ソフトウェアシステムの要件の複雑さに抽象化で挑む

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。

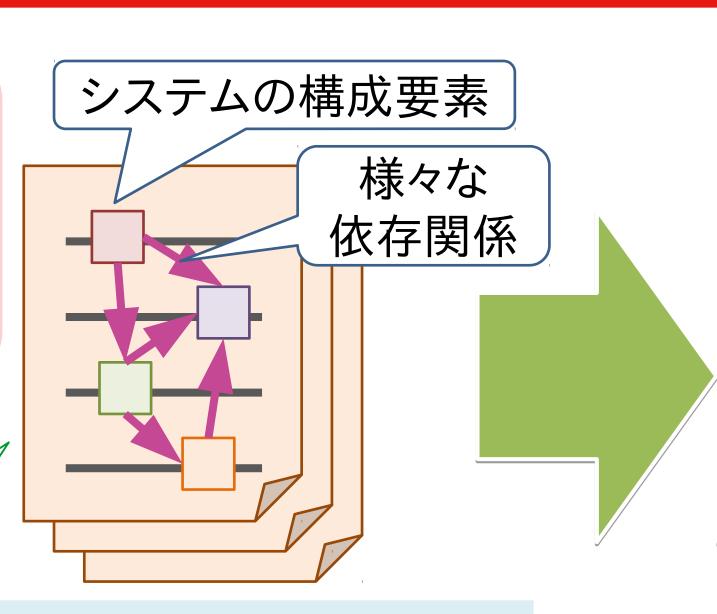
何がわかる?

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。

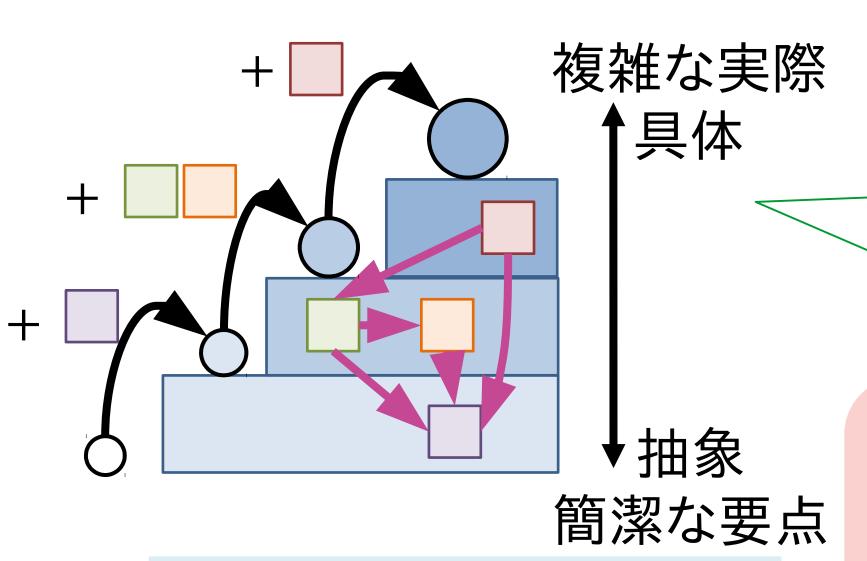
背景

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



様々な要素・機能を すべて含む仕様モデル



段階的詳細化による「証明付き」形式仕様記述

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?

