数理的高信頼ソフトウェアシステム研究センター ・ ERATO 蓮尾プロジェクト (ERATO MMSD)

論理的安全ルールによる自動運転安全性の数学的証明

自動運転の社会受容を促進

連絡先: 蓮尾 一郎・Clovis Eberhart・James Haydon http://group-mmm.org/eratommsd

課題背景

自動運転の社会受容の遅れ

- 2018年の事故以降，自動運転事業化の機運が停滞気味
- 安全性を実現するのみならず，社会に説明して受容してもらわないと公道は走れない
- 何をもって「十分に安全とするか」の合意が不在
  → アプローチ，企業，規格が多数

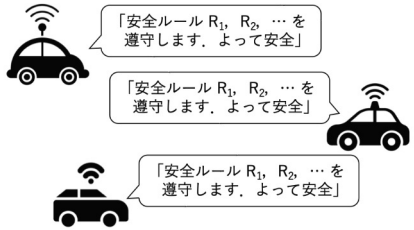
未知・過剰な製造物責任のリスク

- 自動運転の製造物責任の範囲は未確定，（社会的合意，規格，法律等）
- 製造者は将来，想定外の大きな製造物責任を負わされる可能性がある
  → 参入・産業発展の大きな障壁
- 安全ルール（「これを満たせば安全」）の策定が待たれる

→ 正当性が数学的に保証された安全ルールを提供，社会への説明と製造物責任の明確化

論理的安全ルールによる自動運転安全性保証 ～ RSS [Shalev-Shwartz et al., 2017] 及び GA-RSS [Hasuo+, IEEE T-IV, in press] の考え方

規格化団体・規制当局など



安全ルール R_1
同一車線・同一進行方向の交通シナリオにおいては，

- 先行車からの距離を少なくとも

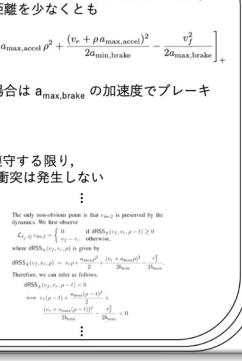
$$d_{\min} = \left[v_r \rho + \frac{1}{2} a_{\max,\text{accel}} \rho^2 + \frac{(v_r + \rho a_{\max,\text{accel}})^2}{2a_{\min,\text{brake}}} - \frac{v_f^2}{2a_{\max,\text{brake}}} \right]_+$$

確保すること

- それが困難な場合は $a_{\max,\text{brake}}$ の加速度でブレーキをかけること

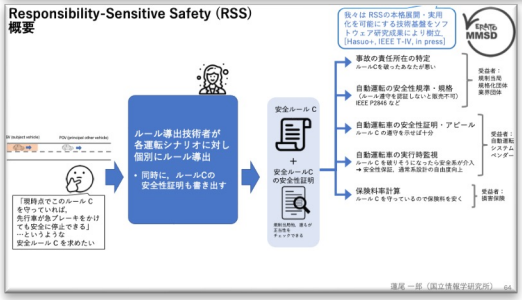
安全性定理
安全ルール R_1 を遵守する限り，自車の責任による衝突は発生しない

安全性定理の数学的証明



- 安全性という複雑な目標を，確認・強制が容易な**安全ルール**に分解
- 安全ルールの正しさを**数学的証明**（究極の保証！）．証明を追いかけることは論理的説明にもなる
- 安全ルールは汎用 ➔ 規準・規格として社会受容を促進
- 事故の責任特定（誰かが安全ルールを破ったはず）

Responsibility-Sensitive Safety (RSS) 概要



我々の成果： RSS の形式論理的拡張による安全ルールの本格展開

[Hasuo+, IEEE T-IV, to appear]

RSS
Responsibility-Sensitive Safety（責任感知型安全論），
Shalev-Shwartz et al., 2017

- 安全ルールの基本的方法論
- 国際規格化の動き (IEEE 2846)
- 複雑なシナリオに対するルール策定・証明手法は未整備
- 特に，衝突回避以外の目的への対応事例がない

↓ ソフトウェア研究の知見

微分プログラム論理 dFHL（今回の成果）

- 安全ルール導出・証明のための論理体系

dFHL による逐次的推論・ルール導出ワークフロー（今回の成果）

- 複雑な行動計画を分割，それぞれ論理的解析し，結果を結合
- 自動推論によるツールサポート

GA-RSS（今回の成果）
Goal-Aware Responsibility-Sensitive Safety

- 衝突回避に加え，緊急停止等の目的達成もサポート
- 複数の行動を組み合わせた大局的安全ルール
- 現実の複雑な交通シナリオへの適用において必須

研究内容： Goal-Aware RSS の実現

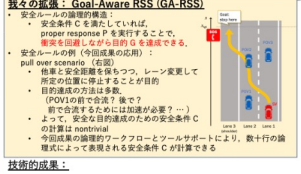
既存技術：（オリジナル）RSS ("Collision-Avoiding RSS", CA-RSS)

