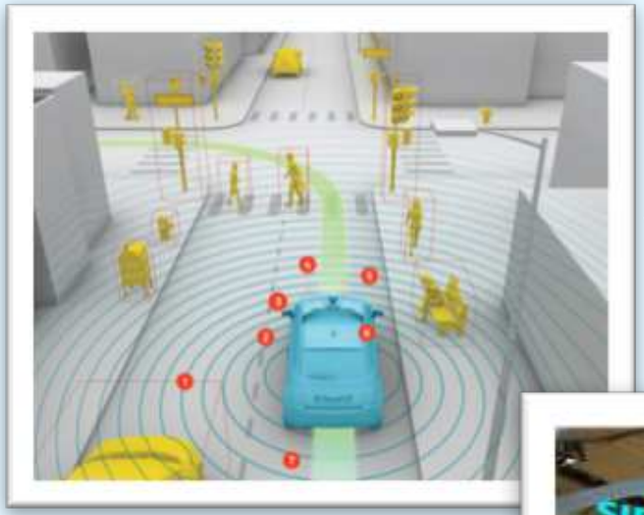


http://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/



Clarus Concept of Operations. Publication No. FHWA-JPO-05-072, Federal Highway Administration (FHWA), 2005

新たな機能・応用



自動運転

wired.com

オンデマンド生産，
“Industrie 4.0”

automotiveit.eu

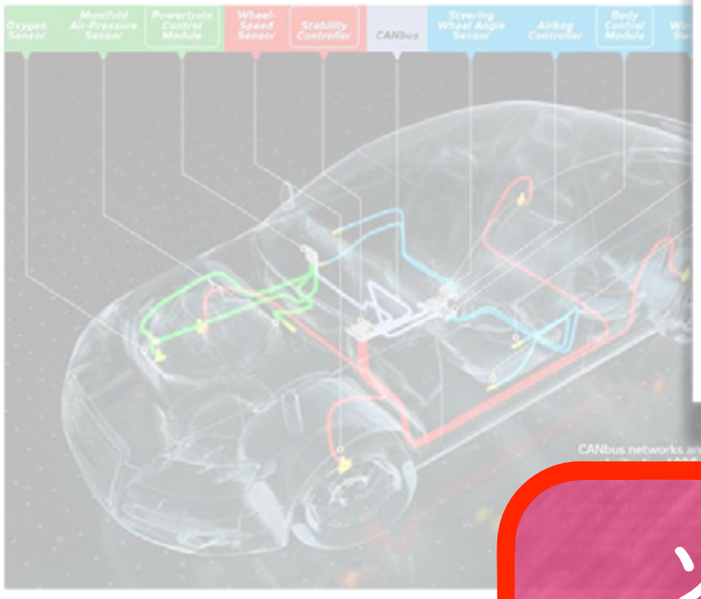
安全性保証と説明責任

* 性能・機能が飛躍的に拡大，しかし
* 工業製品の複雑さも飛躍的に拡大

現代の工業製品における
ソフトウェア制御が原因

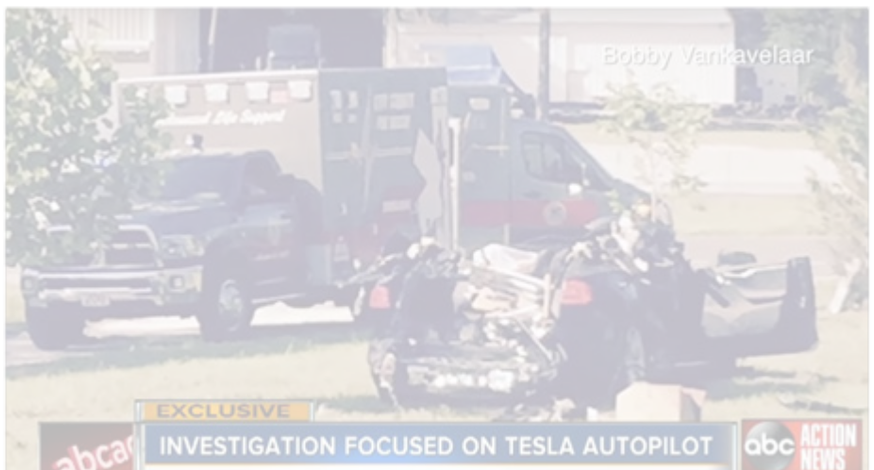
ソフトウェアの品質向上手法を援用
➜ 形式手法の活用

複雑さの爆発



http://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/

安全性保証と説明責任



新たな機能・応用

オンデマンド
生産，
“Industrie 4.0”

automotiveit.eu

アウトライン

- ERATO MMSD プロジェクト概要
- 形式手法と物理情報システム
- プロジェクトの研究開発状況
- 技術紹介
  - 形式手法・テストによるシステム品質保証手法，特に
    - サーチベーステスト
    - 実行時監視
- 今後の協働に向けて

形式手法

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

formal methods

* （もともとは）ソフトウェアの品質保証のための，数学的・記号論理的手法の総体
* 記号的であるため計算機実装が可能

計算機システムに対して多数の実績あり

* IC design (Intel, …)
* device drivers (Microsoft)
* light-weight FM (Facebook)
* …

* 形式手法の例

形式検証 verification

* **Input**:
  * a system model $\mathcal{M}$
  * a specification φ
* **Output**: if $\mathcal{M} \models \varphi$ or not
  * w/ a proof, if yes
  * w/ a counterexample, if not

自動生成 synthesis

* **Input**:
  * a specification φ
* **Output**: a system $\mathcal{M}$ such that $\mathcal{M} \models \varphi$
  * or: a parameter of a given (partial) model

