適切な「ぼかし」で、ソフトウェアの複雑さに挑む

ソフトウェアの要件の「ぼかし方」に関する研究

石川 冬樹研究室　小林 努、猿渡 真之介、森田 大智、石川 冬樹

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、ぼかし方の分析・変更を通じて厳密で柔軟な開発を可能にする他、「ぼかし」の仕組みを拡張し適用範囲を広げる研究を行っています。

何がわかる？

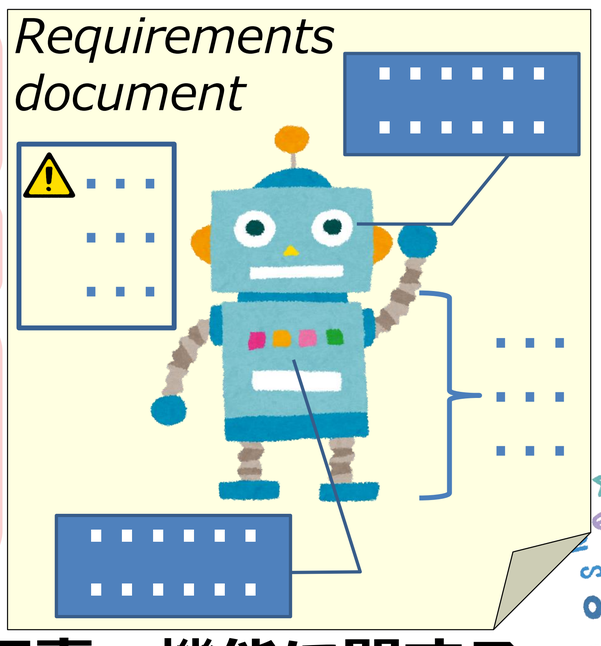
見通しの良いソフトウェアシステムの検証方法の柔軟性と適用範囲を広げることで、
私たちの身の周りの至るところにあるソフトウェアをより安全にすることができます。

