アプリの隠れた性質をあぶり出す

プログラムコードの整合性ある自動抽象化による表明強化の支援

科学技術振興機構　ACT-I 専任研究者 / 国立情報学研究所　特任研究員　小林 努

Web ページ (Researchmap):

研究の概要

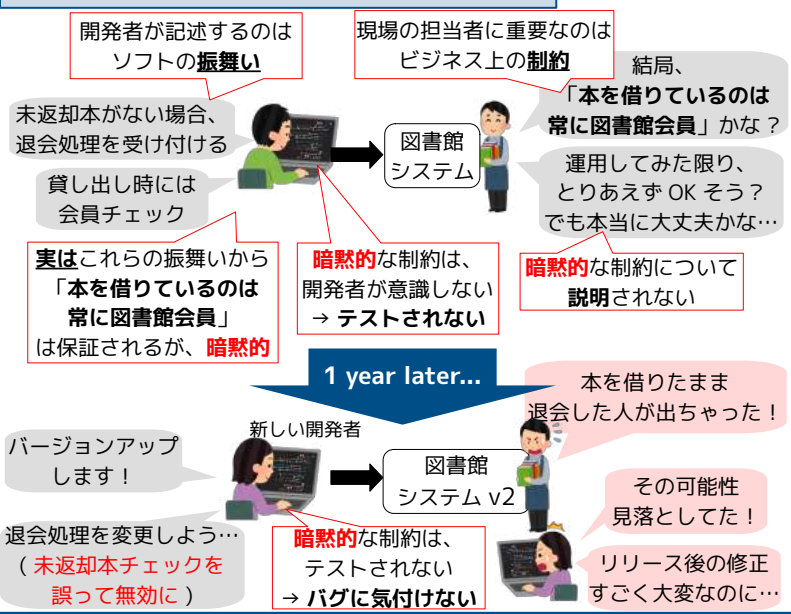
背景：ソフトウェアシステムのビジネスルール

- ソフトウェアシステムが現実世界で解決する問題は多様
  - 問題ごとに異なる文脈とルールがある

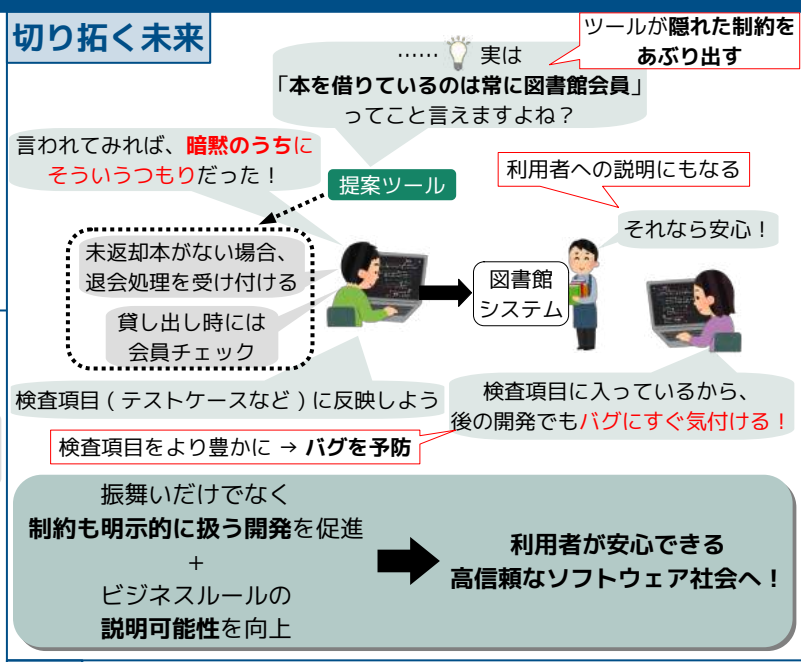
本を借りているのは常に図書館会員　ダブルブッキングが起こらない　A 部門の人が読めるファイルにファイル X の内容がコピーされることはない　…

きちんと考えないと、正しく作ったつもりでも望まぬ結果に…
- 文脈やルールの設計を中心とした開発手法が注目されている

課題：表に表れないビジネス上の制約



切り拓く未来



成果

ソフトの振舞いの本質を論理式で抽出したもの

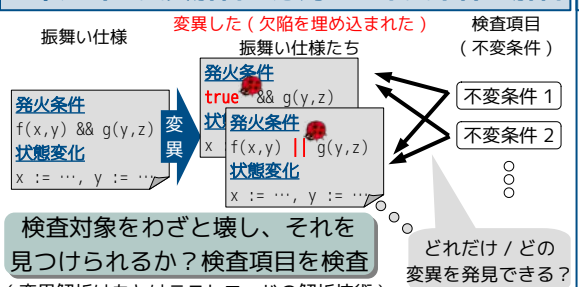
- ソフトの振舞いの形式仕様での表現に対し振舞いが常に満たす制約（**不変条件**）を自動で獲得する手法
  - 変異解析・自動修正問題として定式化
  - 論理式の性質を利用した変異操作を定義
  - 実装・事例研究
- プログラムコードと形式仕様の接続手法構築の試み