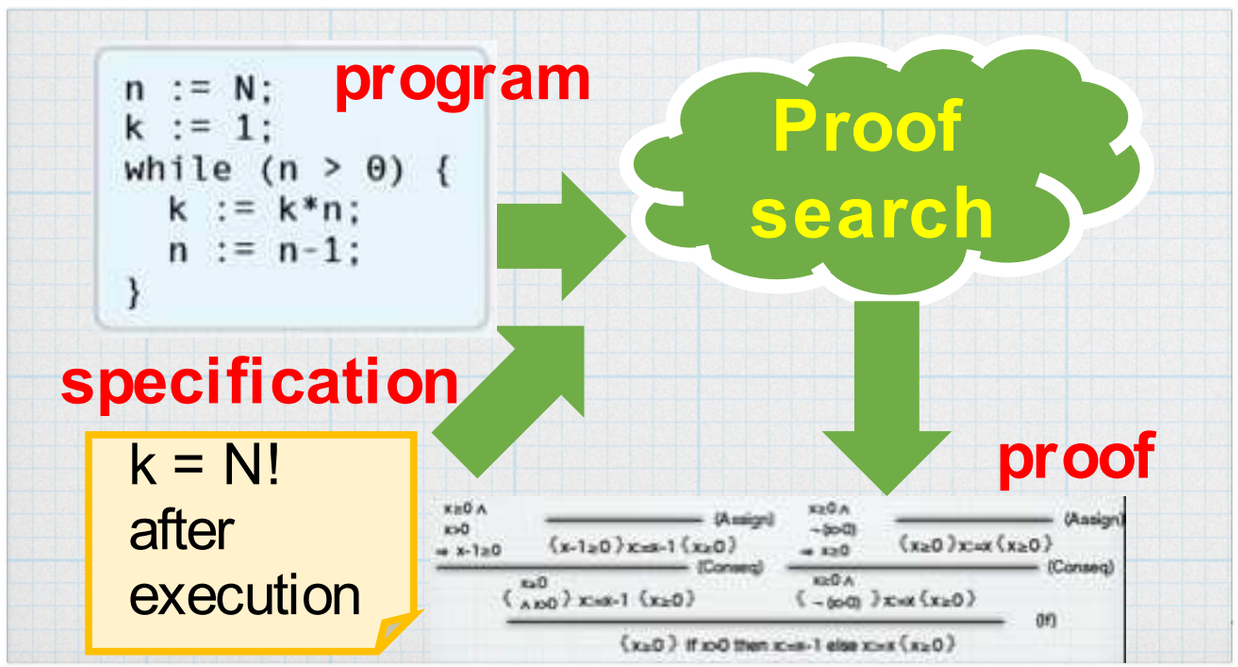
形式仕様記述 specification

Expressing a property desired in a formal language

* machine-representable
* basis for verif. & synthesis

形式検証の例１：定理証明

* 例: Hoare 論理による定理証明
  * イメージ： 紙とペンで証明を書くのと同じ
    * しかし，人力だと間違えるので，計算機上で.
      記号列で証明を表現 ➜ 各ステップの正当性をプログラム（証明支援系）がチェック
    * できれば証明の自動探索（定理証明器）
  * （原理上は）無限の入力空間をすべてカバーできる
    * 証明では「i を入力の自然数とする」とかけますね
  * 数学的証明という，強い品質保証



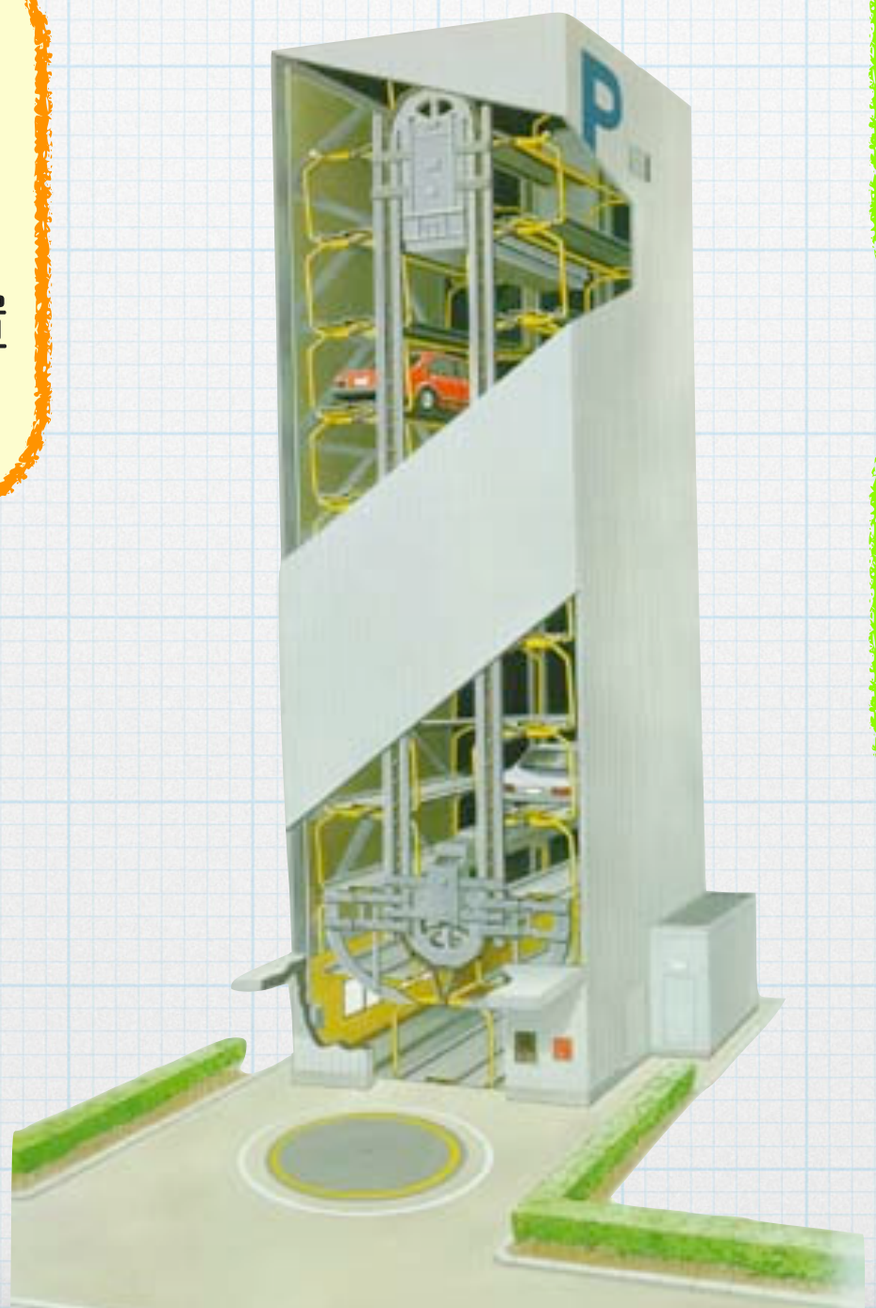

```
Theorem forall_exists : (forall P : Set->Prop,
          (forall x, ~(P x)) -> ~(exists x, P x)).
Proof.
  intros P.
  intros forall_x_not_Px.
  unfold not.
  intros exists_x_Px.
  destruct exists_x_Px as [ witness proof_of_Pwitness].
  pose (not_Pwitness := forall_x_not_Px witness).
  unfold not in not_Pwitness.
  pose (proof_of_False := not_Pwitness proof_of_Pwitness).
  case proof_of_False.
Qed.
```

A Coq proof of ∀x. ¬P(x) → ¬ ∃x. P(x)

ビジネスでの証明

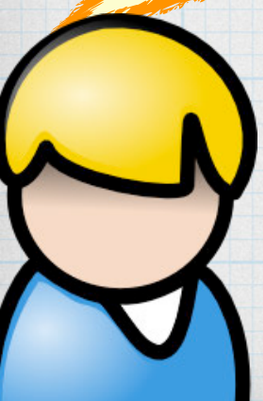
はい，大丈夫です．
なぜなら，任意の状態 s に対して，ゴンドラ g_1 の位置を x_1 とすると，．．．

