ソフトウェアの動作が満たす制約を導く・制約を満たす動作を導く

ソフトウェアシステムの形式仕様の解析・変換

どんな研究？

安全なソフトウェアを設計するために、数学の言語で「ソフトウェアがどう**動作**するか」「動作した結果どのような**制約**を満たすべきか」を記述し、本当に制約が満たされるかを数学の証明問題として確かめる方法が有効です。
しかし、人間にとって**動作や制約を適切に記述することは難しい**タスクです。本研究は、**動作から制約を、制約から動作を自動で導く**ことで、これを補助します。

何がわかる？

例えば、ドローンを動かすソフトウェアを
安全性を数学的に保証しながら作るとき……
「記述した動作は、どんな制約を満たす？」
「高度センサに誤差がない前提で動作を記述したけれど、
誤差のあるセンサを使っても安全に動かすには
どんな動作にすれば良い？」
こんな疑問を解決 → **安全なソフトウェアの構築を補助！**

背景

予約動作
予約数 < 席数　のとき
予約数 := 予約数+1

制約　予約数 ≤ 席数

システムは
こう動作する

動作の結果
この制約が
満たされるべき

予約動作はどんな場合でも
本当に制約を満たす？

予約数 < 席数　だから、
予約数が1増えても
予約数 ≤ 席数　は必ず
成り立つのでOK！

研究内容 1

[小林，JST ACT-I加速]

これで
いいかな

正しいが、
「ゆるい」制約

制約 2　予約数 ≤ 席数+1

十分強い制約を人が書くのは難しい…

形式仕様開発時の課題

提案
ツール

予約動作（変異種 1）
予約数 ≤ 席数　のとき
予約数 := 予約数+1

予約動作（変異種 2）
予約数 < 席数　のとき
予約数 := 予約数+2

提案手法 1
動作記述へのバグ追加（変異）

提案
ツール

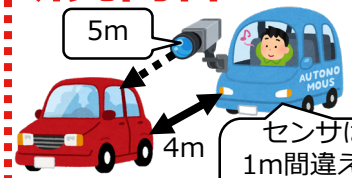
動作にバグを追加した**変異種**も制約 2 を満たす…
制約 2 は**ゆるい**！

制約 2 を**強く**して
予約数 ≤ 席数
にしたら**変異種を許さなくなった**！OK！

提案手法 2
分析・制約の修正

研究内容 2

[Kobayashi+, NFM'21] @ ERATO MMSD プロジェクト



センサは距離を
1m間違えるかも…
念のため1m分
余計に開けて動こう

背景：センサに誤差があっても
安全な制御ソフトウェア

距離の計測値は…
真の距離との差は
最大だと…

速度の計測値は…
真の距離との差は
最大だと…

これらを踏まえて
安全性制約の**保証に必要な動作**は…

複雑

開発の際の課題

誤差を考慮しない
ソフトウェアの動作の記述

提案ツールで変換

様々な**誤差の可能性を考慮**し、
しかも**安全性制約を満たす**
ソフトウェアの動作の記述

提案手法