背景：段階的詳細化を用いた形式的仕様記述

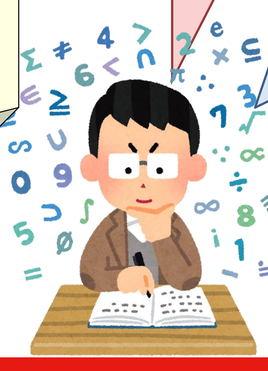
抜け・漏れ

複雑

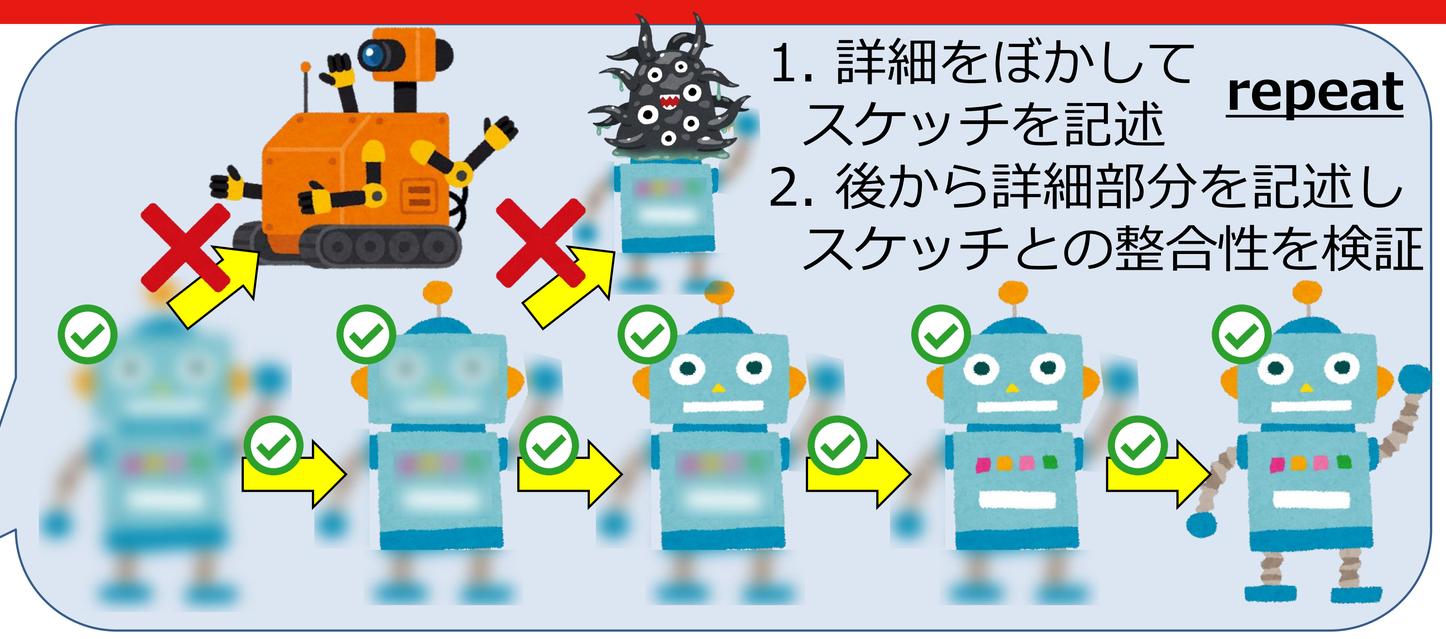
厳密に分析できない



様々な要素・機能に関する自然言語ドキュメント



多段階の詳細度にわたり数学的に仕様を記述・検証



厳密に記述・検証可能

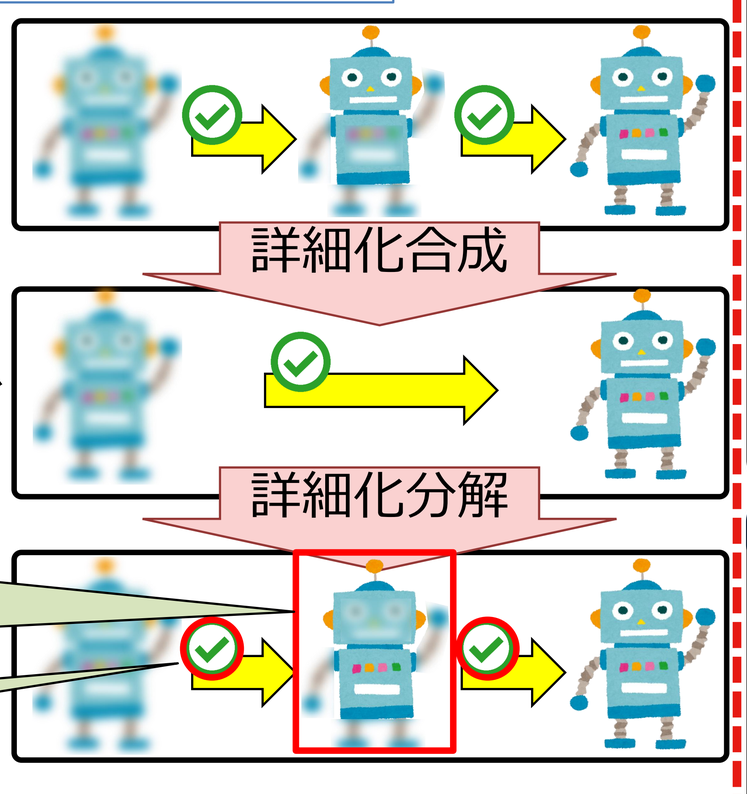
複雑さを分散

研究内容

整合性を保つ詳細化の自動変更　小林

提案技術

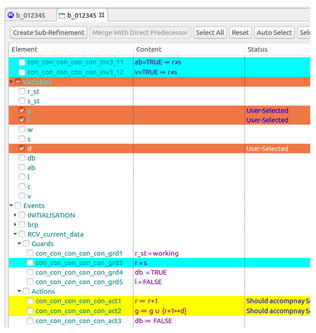
詳細化の合成・分解:
仕様の詳細化について、複数ステップの合成と１ステップの分解（**新しいぼかし方で**）を、整合性の証明を含め構築



