「CPS時代のソフトウェア高信頼化」に関する研究

On Achieving High Reliability of Software in the CPS-Era

中島　震　Shin NAKAJIMA
フランツ　ヴァイテル　Franz Weitl
橋本　祐介　Yu'usuke Hashimoto

何がわかる？

日常生活を支える社会基盤システムにソフトウェア技術が使われるようになりました。これに伴って、生産性向上・開発コスト削減といった従来の考え方が変わり、高い信頼性の確保に技術の研究開発が移ってきています。産業界と連携することで、形式手法と呼ぶ技術を実用化する方法を研究をしています。

どんな研究？

ソフトウェア開発の難しさは、対象システムが複雑で大規模であるという点にあります。システムの特徴を整理し簡明に表すことで、その正しさを系統的に確認する方法が必要です。前者についてはオブジェクト指向モデリングとの統合、後者については、モデル検査に代表される自動検証の方法を研究しています。

内容

産業界の取組みとの連携

ディペンダブルソフトウェア・フォーラム　(DSF, Dependable Software Forum)

参加企業：NTTデータ、富士通、日本電気、日立製作所、東芝、CSK

ソフトウェアの信頼性と安全性向上を目指す　ー　形式手法適用評価WG

CPS時代のソフトウェア工学　：　2010年度SSR（産学戦略的研究フォーラム）調査研究

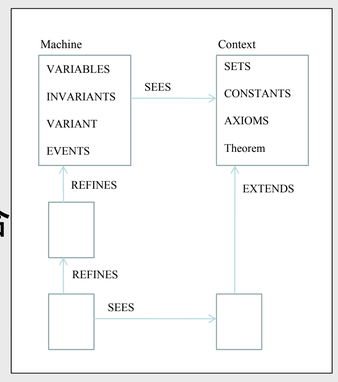
要求モデリングと検証

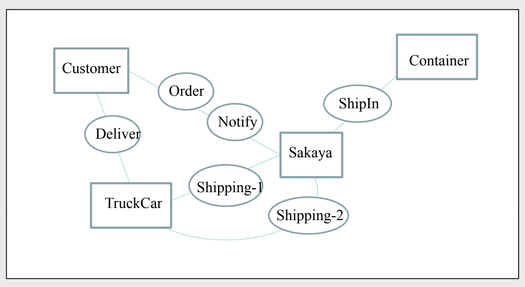
Event-Bを用いるガイドライン

ーオブジェクト指向モデリングとの統合

ーリファインメント計画シート

（superposition refinement）





Event-Bの振る舞い仕様検証

ー抽象化モデル検査

Cプログラム自動検査

ソフトウェア・モデル検査とモジュラー検証

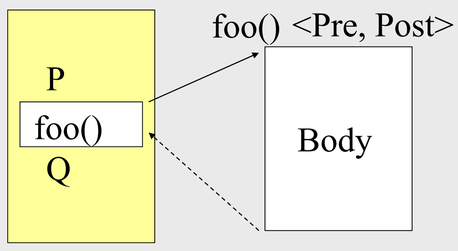
ー状態爆発の問題を避ける工夫

⇒　DbCと有界モデル検査を組み合わせる

ー関数へのポインタのDbCへの導入

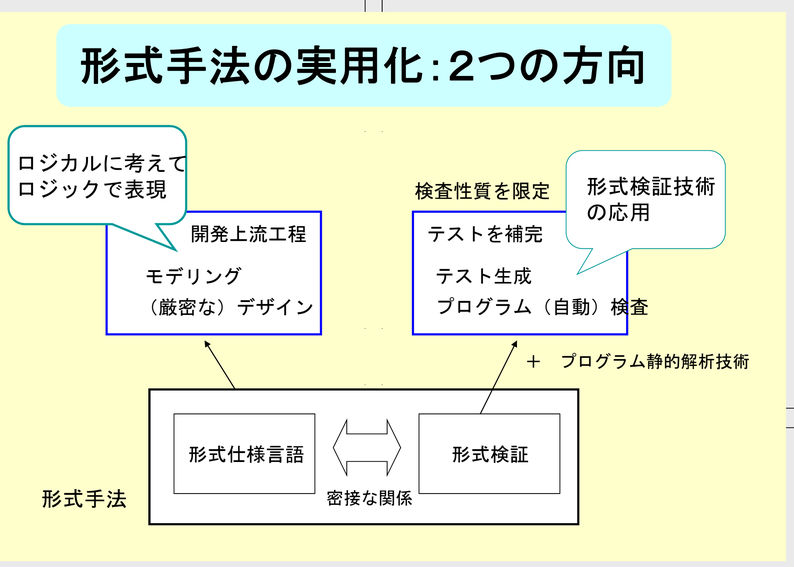
⇒　検査可能なCプログラムが広がる

（CBMCが扱えないプログラムも検査可能）



適用事例: MINIX

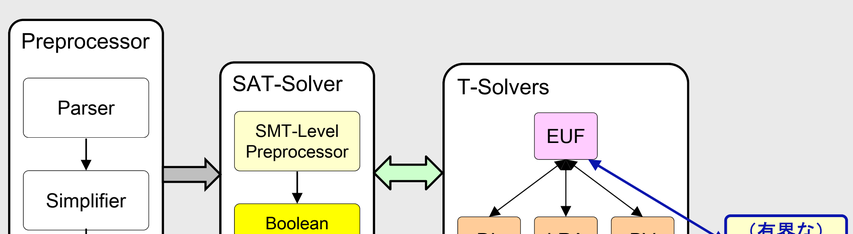
形式手法の実用化：2つの方向



自動検証エンジン

SMTソルバー（Satisfiability Modulo Theory）

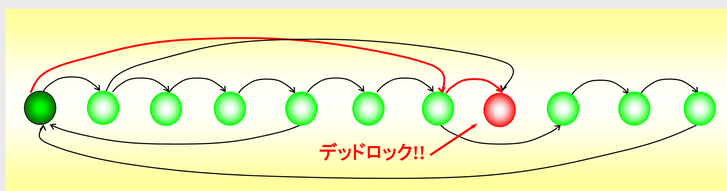
ーOpenSMT　をカスタマイズし「理論ソルバー」を組込み



総研大博士課程
学生募集中

2008年
→
←
2010年

「モデル検査法」（教科書）



連絡先：　中島 震（Shin　NAKAJIMA）／ 国立情報学研究所　アーキテクチャ科学研究系　教授
TEL：03-4212-2507　　FAX：03-3556-1916　　Email：nkjm@nii.ac.jp