ERATO MMSDプロジェクト紹介

物理情報システム品質保証のための包括的学術研究

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

趣旨説明

ERATO MMSD:
主にソフトウェア的視点から，物理情報システムの
信頼性保証手法を研究する学術プロジェクト

* ERATO 蓮尾メタ数理システムデザインプロジェクト 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」

高信頼自動運転システム:
昨今の大きな経済的・社会的要請.
ERATO MMSD の戦略的応用目標

* 数多くの学術分野を包括する学術研究
* 実世界の具体的応用に牽引される形で推進

趣旨説明

* ERATO 蓮尾メタ数理システムデザインプロジェクト 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」

* 以下を展望します：
  * 国内外の研究動向
  * ERATO MMSDで開発している V&V 技術，及び学術的取り組み
  * 「今日」「明日」のみならず「明後日」まで

* 本シンポジウムをきっかけとして，今後皆様と情報を共有させていただきながら，当該分野の振興に貢献を行っていきたく思います

アウトライン

- 本日の趣旨
- 研究開発の背景
- ERATO MMSD 紹介
  - プロジェクト体制
  - 学術的研究の現状
  - 実応用に向けた研究開発の現状
- 世界の同種の取り組みとの比較
- プロジェクトの今後のビジョン

背景（形式手法中心史観です）

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

形式手法 formal methods

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

* （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

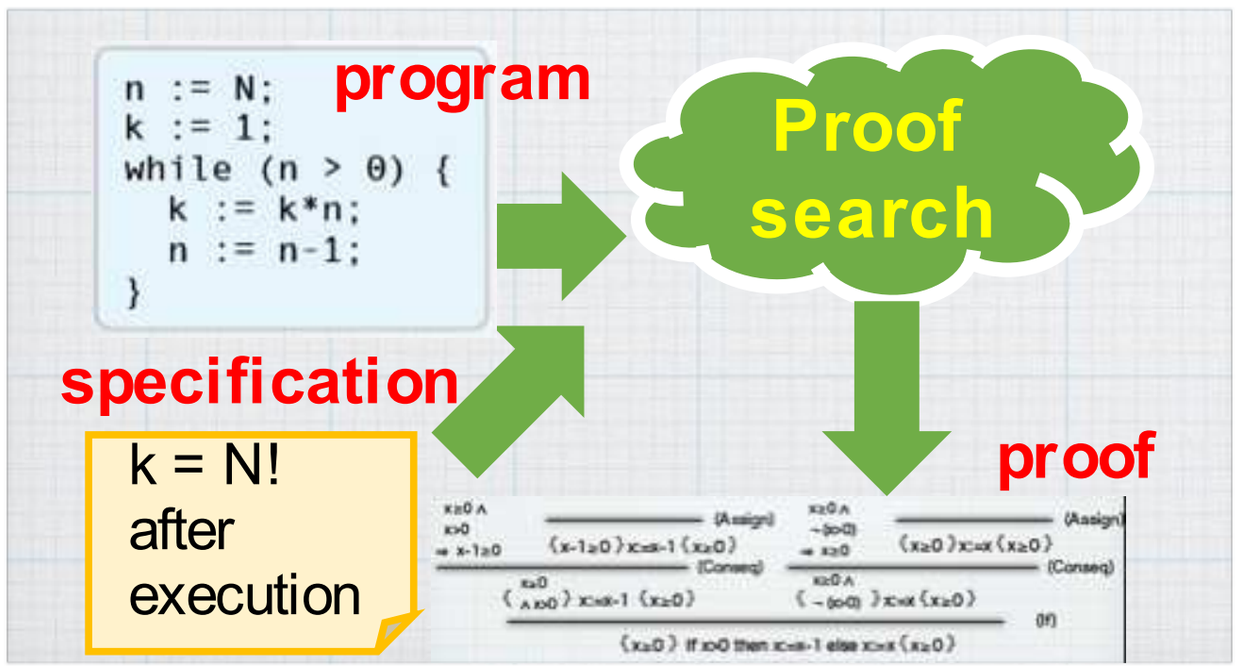
形式仕様記述 specification

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

* Example: program verification by Hoare logic
  * Proof search can be automatic or interactive
    (proof assistants like Coq, Agda, PVS, Isabelle, …)
  * A mathematical proof guarantees correctness
    * Unlike testing (empirical guarantee)
* Can cover infinitely many inputs/environments (in principle)
  * Write “let ***i*** be the input” in the proof!