この駐車場，
どうでしょう．



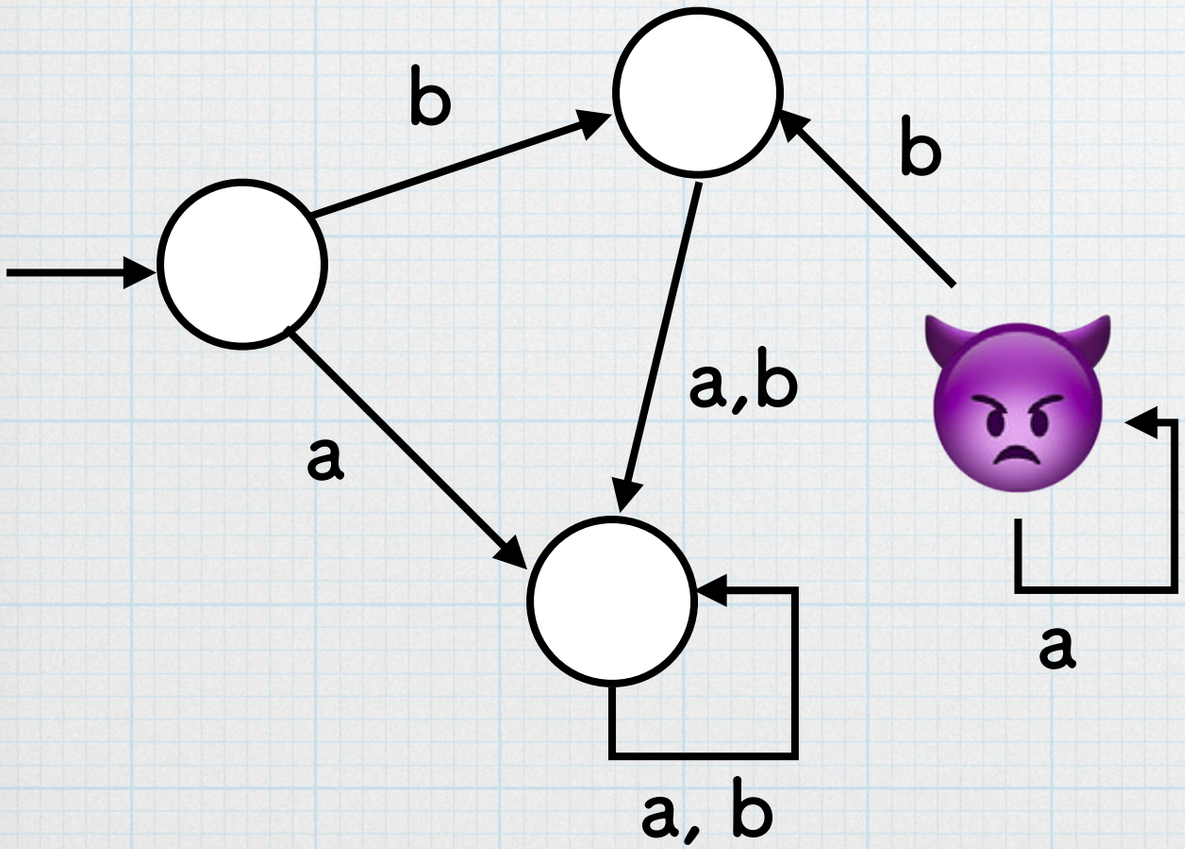
．．．（読んでる）
なるほど．それでは1基いただこう．

ゴンドラが衝突したりしない？ 大丈夫？



形式検証の例２： モデル検査

* オートマトンのアルゴリズムによる「自動証明」
  * 主にグラフの到達可能性判定に帰着
* オートマトンは有限 ➜ 数え上げによる自動証明が可能
* 例： 以下のオートマトンにて，😈 に至ることはない (*)



* （不正解）
  仕様 (*) をすべての入力について確かめる
  （入力は無限個あるので無理）
* （正解）
  到達可能な領域を計算し（グラフ探索，有限時間で飽和），😈 が含まれないことを確かめる

形式手法の歴史（超ダイジェスト）

ソフトウェアの大規模化

ネットワーク，分散並列

物理システムとの融合

統計的機械学習の能力向上

* 1970頃 形式手法によるソフトウェア品質保証（ソフトウェア検証）の研究開始．定理証明，モデル検査

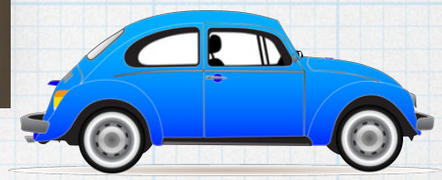
* 1990頃 ソフトウェア検証のツール化・実応用加速
  定理証明： Isabelle, Coq, PVS, …
  モデル検査： SPIN, SMV/NuSMV, mCRL2, PRISM, Uppaal, …

* 2006 物理情報システム (Cyber-Physical Systems, CPS) への応用開始．ソフトウェア検証 + 制御理論
  （この経緯は［奥村，研究 技術 計画 2017］に詳しい）

* 2016 機械学習システムへの応用．
  形式的推論と統計的推論

これまでの物理情報システム研究

（特に安全性・信頼性の側面）



物理情報システム
（特に hybrid system）

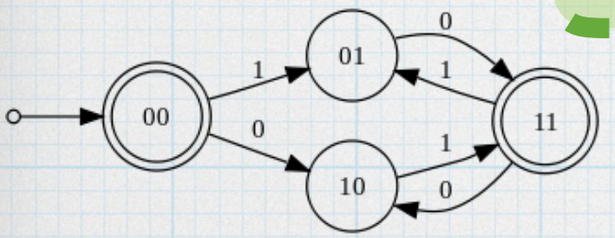
解析

形式手法

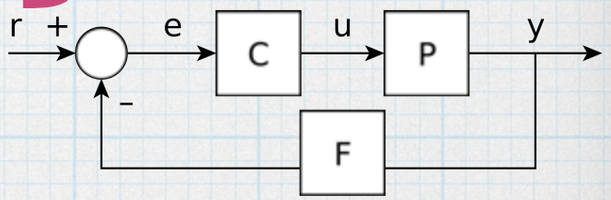
協働

制御理論

$\Box(p \Rightarrow \Diamond q)$



$x' = f(x, u)$

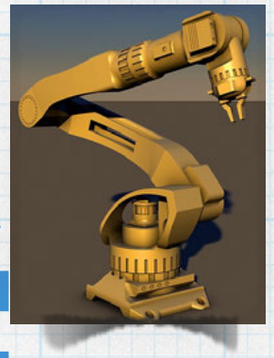


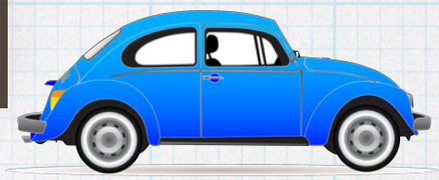
追いつかなければ…??

