

複雑な要件の抽象化・詳細化に関する研究

小林 努, 石川 冬樹, 本位田 真一

どんな研究?

信頼できるシステムを作るために、正しさを保ったままシステムを適切に何段階か「ぼかし」ながら数学的な検証を行う手法が注目されています。私たちは、「ぼかし方」を計画・編集することでシステムの検証を見通し良くする研究に取り組んでいます。

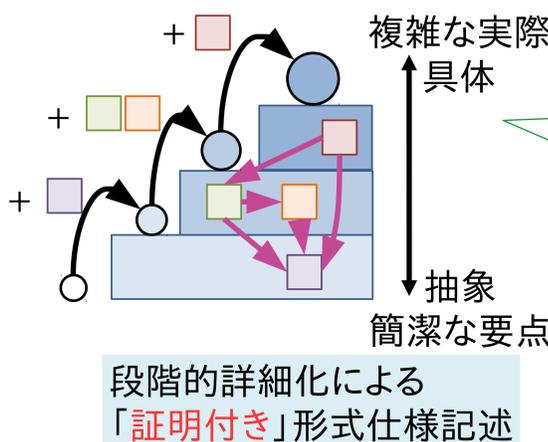
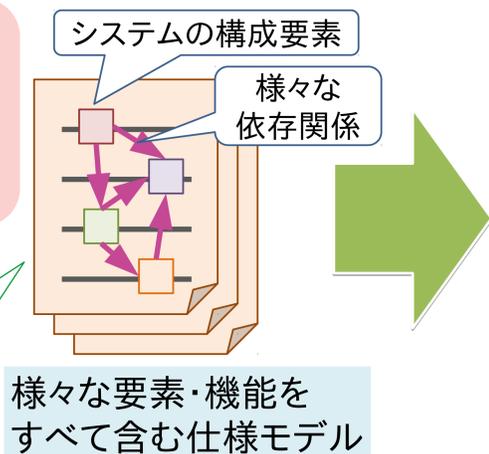
何がわかる?

見通し良くソフトウェアを検証できるようにすることで、私たちの身の周りの至るところにあるソフトウェアをより安全にすることができます。

背景

システムが行うこと・システムへの期待をきちんと分析したい!