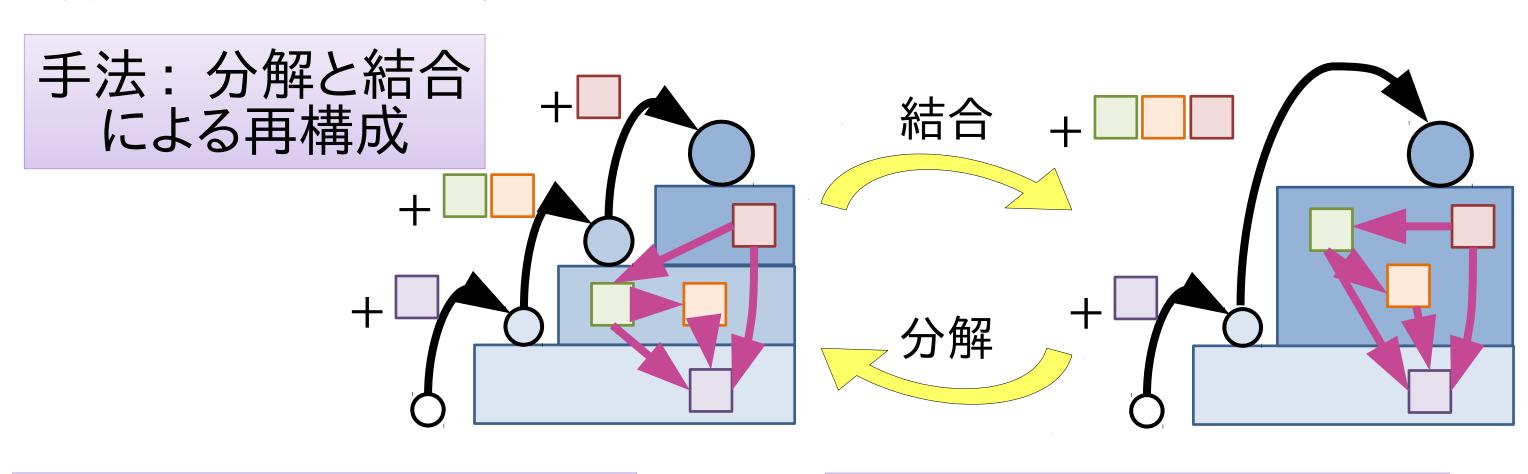
研究内容

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 筋が通る より容易にする! 「カタマリ」や その並びを整理 要件・要素間の 利用者 依存関係 周辺 機器 要件 問題の構造 要素間の意味上の 関係の要件 要素が要素ならば 要素 は 要素 である 要素は要素より先に導入せよ 要素は要素と同時に導入せよ 抽象化断片 体系的に 複雑さを抑える 詳細化を 計画を立案 詳細化計画 計画できる!

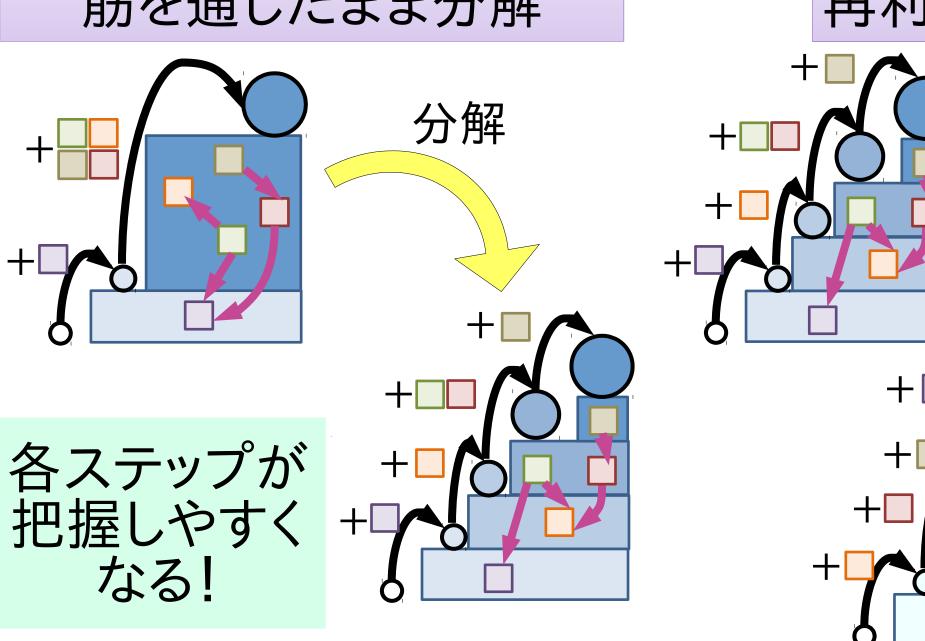
詳細化構造の再構成による 仕様のメンテナンス性・再利用性向上

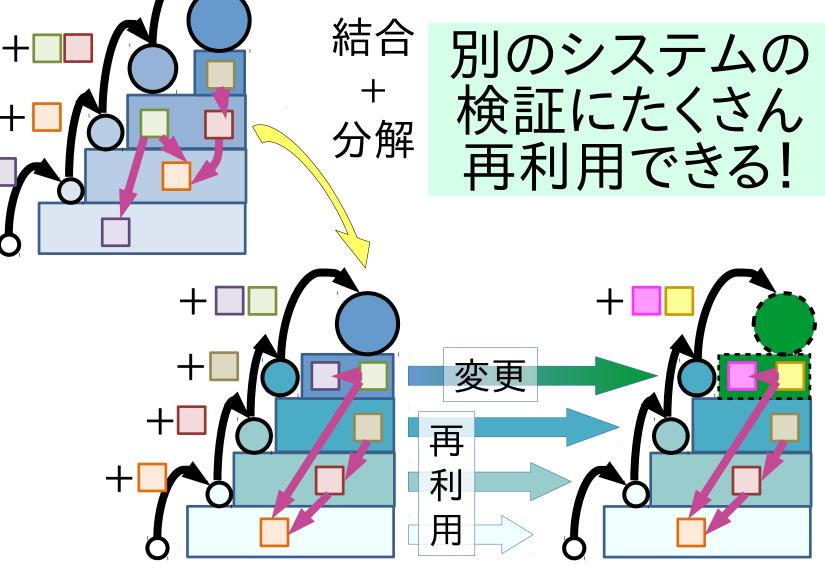
仕様記述の詳細化構造を 筋を通したまま変える!



応用 1: 大きなステップを 筋を通したまま分解

応用 2: 再構造化で 再利用可能な部分を抽出





石川,科研費 若手研究(A)「段階的詳細化における複雑さの分散と整合性の保証に関する研究」 Kobayashi et al., Understanding and Planning Event-B Refinement through Primitive Rationales, ABZ'14 Kobayashi et al., SliceAndMerge: A Rodin Plug-in for Refactoring Refinement Structure of Event-B Machines, Rodin Workshop '16

連絡先:小林 努/ 東京大学大学院 コンピュータ科学専攻 博士課程

Email: t-kobayashi@nii.ac.jp