- 物理情報システム研究への取り組みでは欧米が先行
  - 米国： NSF の CPS 研究イニシアチブ (2006-)
  - 欧州： 形式手法の定量的拡張（確率，時間，…）

これまでの物理情報システム研究

（特に安全性・信頼性の側面）



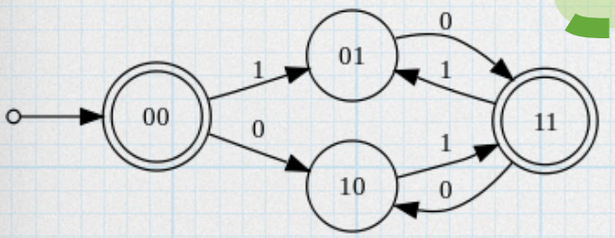


物理情報システム
（特に hybrid system）

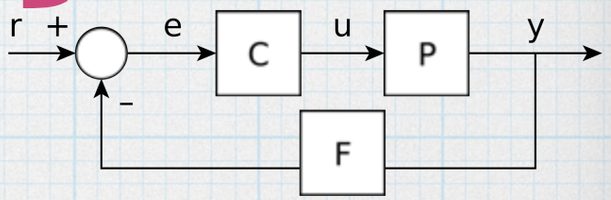
解析

形式手法 ⟷ 協働 ⟷ 制御理論

$\Box(p \Rightarrow \Diamond q)$



$x' = f(x, u)$



- 課題： 実システムに対するスケーラビリティ
  - ホワイトボックスモデルの完全な理解が前提
  - 結論の数学的正しさを絶対視
  - 不確かさを許容する余地が少ない ➜ 統計的機械学習との相性の問題

可能？
役に立つ？

ERATO MMSD の研究開発の目標：
これらの柔軟なミックス ➜ 実システムへ応用

ソフトウェア品質保証におけるスペクトル

形式手法

テスト test | モデル検査 | 自動定理証明 | 対話定理証明

低 コスト 高

ブラックボックス モデルを許容

ホワイトボックスモデルを要求

高 自動化の度合い 低

自動

専門家を月・年単位で拘束

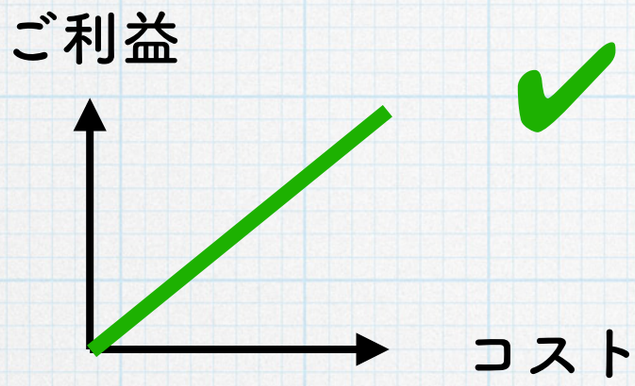
低 保証の網羅性 高

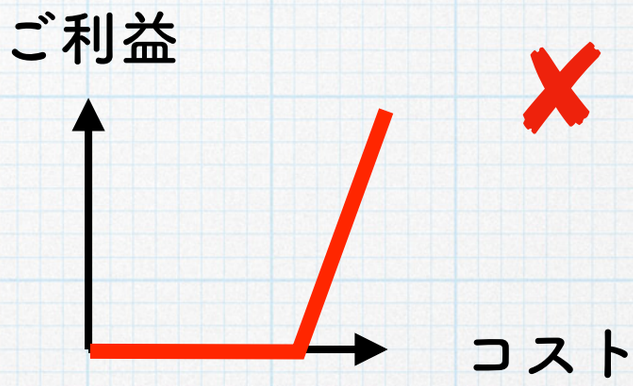
低 保証の数学的厳密性 高

経験論的保証

数学的保証 ➜ 「形式検証」

スケールダウンできる形式手法





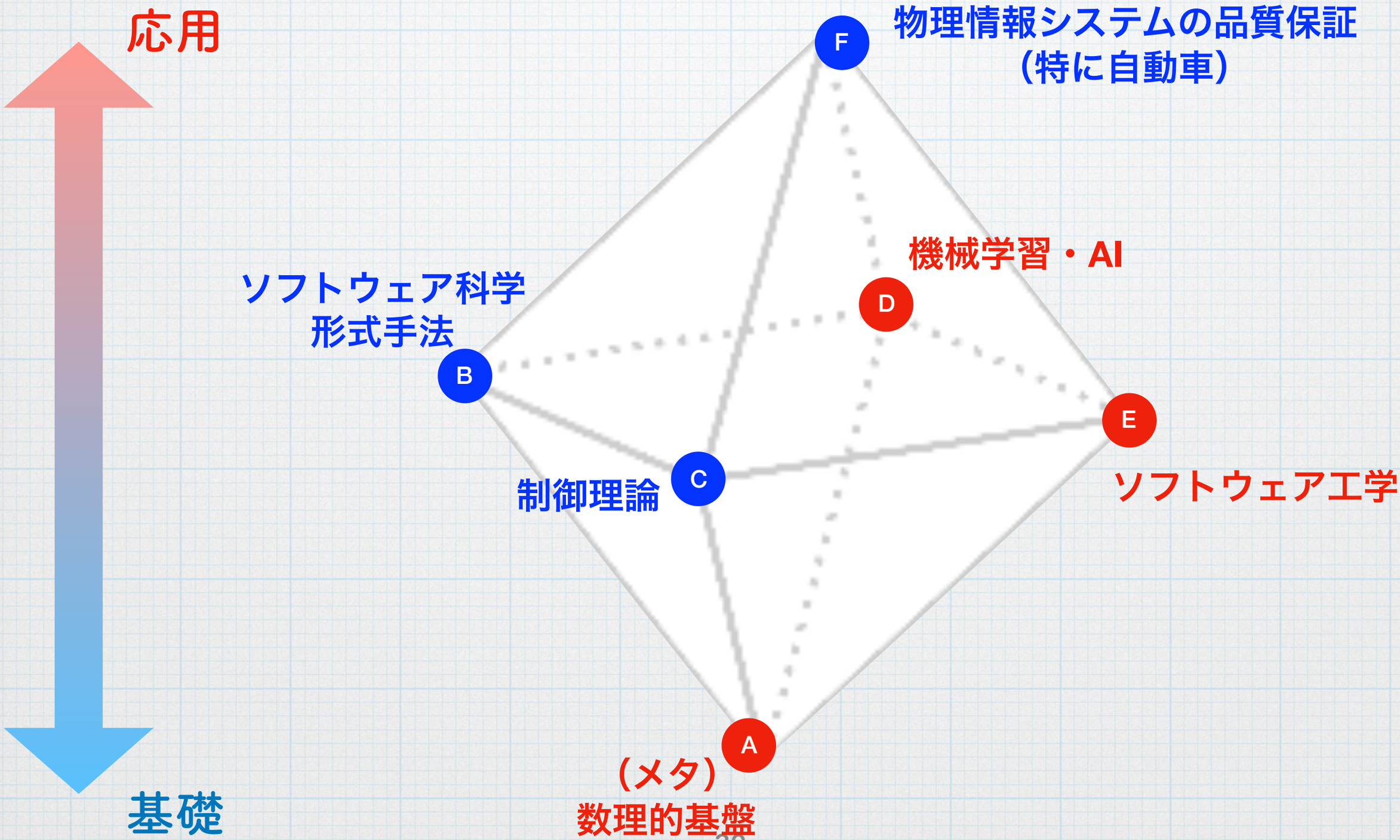
* 形式手法の多くはスケールダウンできない
  * ホワイトボックスモデルを要求.
    全てのコンポーネントの形式モデル
  * ホワイトボックスモデルがないと何もできない ➜ ご利益 0
  * 「まずホワイトボックスモデルを書いてください．話はそれからだ」