今までになかったぼかし方を自動で構築！

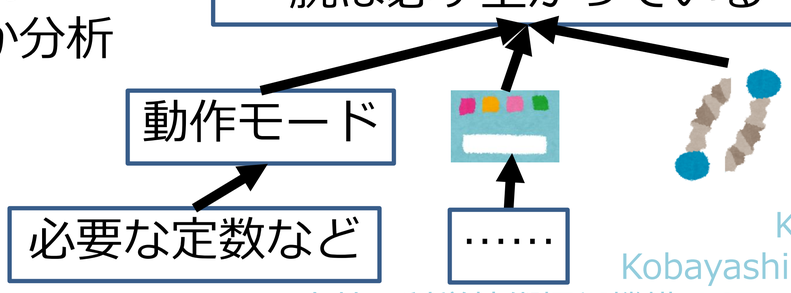
整合性も保証！

要素間の依存関係分析:
対象システムの仕様の式と構成要素がそれぞれどう依存しているか分析



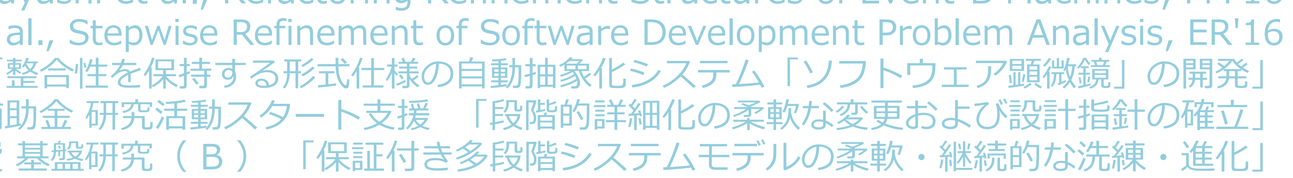
← ツール実装「Slice'n'Merge」
http://research.nii.ac.jp/slicenmerge/

式：動作モードが……で、胴体のランプが……の場合
腕は必ず上がっている



応用１：ぼかし方の計画の分析

問題：どのような順序で詳細化を行えばいいか指針がない



仕様を入力として、
いろいろなぼかし方を生成・分析
→ どのようなぼかし方が複雑さを軽減するかの知見を獲得

応用２：ぼかしによる効果的な仕様の再利用

問題：既存の仕様を過不足なく再利用したい

再利用可能な部分以外をぼかす
→ 再利用可能な部分を過不足なく獲得し、効果的に再利用

仕様を理解しやすくするなど他にも応用いろいろ！

Kobayashi et al., Refactoring Refinement Structures of Event-B Machines, FM'16
Kobayashi et al., Stepwise Refinement of Software Development Problem Analysis, ER'16

小林，科学技術振興機構 ACT-I　「整合性を保持する形式仕様の自動抽象化システム「ソフトウェア顕微鏡」の開発」
小林，科研費補助金 研究活動スタート支援　「段階的詳細化の柔軟な変更および設計指針の確立」
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」