人にとっても検証ツールにとっても、「なぜうまくいくか」の裏付けがほぼ不可能



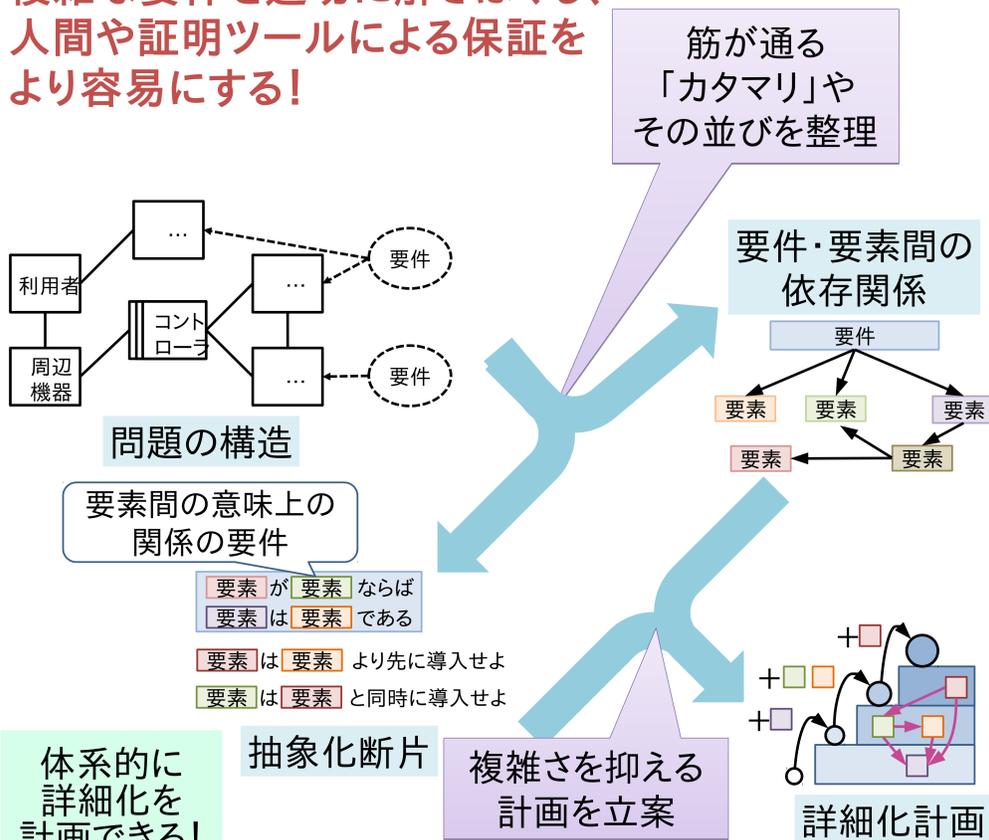
抽象モデルから少しずつ要素・機能を導入するよう「筋を通しつつ」解きほぐす

・どう計画すべき?
・作った後に構造を変えたくなかったら?

研究内容

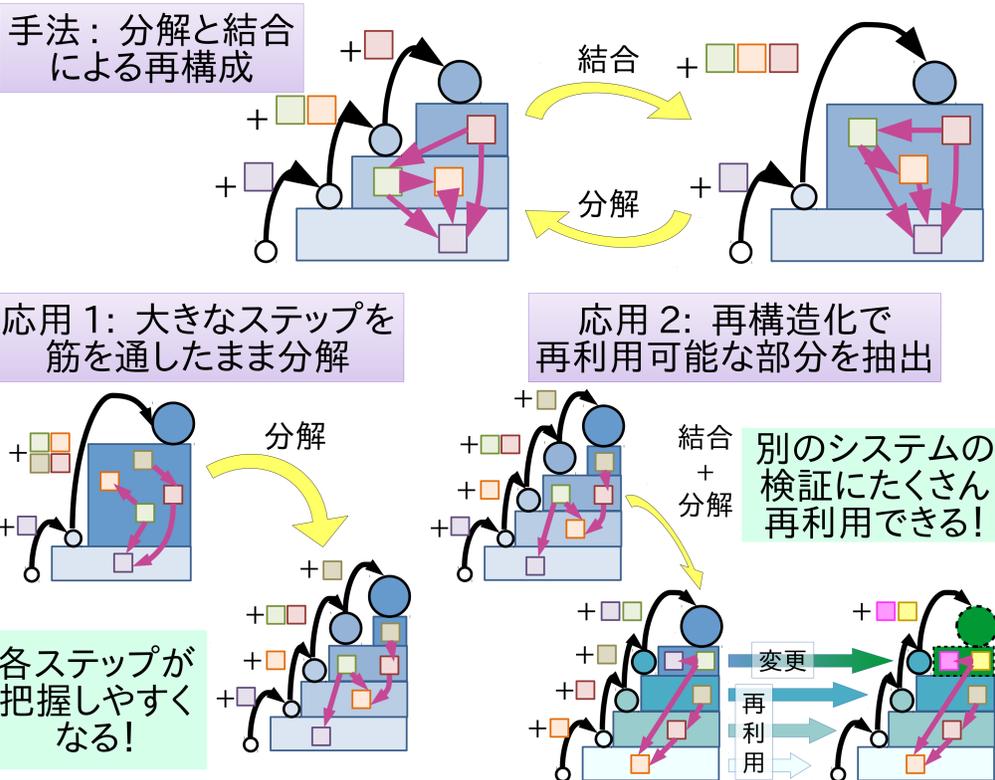
要素の意味と依存関係の分析による詳細化の計画手法・支援ツール

複雑な要件を適切に解きほぐし、人間や証明ツールによる保証をより容易にする!



詳細化構造の再構成による仕様のメンテナンス性・再利用性向上

仕様記述の詳細化構造を筋を通したまま変える!



石川, 科研費 基盤研究(B)「保証付き多段階システムモデルの柔軟・継続的な洗練・進化」
Kobayashi et al., Refactoring Refinement Structures of Event-B Machines, FM'16
Kobayashi et al., Stepwise Refinement of Software Development Problem Analysis, ER'16