* ERATO MMSD の目指すところ
  * テストも組み合わせた，柔軟なソリューションを提案
  * 応用シナリオ・リソースに合わせた品質保証

アウトライン

- ERATO MMSD プロジェクト概要
- 形式手法と物理情報システム
- プロジェクトの研究開発状況
- 技術紹介
  - 形式手法・テストによるシステム品質保証手法，特に
    - サーチベーステスト
    - 実行時監視
- 今後の協働に向けて

物理情報システムのための分野横断： ERATO MMSDの場合



研究体制

* G0： メタ理論的統合グループ
（勝股）
論理学，代数学，圏論，
プログラミング言語理論，…

* G1： ヘテロジニアス
形式手法グループ（蓮尾・岸田）
ソフトウェア科学，
制御理論，形式手法，モデル検査，
自動定理証明，…

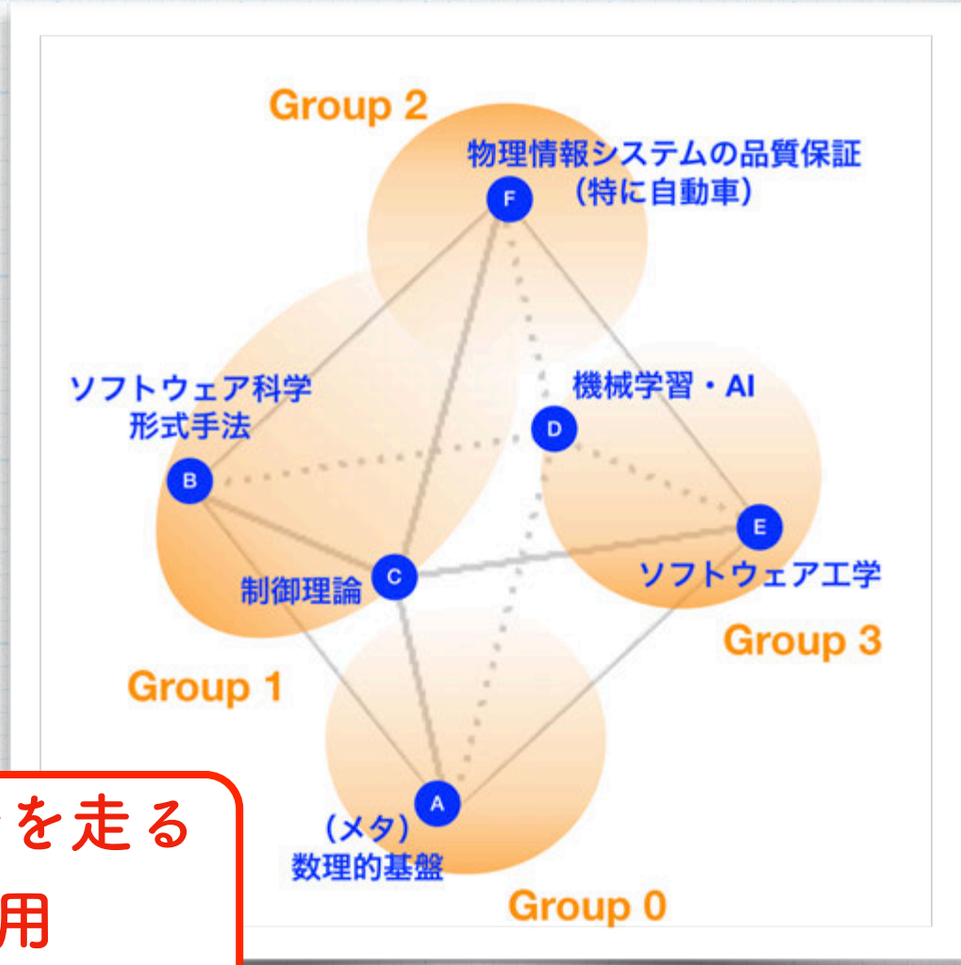
* G2： 産業応用グループ(Czarnecki)
自動運転システム

* G3： インテリジェンス協働
形式手法グループ（石川）
ソフトウェア工学，テスト，モデリング，要求工学，…

学術研究の進捗状況

* グループ間の協働の進展
  * 新たな応用が導く理論発展
    * 実行時監視
    * 深層学習のための圏論的理論
  * 機械学習利用 ➔ 効率的テスト
  * 数理的基盤(G0)の重要性
    * 学術的＆人的
  * 国際的 visibility:
    * いわゆる「トップ国際会議」(CORE rank A, A*) 論文 > 30 報
    * 最優秀論文賞： ICECCS'18, FoSSaCS'19（共にCORE rank A）
    * 理論計算機科学の最高峰国際会議 LICS'19（CORE rank A*）では，全採択数 60 報のうち 6 報でERATO MMSD 研究者が（共）著者

学術研究で世界的先端を走るからこそ可能な産業応用



応用上の進捗状況

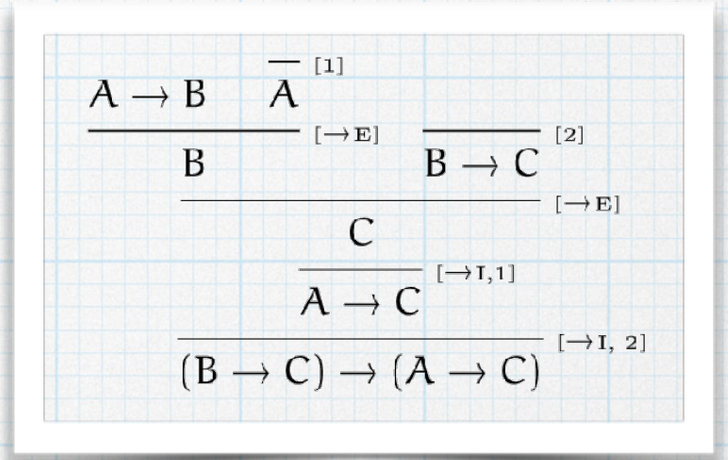
* プロトタイプツール多数
  * 実行時監視ツール
    * MONAA [Waga+, FORMATS'17] https://github.com/maswag/monaa
    * SyMon [Waga+, CAV'19] https://github.com/MasWag/symon
  * サーチベーステストツール
    * FalStar [Zhang+, EMSOFT'18] https://github.com/eratommsd/falstar
  * その他：確率的プログラム自動検証ツール，RNN2WFA ツール（recurrent neural network を重み付きオートマトンに近似），...