ビジネスルールの本質に焦点を当てる

ソフトウェア工学分野でホットな自動修正のアプローチ

成果の詳細

基本方針：変異解析を応用した不変条件の解析



（変異解析はもとはテストコードの解析技術）

式の強化操作・弱化操作

形式仕様記述言語 Event-B の全ての述語と式について操作を定義
- 述語を確実に強化（弱化）
  - **P∨Q を強化** … ⊥、 P 、 Q 、 P∧Q 、（強化版 P)∨Q 、…
  - **S⊆T を弱化** … T、（S の subset)⊆T 、 S⊆(T の superset)、…
- 集合の式を確実に拡張（縮小）
  - **S を拡張** …（全体集合）、 S∪(仕様に出現する同じ型の式)、…
  - **S から T への関数 を縮小** … ∅、（S の subset）から T への関数、S から（T の subset）への関数、S から T への全単射関数、…

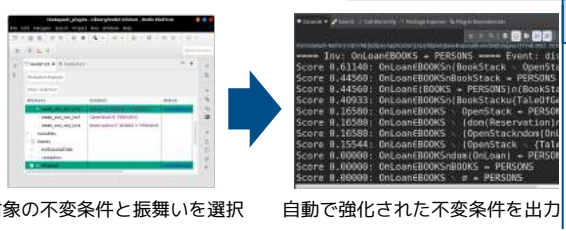
既存の変異解析手法よりも体系立った変異

実装・事例研究

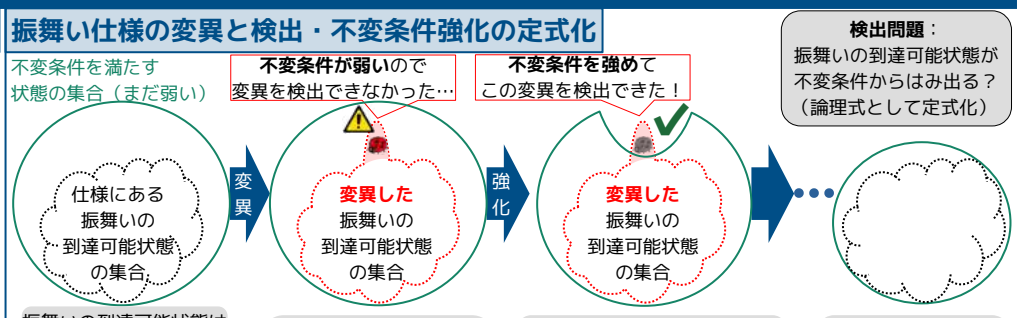
形式仕様記述言語 Event-B の開発環境 Rodin のプラグインとして実装

- フラッシュメモリ用のファイルシステムの仕様
- 水星探査プロジェクト BepiColombo の X 線分光計ソフトの仕様
- Ada プログラムコードから抽出された、衛星の姿勢・軌道制御システムの仕様

などに適用



振舞い仕様の変異と検出・不変条件強化の定式化



振舞いの到達可能状態は複雑で把握しづらい

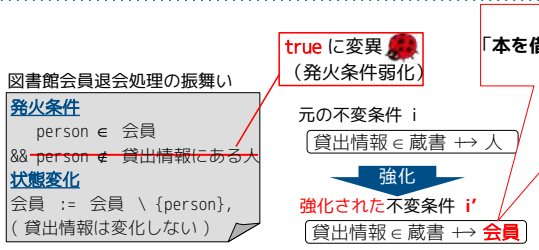
不変条件：振舞いの到達可能状態なら必ず満たす制約 → **振舞いを説明する性質**

到達可能状態が広がるような欠陥（発火条件弱化・状態変化拡張）を振舞いの仕様に埋め込む

元の振舞いの到達可能状態の満たす制約がより詳しく判明 → 振舞いの**「学習」が進んだ！**

最終的には振舞いにとても近く、しかも簡潔な制約の獲得を目指す

ポイントを突いて制約を強化・振舞いを説明



プログラムコードと形式仕様との接続の試み

- 「**ドメイン駆動設計**」で開発されたコードと Event-B 形式仕様との接続を模索
- ドメイン駆動設計のパターンと仕様上のパターンの対応を分析
  - アプリケーションサービス
  - ドメインサービス
  - …

エンジニアから注目されている、実用的かつビジネスルールを明示的に扱う設計手法