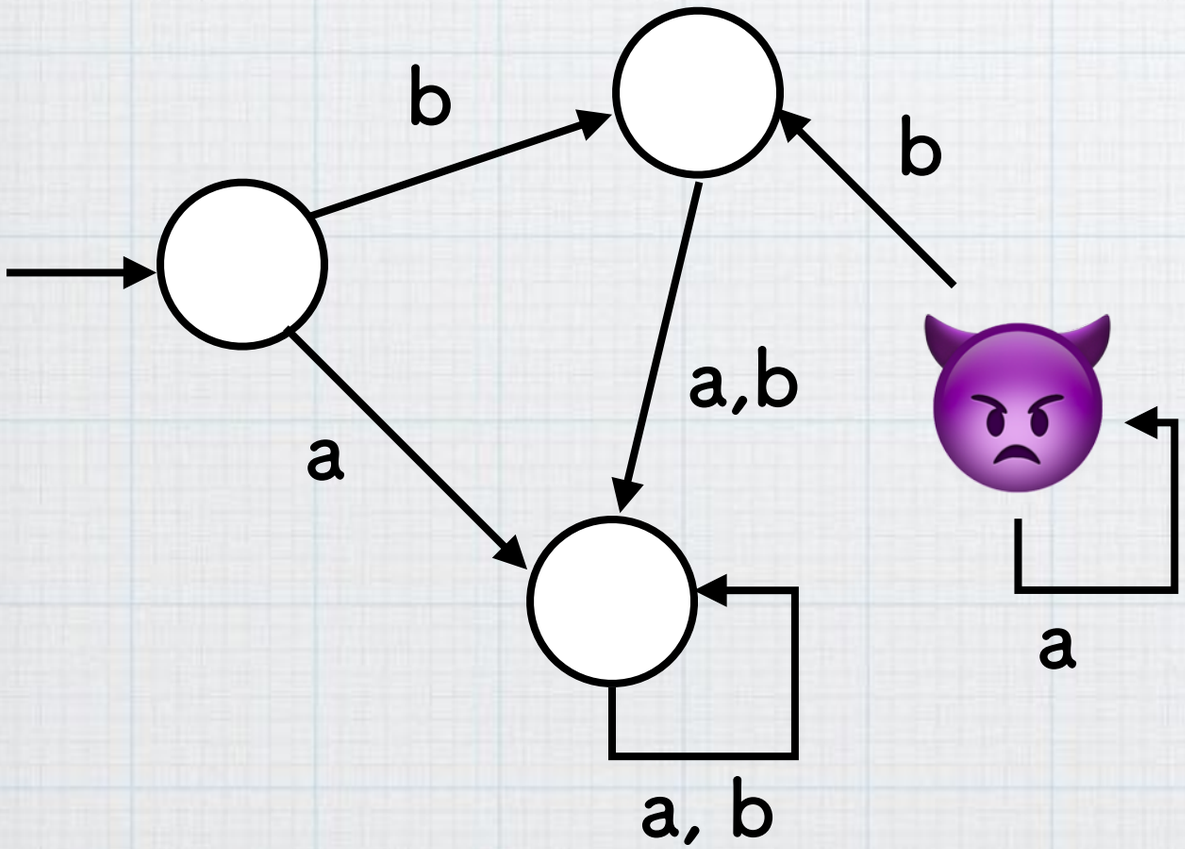



```
Theorem forall_exists : (forall P : Set->Prop,
          (forall x, ~(P x)) -> ~(exists x, P x)).
Proof.
  intros P.
  intros forall_x_not_Px.
  unfold not.
  intros exists_x_Px.
  destruct exists_x_Px as [ witness proof_of_Pwitness].
  pose (not_Pwitness := forall_x_not_Px witness).
  unfold not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

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 (*)



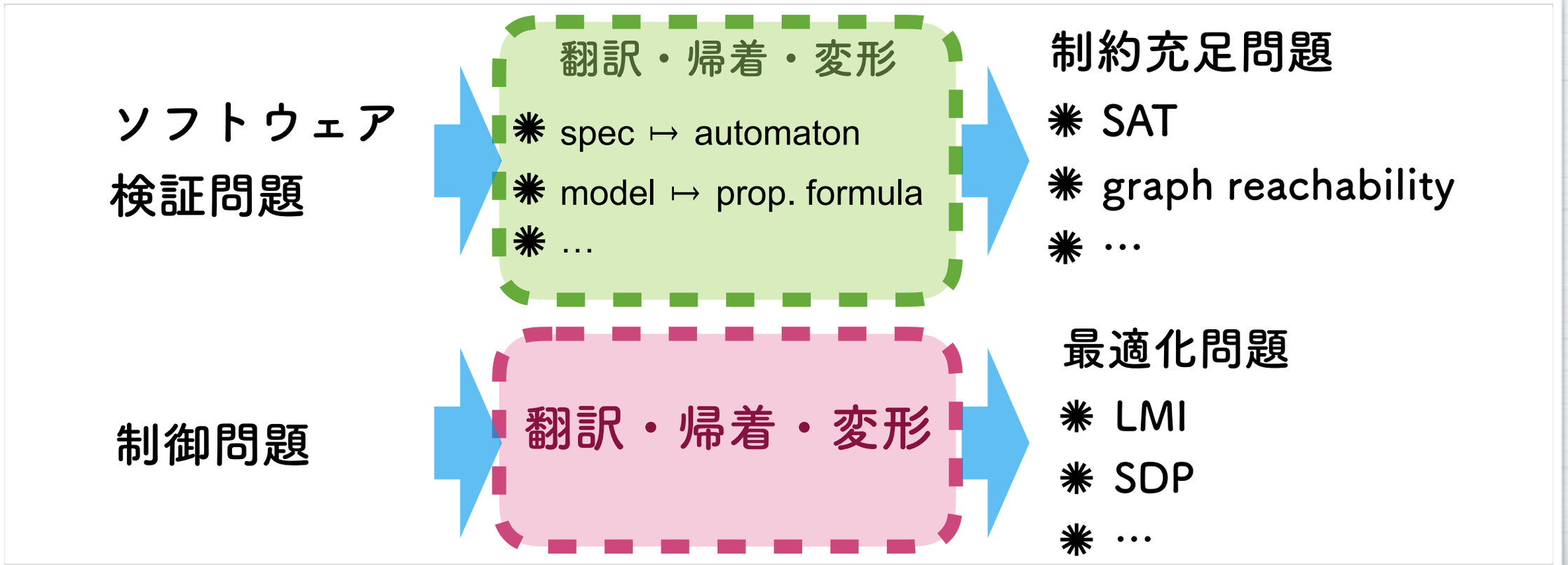
* （不正解）
  仕様 (*) をすべての入力について確かめる（無限個ある）
* （正解）
  到達可能な領域を計算し（グラフ探索，有限時間で飽和），😈が含まれないことを確かめる

制御理論 と 形式手法・ソフトウェア科学

* 対比

制御理論		形式手法・ソフトウェア科学
連続空間・連続時間	対象システム	離散空間・離散時間
微分方程式	モデリング	オートマトン，プログラム
連続量最適化 LMI, SDP, …	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

* しかしワークフローは共通．「ダイナミクスを解きほぐす」



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）