* U Waterloo の自動運転プロジェクト autonomoose と協働，
  形式手法の応用に向けて，具体的トピックについて研究推進中

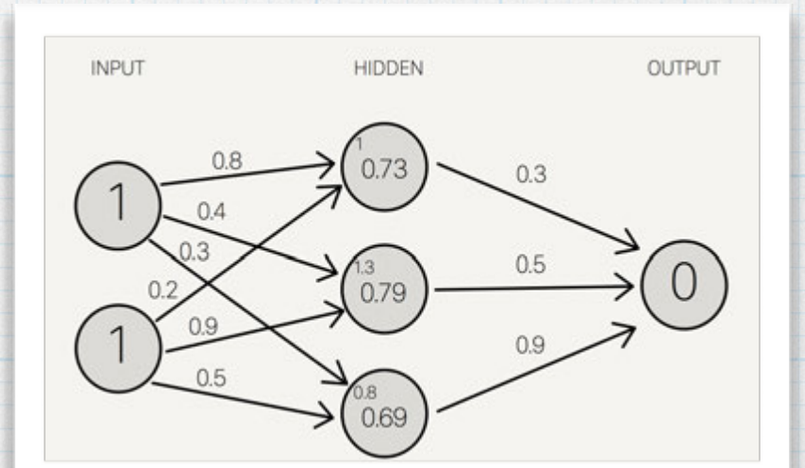
* 国内の企業10社弱と共同研究・学術指導・定期的議論
  （自動車メーカー，自動車部品メーカー，総合電機メーカー，
  ソフトウェアベンダーなど）

ところで：AI 研究の歴史（超ダイジェスト）

* 1980-1987「論理的人工知能，エキスパートシステム」
  * 与えられたルールによる論理的推論
    * 判断の過程が明らかにトレースできる
    * 「与えられたルール」の準備が大変
      （人力ではおそらく不可能）
  * Prolog, 第５世代コンピュータ
  * 関連する数学分野： 論理学，数学基礎論



* 2011-現在「統計的機械学習」
  * 大量のデータから自動で統計的に特徴量抽出
    * 驚くべきスケーラビリティ．
      画像処理，物体認識，自動翻訳，…
    * 判断の過程はブラックボックス
  * ディープニューラルネットワーク
  * 関連する数学分野： 統計学，最適化

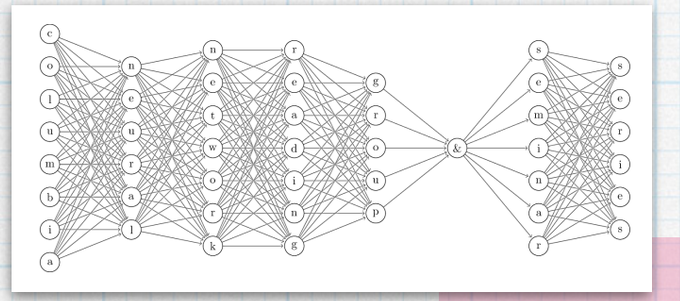


ERATO MMSD の研究開発の目標：
両者を組み合わせた高信頼物理情報システム

理システムデザインプロジェクト
tics for Systems Design Project
onal Institute of Informatics & Japan Science and Technology Agency

ERATO MMSD

統計的機械学習 vs 演繹的形式推論



$$\frac{A \quad A \supset B}{B}$$

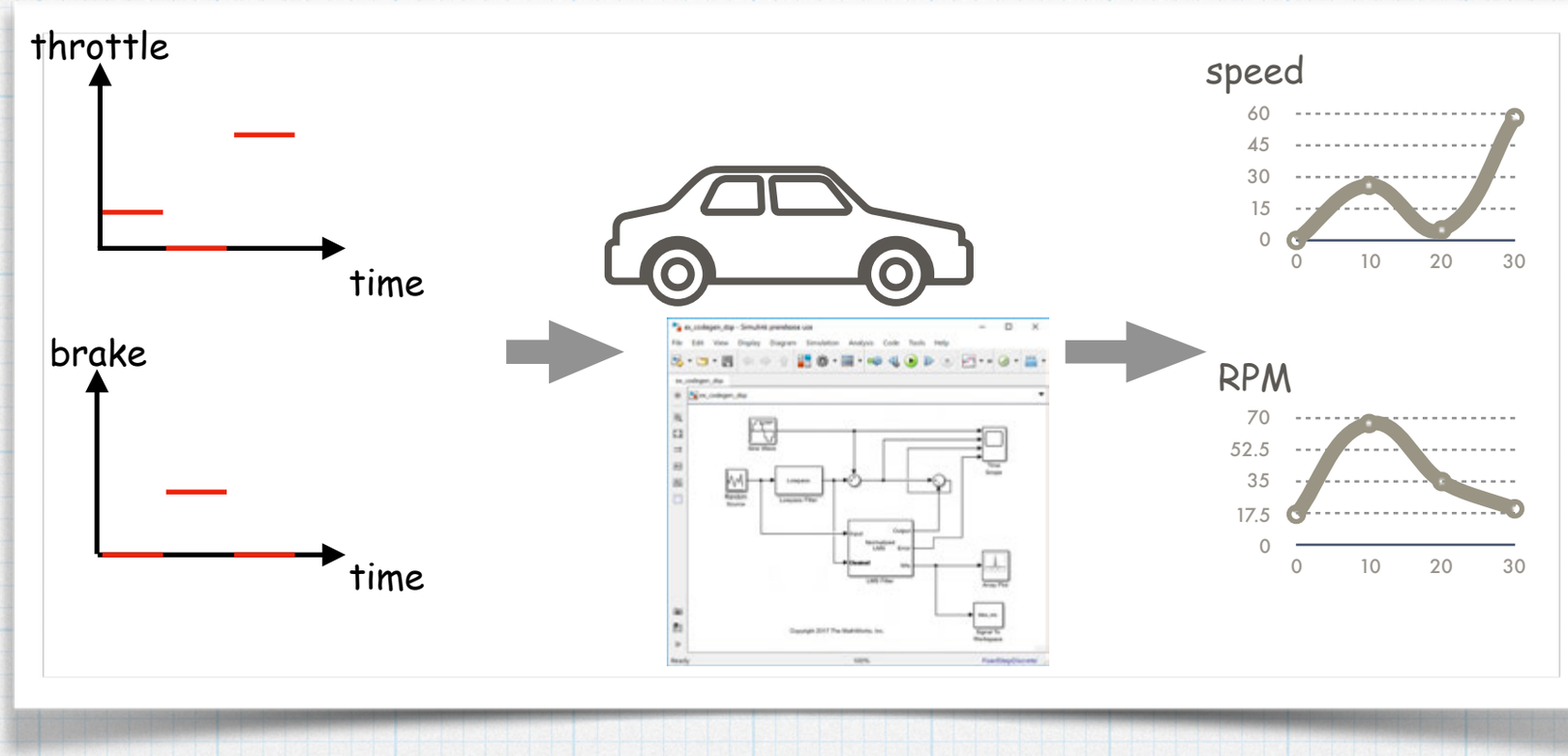
統計的機械学習		演繹的形式推論
データのノイズを許容	入力の誤り	公理は絶対誤りは想定せず
保証されない	結論の正しさ	論理的に保証（cf. 数学的証明）
高い データから自動で特徴量発見	スケーラビリティ	低い 公理の準備は人力 （cf. エキスパートシステム）
低い 判断の理由はパラメータ（重み）	説明可能性	高い 推論過程が証明として明示的

アウトライン

- ERATO MMSD プロジェクト概要
- 形式手法と物理情報システム
- プロジェクトの研究開発状況
- 技術紹介
  - 形式手法・テストによるシステム品質保証手法，特に
    - サーチベーステスト
    - 実行時監視
- 今後の協働に向けて