仕様・設計の「ぼかし方」から全体を把握、再利用のとっかかりを探す

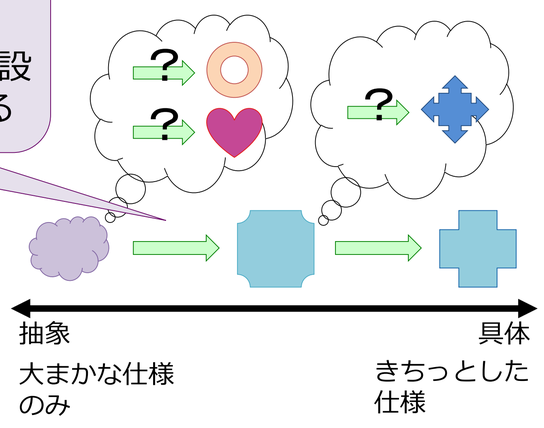
猿渡

「ぼかし」ながら作られたシステムは「ぼかし」の部分に仕様・設計の柔軟性がある

「ぼかし」の部分は大まかに仕様を満たす

矛盾が生じないよう徐々に仕様・設計を細かくして確認しながら作る

矛盾がなければ違う形に変えることができる！



「ぼかし」の部分＝様々な可能性！

「ぼかし」の箇所や「ぼかし」具合を把握することでどのようにシステムが作られたかを理解

システムの整合性を崩さずに仕様を追加、変更する際のヒントになる

性能の向上のためにシステムに新しい仕様を追加したい！

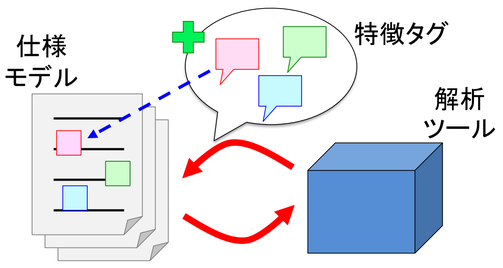
似たようなケースに対してこのシステムを再利用したい！

仕様の変更が容易であるか、システムが再利用可能なのかが知りたい！

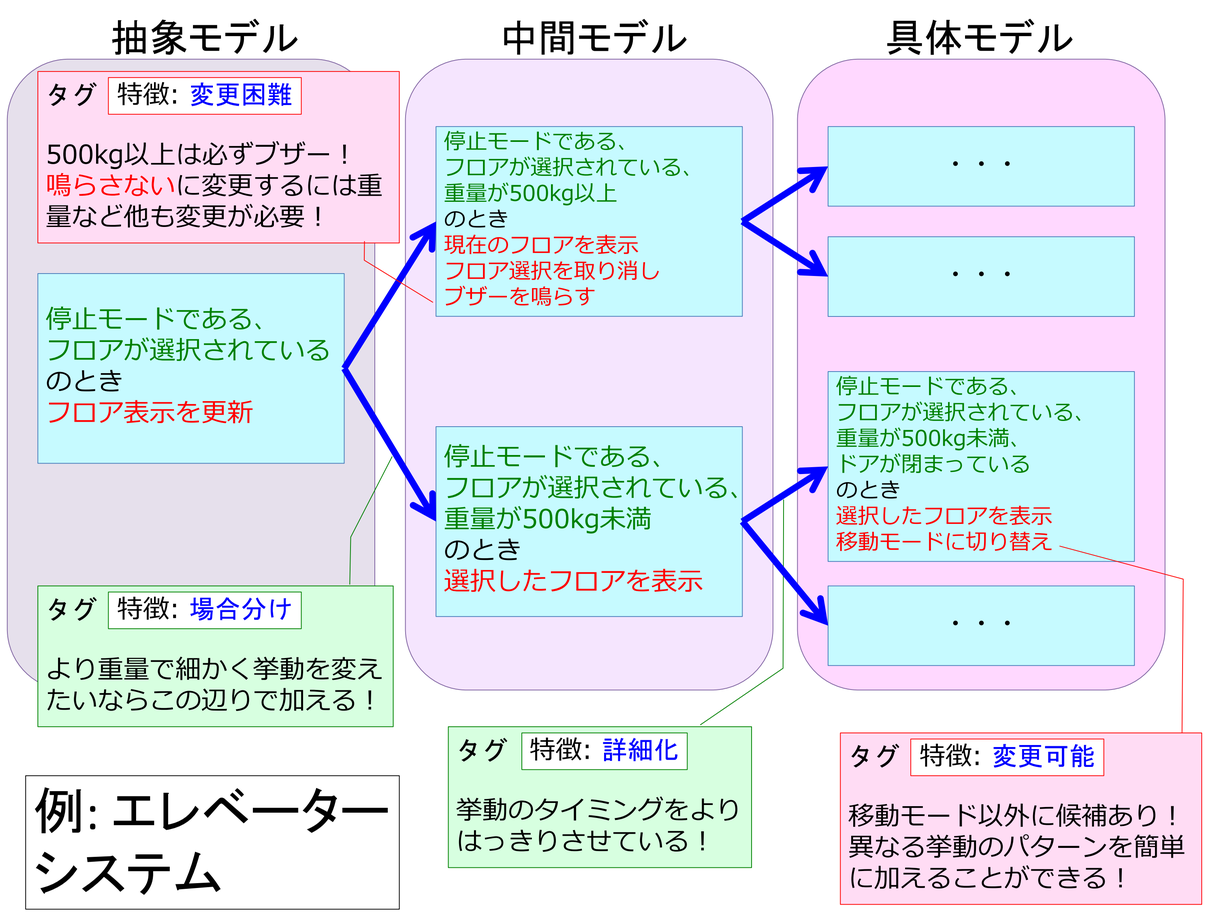
「ぼかし方」を把握することでどうすればシステムの仕様の変更が可能か判断ができる！