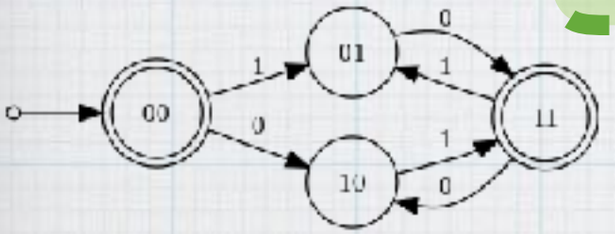
物理情報システム
（特に hybrid system）

解析

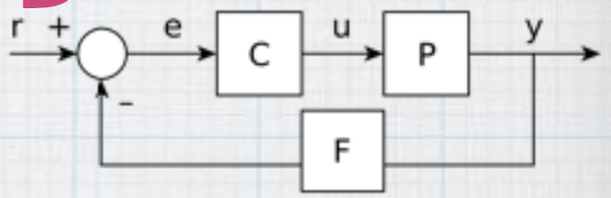
形式手法 ⇔ 制御理論

協働

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



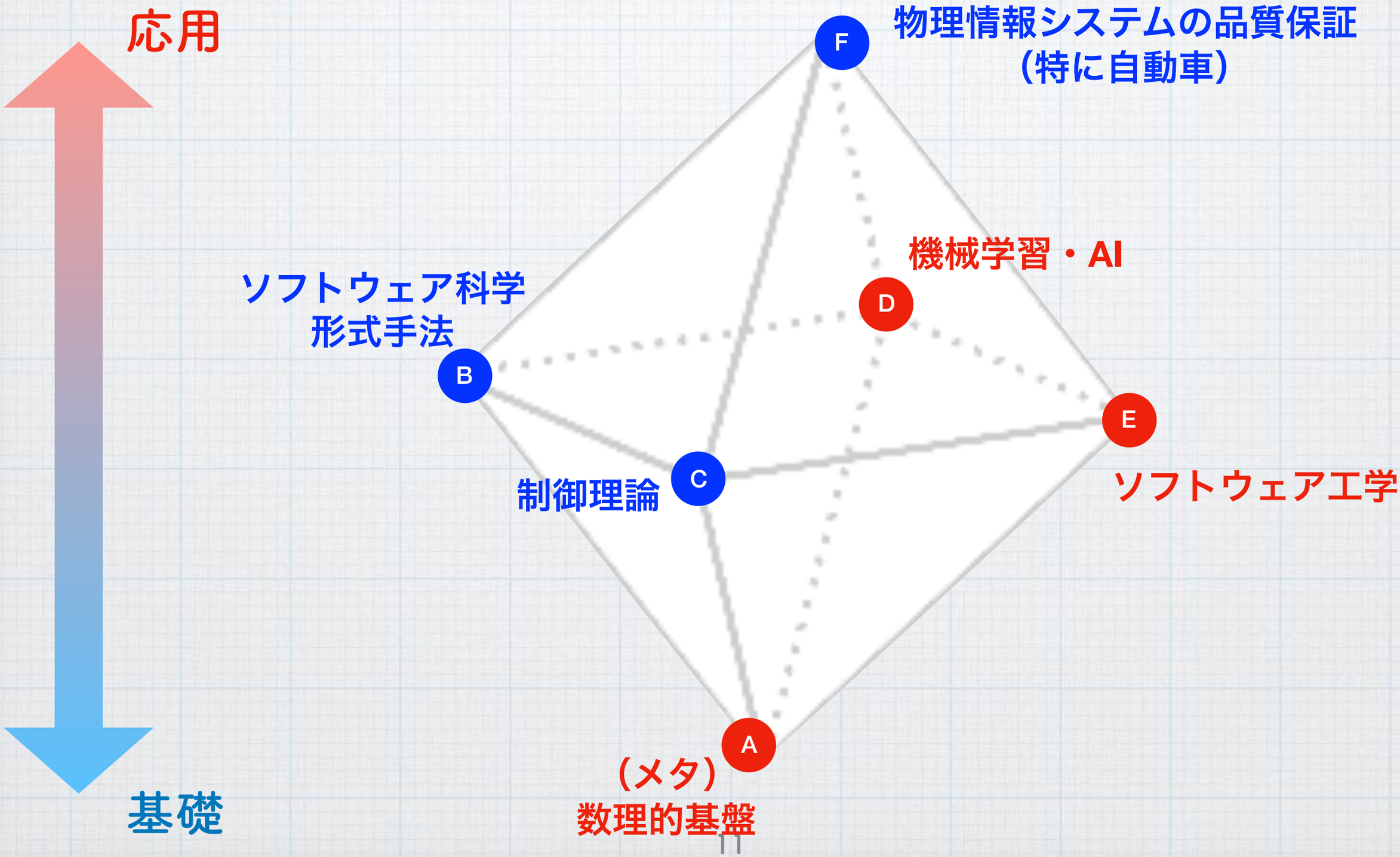
$x' = f(x, u)$



- 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？

物理情報システムのための分野横断： ERATO MMSDの場合



高信頼自動運転システムへの学術研究

* 発表の場は国際会議が主力.
  * IEEE ITS Society Conferences: IV, ITSC, …
  * 制御理論: CDC, ACC, …
  * ハイブリッドシステム（形式手法＋制御）：
    HSCC, ICCPS, EMSOFT, …
  * 形式手法： CAV, ATVA, TACAS, …
  * 形式手法の数理的理論： LICS, POPL, FoSSaCS, …

* CORE Rank (portal.core.edu.au/conf-ranks/)が，学術界における visibility の目安

* 計算機科学の論文データベース https://dblp.org/
  （制御系の論文は取りこぼしも）

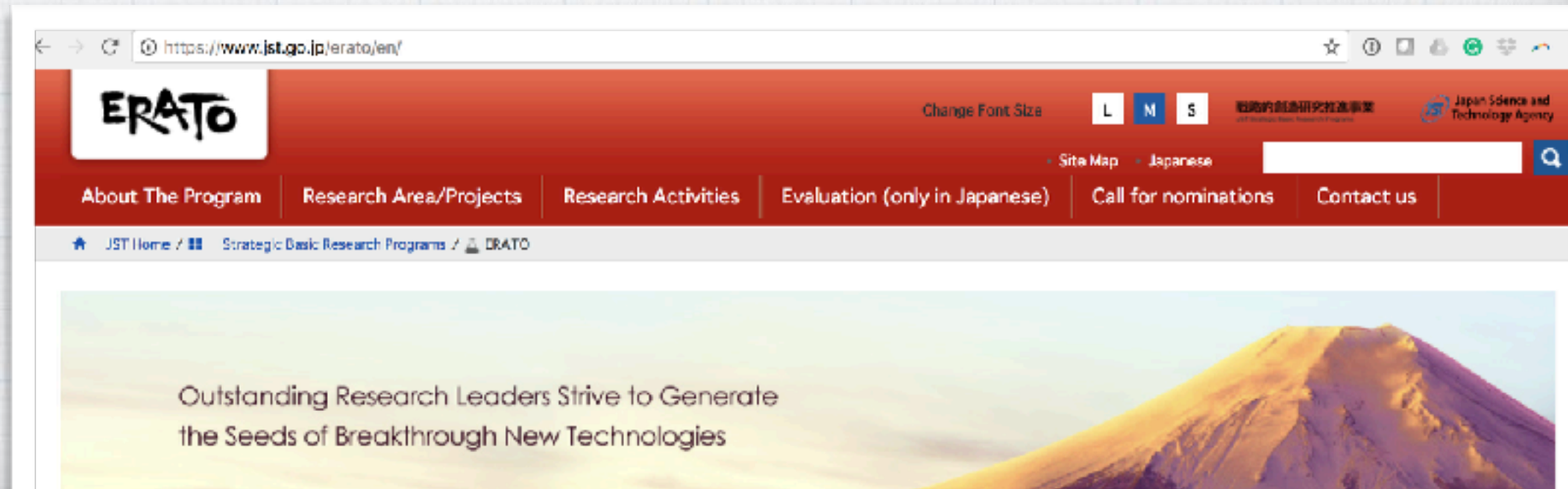
アウトライン

* 本日の趣旨
* 研究開発の背景
* ERATO MMSD 紹介
  * プロジェクト体制
  * 学術的研究の現状
  * 実応用に向けた研究開発の現状
* 世界の同種の取り組みとの比較
* プロジェクトの今後のビジョン