強化学習によるサーチベーステスト：Simulink モデルの反例生成

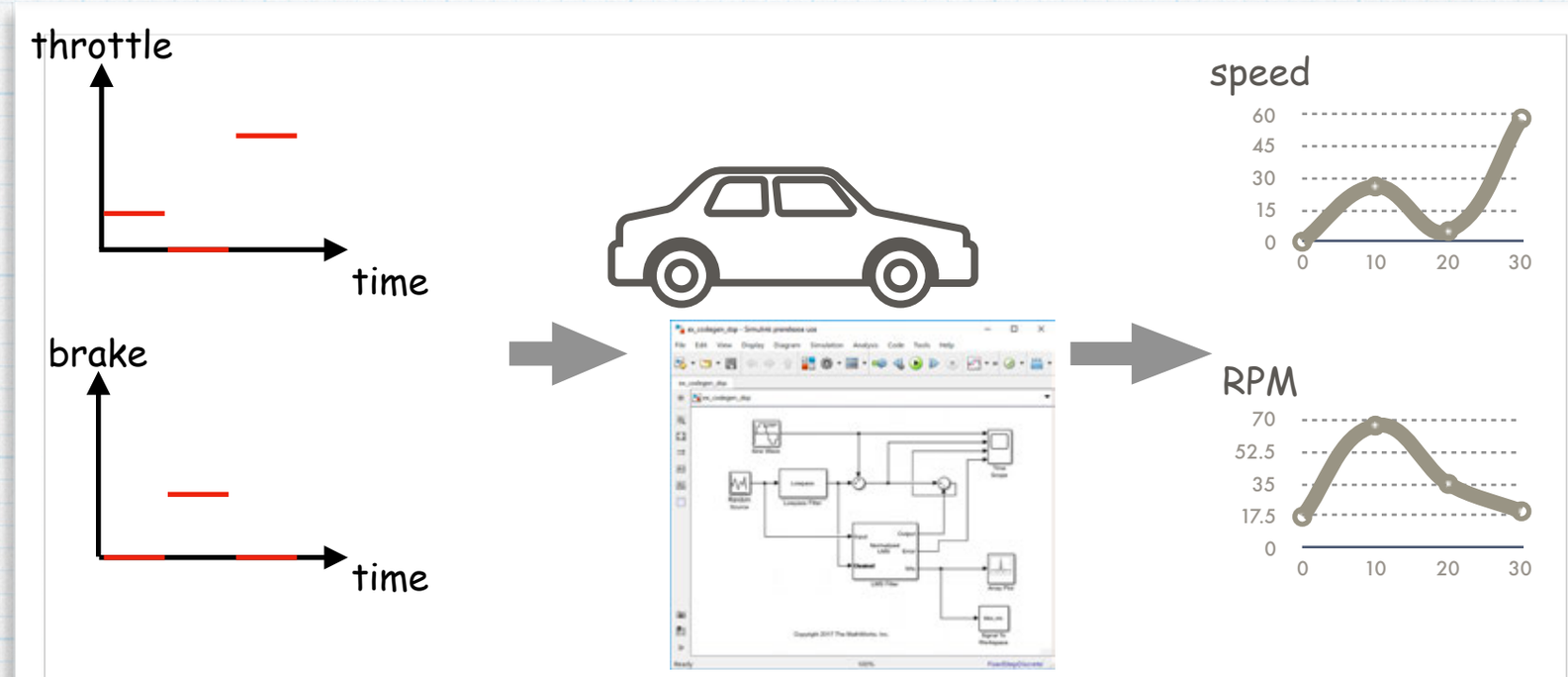
[Akazaki & Hasuo, CAV'15]
[Zhang, Ernst, Sedwards, Arcaini & Hasuo, EMSOFT'18]
[Zhang, Hasuo & Arcaini, CAV'19] …



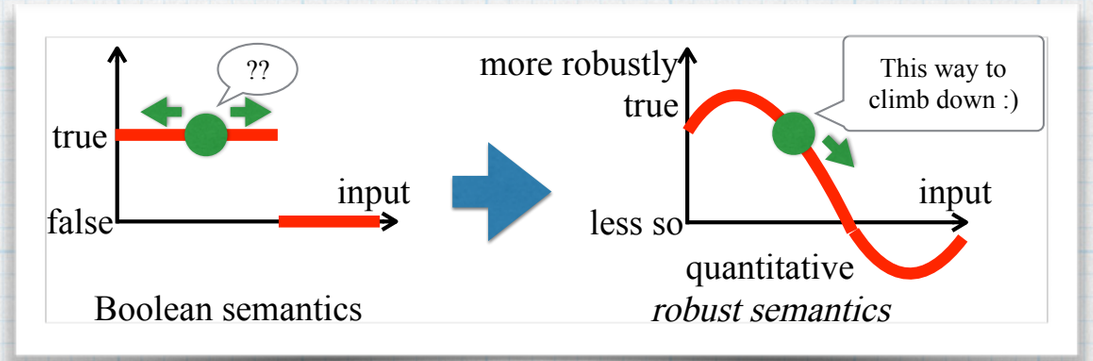
* ブラックボックステスト.
  入出力の対応を見ながら，反例となる入力シグナルを探索
  * Given: Simulink モデル M, 時相論理仕様 ϕ
    * 仕様 ϕ の例：
      ギヤが4速になったらそれから3秒以内に時速 50 km/h 以上になる
  * 目標：
    出力シグナル M(i) が ϕ を
    みたさないような，入力シグナル i

強化学習によるサーチベーステスト：Simulink モデルの反例生成

[Akazaki & Hasuo, CAV'15]
[Zhang, Ernst, Sedwards, Arcaini & Hasuo, EMSOFT'18]
[Zhang, Hasuo & Arcaini, CAV'19] …



* 主流のアプローチ [Fainekos & Pappas, TCS'09]：
  * 強化学習，確率的最適化で「あぶないところ」を狙う
  * そのため，時相論理式 ϕ の真偽値を，ブール値（2値）から連続実数値に拡張 ➜ 勾配降下法