仕様の詳細化における特徴解析によるモデル理解と仕様変更支援手法・ツール

仕様モデルの「ぼかし」がきちっと決まっていく流れ（詳細化）の特徴を解析、モデルにタグを付けていく！



仕様モデルだけではわかりづらかった「ぼかし」の実態が詳細化の特徴から見えてくる！



ハイブリッドシステムへの段階的詳細化の適用

森田

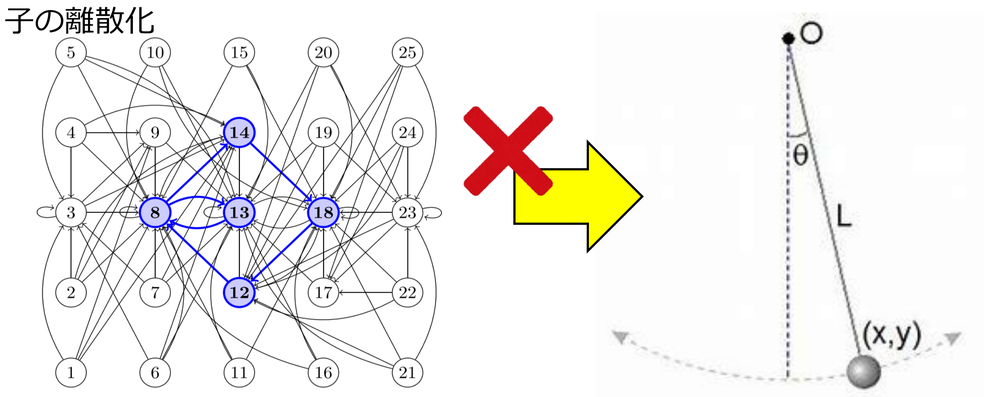
ハイブリッドシステム

センサーネットワークなどで実世界をモニタリングしながら、機械をコンピューター制御することで、実世界をコントロールするシステム

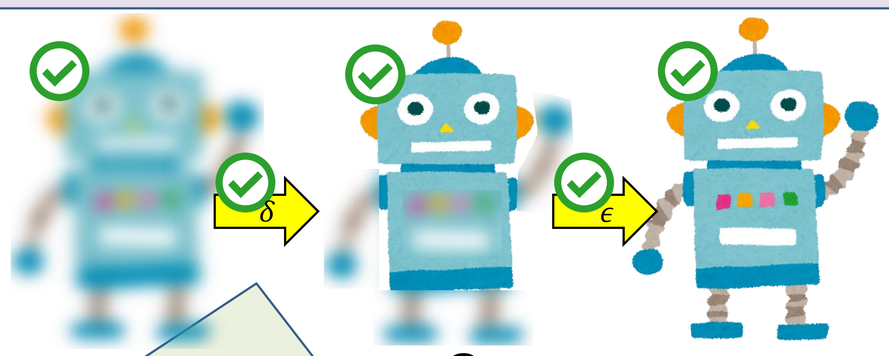
ハイブリッドシステムも段階的に検証したい

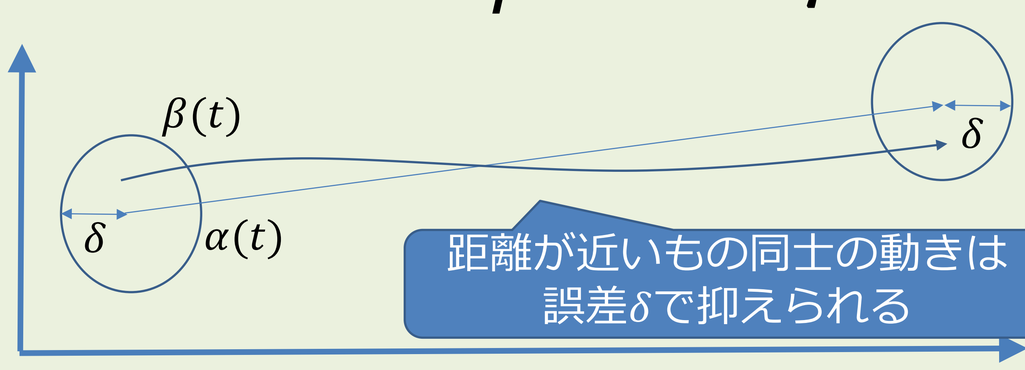
- 連続的な物理現象に対して、数学的検証を積み重ねて整合性の担保をするのは難しい