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

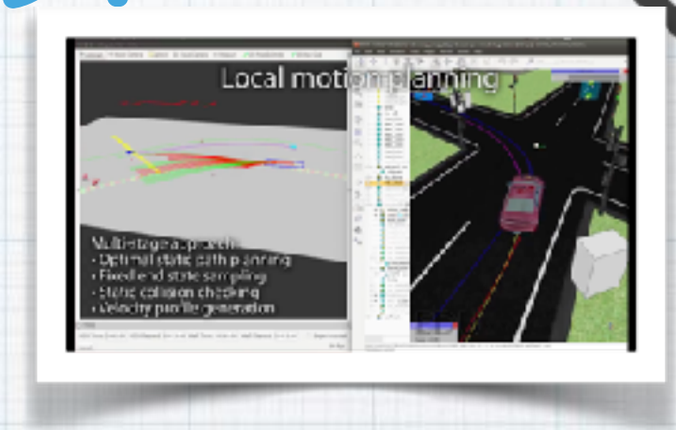
ERATO Program

* Funds large-scale projects for basic research.
  Run by JST (Japan Science and Technology Agency)
  * Biggest perpetual govt. funding granted to individual researchers
  * 5.5 years. Max 1.2B JPY (~ 10.5M USD ~ 9M EUR)
* 2-4 projects start every year,
  selected from all science & technology disciplines (physics, biology, …)



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



* JST ERATO プロジェクト
  * 2016/10-2022/03. 直接経費総額10億円超
* 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
  * 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

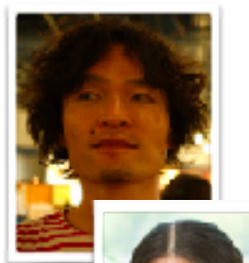
Group 0 @ NII:
Metatheoretical Integration
Leader: Shin-ya Katsumata

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

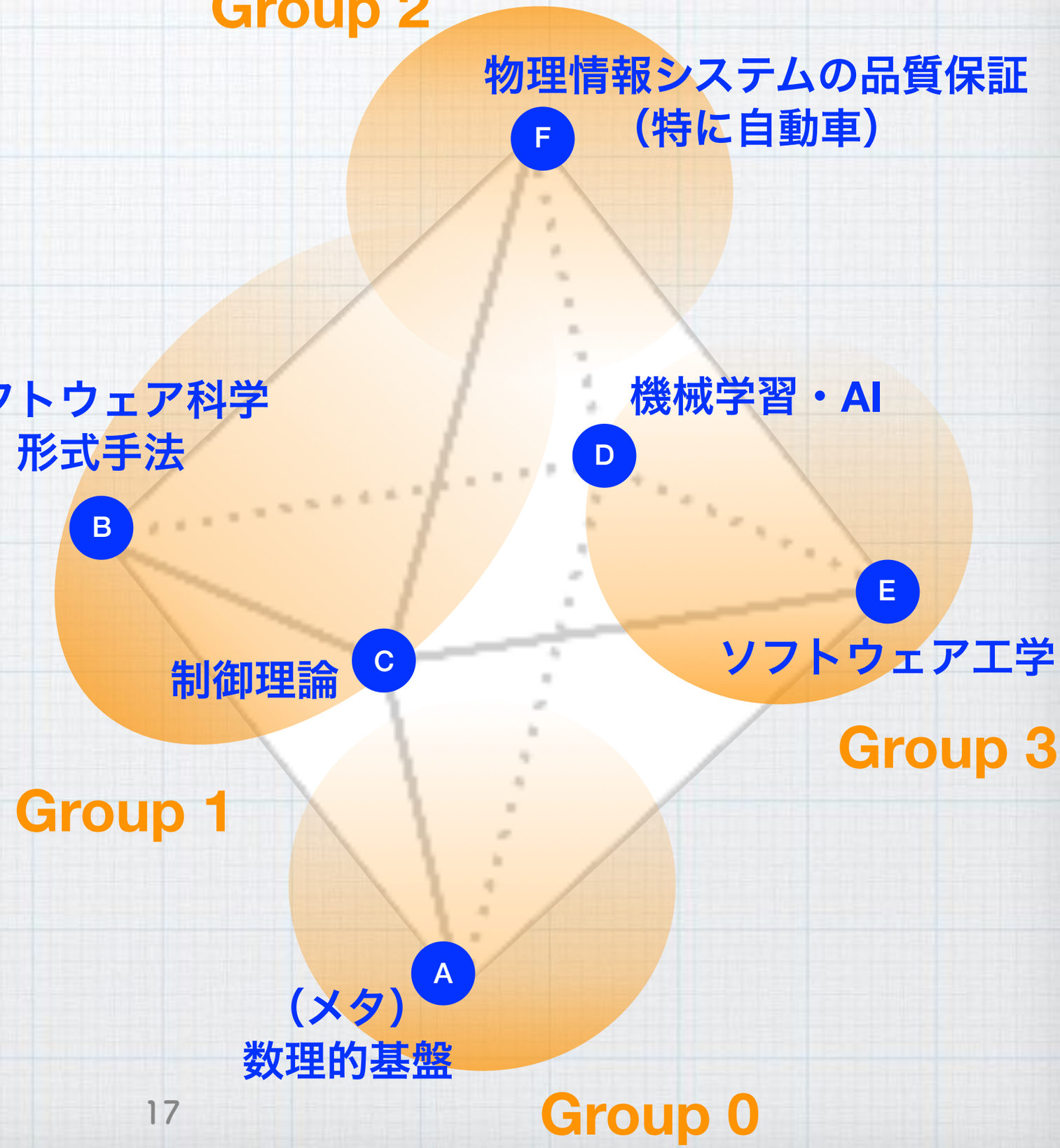
研究体制