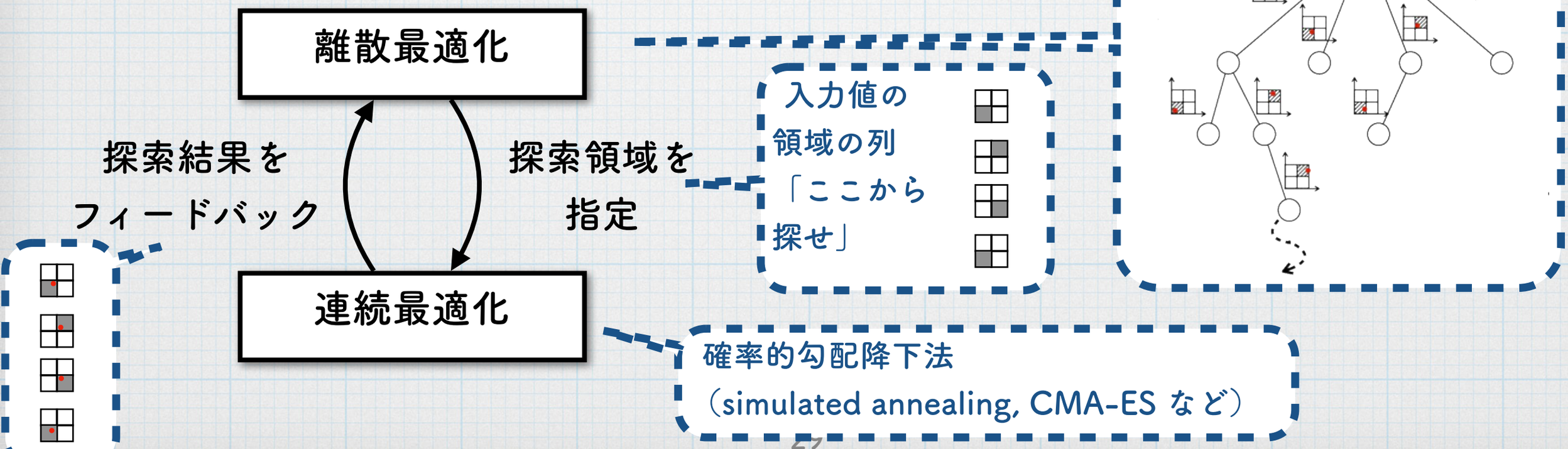
強化学習によるサーチベーステスト：Simulink モデルの反例生成

[Akazaki & Hasuo, CAV'15]
[Zhang, Ernst, Sedwards, Arcaini & Hasuo, EMSOFT'18]
[Zhang, Hasuo & Arcaini, CAV'19] …

* Survey: [Kapinski+, IEEE Control Syst. '16]

  J. Kapinski, J. V. Deshmukh, X. Jin, H. Ito, and K. Butts, "Simulation-based approaches for verification of embedded control systems: An overview of traditional and advanced modeling, testing, and verification techniques," IEEE Control Syst., vol. 36, no. 6, pp. 45–64, Dec. 2016.

* ERATO MMSD の貢献 [Zhang+, EMSOFT'18] を例に． [Zhang+, CAV'19] も同種のアイデア
  * 確率的勾配降下法における離散構造の利用，
    これによる反例発見能力の向上
  * 階層的最適化アーキテクチャ



実行時監視：さまざまな定式化

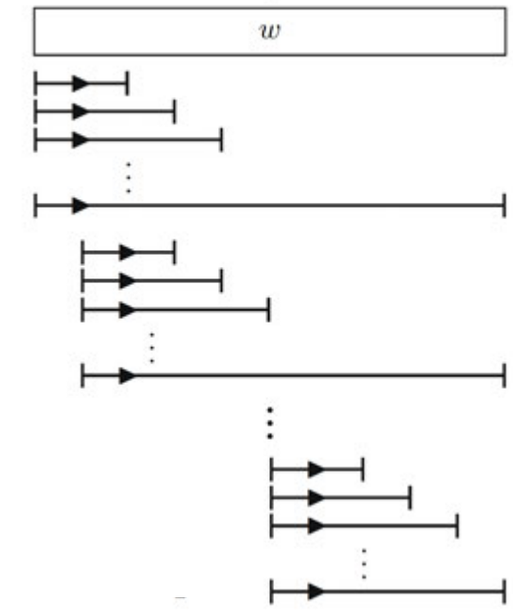
* Given: 離散時間ログ w = abaaacb…bbc
  仕様 ϕ 「b の後，6 step 待っても c が現れず」
  Answer: w の部分列で ϕ を満たすもの全体

* Given: 連続時間ログ w = (a, 0.12) (b, 1.28) …
  仕様 ϕ 「b の後，6 秒待っても c が現れず」
  Answer: w の部分列で ϕ を満たすもの全体

[Ulus, CAV'17] [Waga+, FORMATS'17] など

解は無限個
（開始時刻は t=1? t = 1.01? t = 1.001? …）
➔ 時間付きオートマトンの zone 構成で，効率的に表現・計算可能

時間的因果関係があり，そう簡単ではない



* Given: 連続時間ログ w = (a, 0.12) (b, 1.28) …
  パラメータ付き仕様 $\phi(p)$ 「b の後，p 秒待っても c が現れず」「a は概ね p 秒周期で現れる」
  Answer: (p, {w の部分列で $\phi(p)$ を満たすもの}) のペア全体

[Waga+, ICECCS'18] [Waga+, NFM'19] [Waga+, CAV'19] など

実行時監視： ERATO MMSD の取り組み

* Given: 離散時間ログ w = abaaacb…bbc
  仕様 ϕ 「b の後，6 step 待っても c が現れず」
  Answer: w の部分列で ϕ を満たすもの全体

* Given: 連続時間ログ w = (a, 0.12) (b, 1.28) …
  仕様 ϕ 「b の後，6 秒待っても c が現れず」
  Answer: w の部分列で ϕ を満たすもの全体
  [Ulus, CAV'17] [Waga+, FORMATS'17] など

時間付きオートマトンの理論による高速アルゴリズム．ラップトップで毎秒，数M の長さのログを処理
[Waga+, FORMATS'17]
https://github.com/maswag/monaa
ルネサス RH850 実装もあり

パラメータ・時間付きオートマトンの理論による高速アルゴリズム．ラップトップで毎秒，数十 K の長さのログを処理
[Waga+, NFM'19]
https://github.com/maswag/symon

* Given: 連続時間ログ w = (a, 0.12) (b, 1.28) …
  パラメータ付き仕様 $\phi(p)$ 「b の後，p 秒待っても c が現れず」「a は概ね p 秒周期で現れる」
  Answer: (p, {w の部分列で $\phi(p)$ を満たすもの}) のペア全体
  [Waga+, ICECCS'18] [Waga+, NFM'19] [Waga+, CAV'19]など

アウトライン

- ERATO MMSD プロジェクト概要
- 形式手法と物理情報システム
- プロジェクトの研究開発状況
- 技術紹介
  - 形式手法・テストによるシステム品質保証手法，特に
    - サーチベーステスト
    - 実行時監視
- 今後の協働に向けて

産学協働に向けて

* 学術研究と産業応用は，研究推進の車の両輪．本気で取り組んでいます．スパイラル

* いくつかのツールを公開しています
  * 研究レベルのプロトタイプですが，ニーズに合わせて改良・適合が可能
  * 論文リストから辿っていただけます

* 個別の共同研究・学術指導
  * 具体的な課題を持ち込んでいただくと，話が早いです．
    プロジェクトの持てる手法を総動員して解きます

* 自動運転をテーマにした研究会を組織する予定です（企業の方対象，今年度上半期）
  * 定期セミナーで技術紹介，情報共有
  * 先日のシンポジウム「高信頼自動運転システムのための先進的研究
    ――数理的理論から，AI 協働，ソフトウェアプラットフォームへ」をきっかけに
    （ビデオ・スライド公開中）

くわしくは，ERATO MMSD プロジェクトウェブページまで！
https://group-mmm.org/eratommsd （「erato mmsd」で検索）