- 厳密なぼかしだと影響の小さい項を追加するができない
- 離散化などの、厳密なぼかしではないけど検証するのに強力なツールも扱えるようにしたい

例) 振り子の離散化



誤差δを担保した詳細化を採用

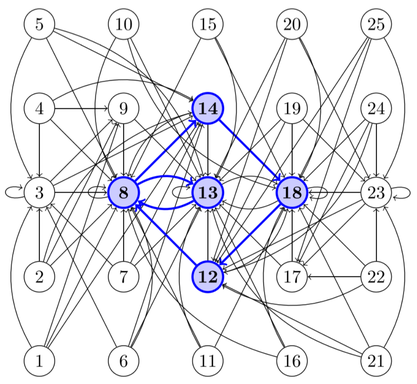


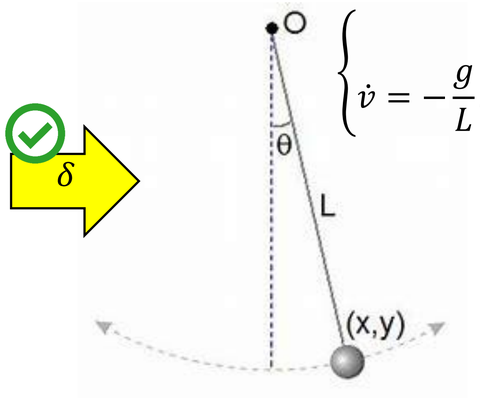


soundness theorem

仕様ϕを検証

仕様ϕが誤差δで成立！





$$\begin{cases} \dot{\theta} = v \\ \dot{v} = -\frac{g}{L} sin\theta - \frac{k}{m} v + u \end{cases}$$

NII
連絡先：小林　努／　国立情報学研究所　アーキテクチャ科学研究系　特任研究員
Email：t-kobayashi@nii.ac.jp