* 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，要件工学，…

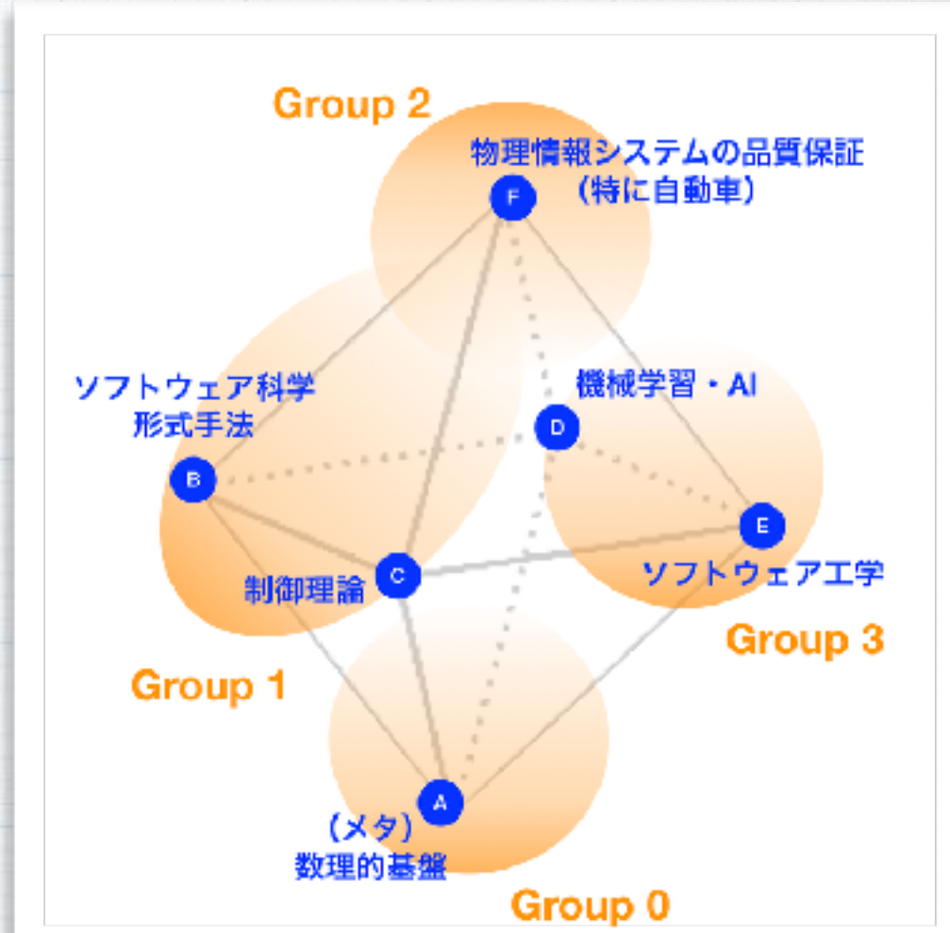


協力体制

- 海外の大学
  - U Waterloo, Canada (Czarnecki, ERATO)
  - Arizona State U, US (Fainekos)
  - U Colorado Boulder, US (Sankaranarayanan)
  - CMU, US (Platzer)
  - Verimag, France (Maler, Dang)
  - ENS Paris, France (Rival)
  - ENS Paris Saclay, France (Haas)
  - U Paris XIII, France (Andre)
  - U Innsbruck, Austria (Kaliszyk)
  - Radboud U Nijmegen, the Netherlands (Jacobs)

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（Andre, Waga） ポスター
    * 深層学習のための圏論的理論（Sprunger & Katsumata） ポスター
  * 機械学習利用 ➔ 効率的テスト (Zhang) ポスター
* 数理的基盤(G0)の重要性
  * 学術的＆人的
* 国際的 visibility:
  * CORE rank A* (top 4%, LICS, CAV, …): > 10 報
  * CORE rank A (top 18%, ATVA, TACAS, GECCO, …) > 20 報
  * 最優秀論文賞： ICECCS'18, FoSSaCS'19（共にCORE rank A）