- 安全ルールの論理的構造：
  - 安全条件 C を満たしていれば，proper response P を実行することで，衝突を回避できる．
  - よって，「安全条件 C を守っていれば未来の衝突を回避できる」と言える
- 安全ルールの例 [Shalev-Shwartz et al., 2017]：single-lane, same-direction scenario

- 上記安全距離を守っていれば，加速度 $a_{\max,\text{brake}}$ ブレーキをかけることで衝突回避できる
- 保証されるのは衝突回避のみ
- 複雑なシナリオに対してのルール策定は未達
  - 方法論・ソフトウェアサポートが不在
  - 上記の単純シナリオのルールが，現存するほぼ唯一の例

我々の拡張：Goal-Aware RSS (GA-RSS)

- 安全ルールの論理的構造：
  - 安全条件 C を満たしていれば，proper response P を実行することで，衝突を回避しながら目的 G を達成できる．
- 安全ルールの例（今回成果の応用）：pull over scenario（右図）
  - 他車と安全距離を保ちつつ，レーン変更して所定の位置に停止することが目的
  - 目的達成の方法は多数．（POV1の前で合流？ 後で？ 前で合流するためには加速が必要？ …）
  - よって，安全な目的達成のための安全条件 C の計算は nontrivial
  - 今回成果の論理的ワークフローとツールサポートにより，数十行の論理式によって表現される安全条件 C が計算できる



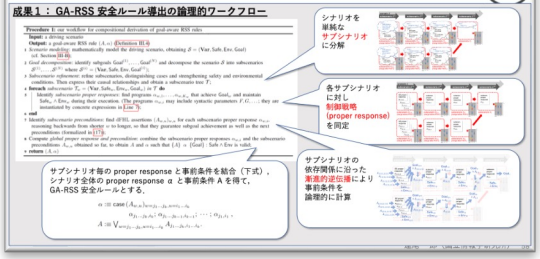
技術的成果：
GA-RSS 安全ルールのシステマティックな導出を可能にする

- 汎用の論理的ワークフローの設計
- 上記ワークフローで必要なプログラム論理体系の設計
- 上記ワークフローのソフトウェアによる実現

技術的成果 1~3

Ichiro Hasuo, Clovis Eberhart, James Haydon, Jeremy Dubut, Brandon Bohrer, Tsutomu Kobayashi, Sasinee Pruekprasert, Xiao-Yi Zhang, Erik Andre Pallas, Akihisa Yamada, Kohei Suenaga, Fuyuki Ishikawa, Kenji Kamijo, Yoshiyuki Shinya, Takamasa Suetomi. *Goal-Aware RSS for Complex Scenarios via Program Logic*. IEEE Trans. Intelligent Vehicles, in press. 特許出願済

成果 1：GA-RSS 安全ルール導出の論理的のワークフロー



技術的成果 1~3

Ichiro Hasuo, Clovis Eberhart, James Haydon, Jeremy Dubut, Brandon Bohrer, Tsutomu Kobayashi, Sasinee Pruekprasert, Xiao-Yi Zhang, Erik Andre Pallas, Akihisa Yamada, Kohei Suenaga, Fuyuki Ishikawa, Kenji Kamijo, Yoshiyuki Shinya, Takamasa Suetomi. *Goal-Aware RSS for Complex Scenarios via Program Logic*. IEEE Trans. Intelligent Vehicles, in press. 特許出願済

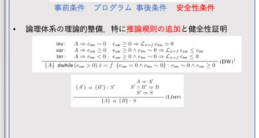
成果 2：GA-RSS 論理的のワークフローのためのプログラム論理体系 （成果 1，逆伝搬に使用）

- プログラム検証のための Floyd-Hoare logic [Hoare, CACM'69] ＋連続ダイナミクスのための ODE 拡張 (cf. [Platzer '18])
- ＋プログラム実行中に真であるべき安全性条件の追加

$$\{A\}\ \alpha\ \{B\} : S$$

事前条件　プログラム　事後条件　安全性条件

- 論理体系の理論的整備，特に推論規則の追加と健全性証明



成果 3：GA-RSS 論理的のワークフローのソフトウェア実装 （成果 1，逆伝搬の計算に使用）

- 数十行の論理式
  ＋ 代数・論理的記号操作（代入，2次方程式解，不等式証明等）
  ➔ 人手，pen-and-paper では困難
- 計算機代数システム Mathematica を用いた半形式的ソフトウェア実装を実現
  - プログラム論理の推論規則の適用は人手，非形式的だが，well-documented, traceable
  - プログラム・ダイナミクスに陽に関わらない代数・論理的記号操作（代入，2次方程式解，不等式証明等）を Mathematica で形式化
- 定理証明システム KeYmaera X [Platzer '18] を用いたフル形式的ソフトウェア実装を構想中．予備的試行はスムーズ