  * 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



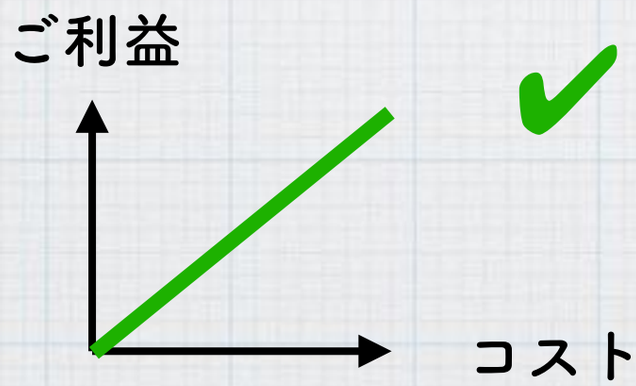
応用面での進捗状況

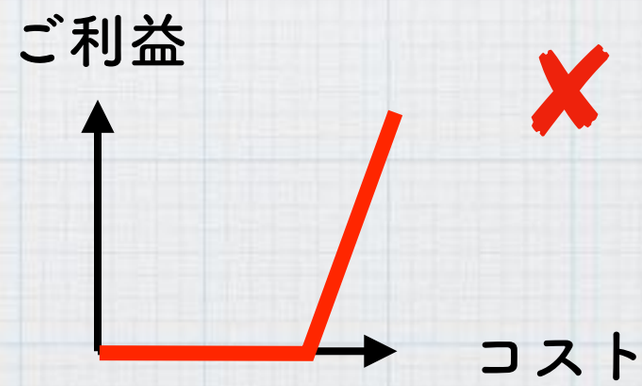
* プロトタイプツール多数
  * 実行時監視ツール
    * MONAA [Waga+, FORMATS'17] https://github.com/maswag/monaa
    * SyMon [Waga+, CAV'19] https://github.com/MasWag/symon
  * サーチベーステストツール
    * FalStar [Zhang+, EMSOFT'18] https://github.com/eratommsd/falstar
  * その他：確率的プログラム自動検証ツール，RNN2WFA ツール（recurrent neural network 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

* 多くのツールでのポイント：「スケールダウン」できること
  * 既存の製品・モデル・業務フローで利用可能なツール.
    「最初から全部形式化してもらわないと困ります」とは言わない

スケールダウンできる形式手法

* Scalability はしばしば「スケールアップできること」と理解される
  * 2倍のコストで，2倍のご利益
* 実応用の現場では，「スケールダウンできる」ことも重要
  * 1/2 倍のコストで，1/2 倍のご利益 （0でなく）
* 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
  * それがないと動かない ➜ ご利益 0
  * 「まず形式モデルを書いてください」





応用面での進捗状況

* 企業との協働
  * 5～10社と協働.
    （定期的議論，NDA，学術指導，共同研究，
    研究員受け入れ）
  * 具体的題材をいただき，
    * 手持ちの手法を総動員して解決
    * このトライアルから生まれる新しい学術研究

* autonomoose プロジェクト(Group 2, @ Waterloo)
  との協働
  * コア領域を選定済，プロジェクト期間残り3年で
    ソフトウェアツール群の樹立を目指す（詳細は後述）
    * 形式安全アーキテクチャ
    * テストシナリオ生成

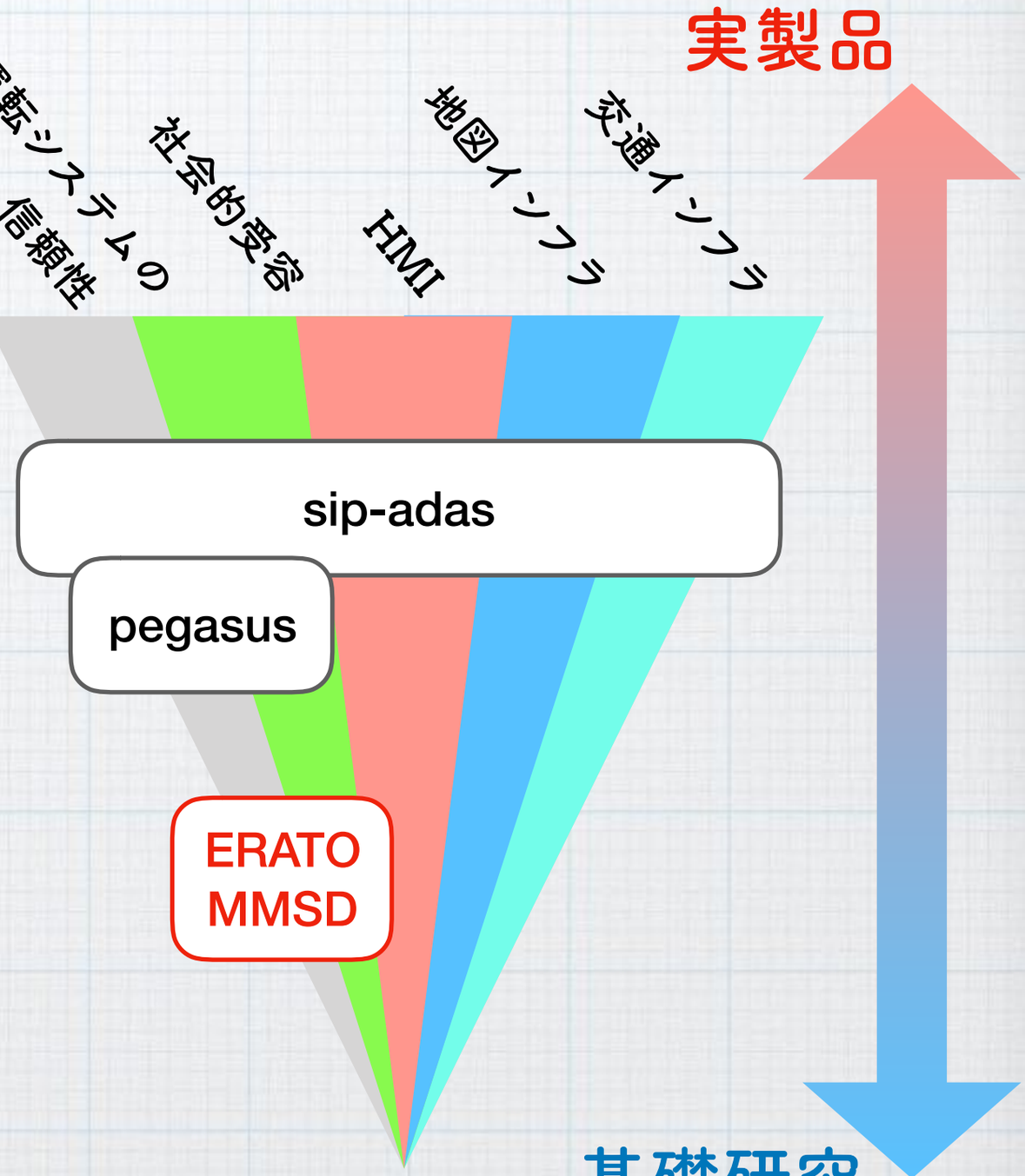
アウトライン

* 本日の趣旨
* 研究開発の背景
* ERATO MMSD 紹介
  * プロジェクト体制
  * 学術的研究の現状
  * 実応用に向けた研究開発の現状
* 世界の同種の取り組みとの比較
* プロジェクトの今後のビジョン

同種の取り組みとの比較

* 数多い自動運転プロジェクトに比べて：
  ソフトウェア信頼性研究から始まった
  自動運転プロジェクト
    * safety-progress のトレードオフにおいて，safety が起点

* 独 pegasus プロジェクト pegasusprojekt.de
    * ドイツの産官学プロジェクト．
      2016.1-2019.6，34.5 mil. EUR
    * 目標： 自動運転システムの（信頼性などの）
      性能評価基準の明確化
    * 実製品応用に主眼．
      データ活用，システム結合，具体的走行シナリオ
    * 比較して： ERATO MMSD は基礎的学術研究
        * 新奇な要素技術開発に注力
        * 新たな理論，アルゴリズム ➜
          自動運転のみならず，より広く適用可能

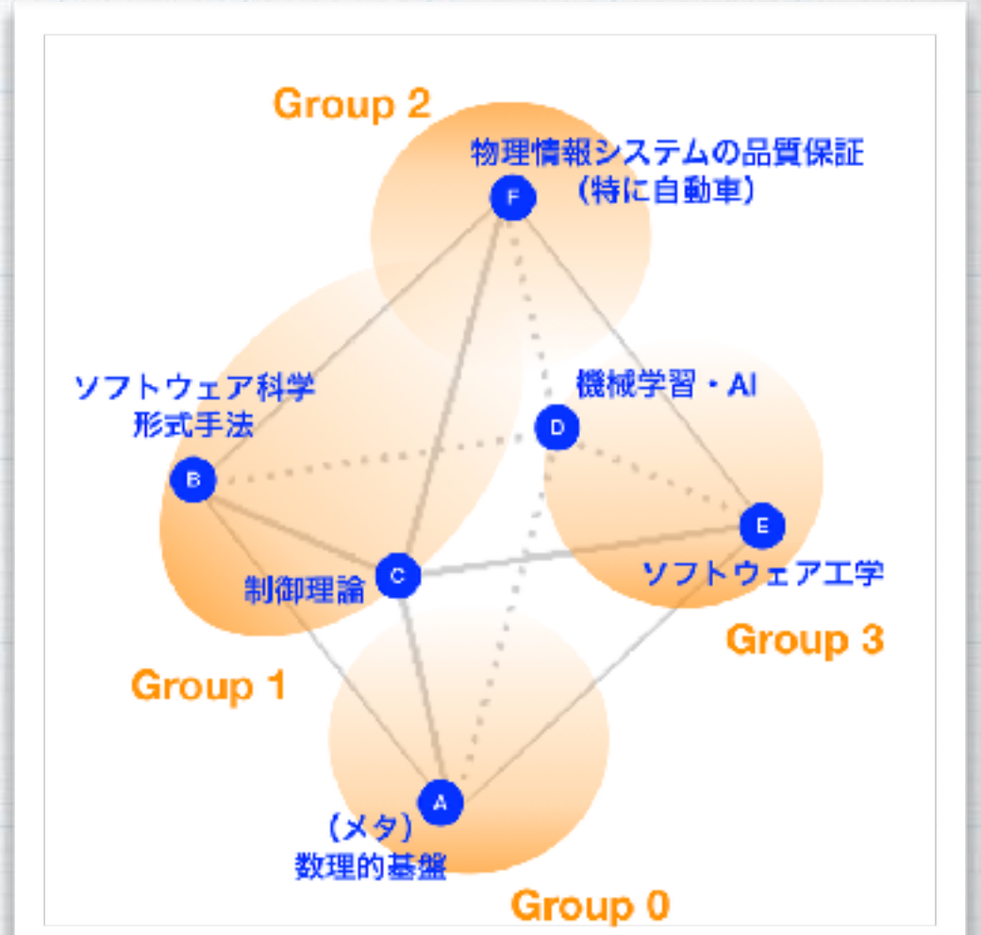


アウトライン

- 本日の趣旨
- 研究開発の背景
- ERATO MMSD 紹介
  - プロジェクト体制
  - 学術的研究の現状
  - 実応用に向けた研究開発の現状
- 世界の同種の取り組みとの比較
- プロジェクトの今後のビジョン

ERATO MMSD の「今日」

* 新規な理論・アルゴリズム
  * 学術界で確かな国際的 visibility
  * ツールプロトタイプも多数
    （一部は公開済み，前述）
    * 実行時監視，サーチベーステスト，…



* 多分野を統合する学術研究が，
  具体的応用に牽引され，
  また，確固とした数理的基盤に支えられるような
  研究体制ができた．

ERATO MMSD の「明日」

* （プロジェクト終了時，2022年3月までの未来像）

* 以下のツール群を具体的目標に設定．自動運転システムの研究開発に確かな貢献を行う．
  （各項目については後で説明します）
  * 1. 形式的安全アーキテクチャ
  * 2. 自動運転システムのテストシナリオ生成ツール
  * 3. （安全ながら保守的になりすぎない）
    自動運転システムの判断・経路生成アルゴリズム
  * 4. 形式仕様記述を支援する対話型ツール
  * 5. 上記を結合する自動運転ソフトウェアプラットフォーム．認識・判断・操作・信頼性保証

* これらツール群の技術移転（持続的な保守・改良のため商業化）

* 基礎的方法論の戦略的特許出願 ➜ 業界全体に広く使っていただくことが目的

* 各企業さまとの協働を継続
  ➜ ニーズとシーズのマッチング，我々の一般論を個別応用へ適合

ERATO MMSD の「明後日」

* スケールダウンできる形式手法を実現
  コスト-利益のバランスを選べるツール・手法を産業界に多数提供

* その実現のため，以下のペアそれぞれにおいて，両輪の発展を行う（詳細は後ほど）
  * 論理的手法 vs 統計的手法
  * 形式検証 vs テスト
  * 学術的基礎研究 vs 産業応用