ディペンダビリティ達成の道具としてのモデル検査法の研究

Model-Checking as a Tool for Achieving High Dependability

中島　震
Shin NAKAJIMA

何がわかる？

社会基盤システムのソフトウェアに対する依存度が高くなり不具合の影響が大きくなってきました。提供サービスや機能競争が激しく開発期間は短くなる一方です。限られた期間の中で大きな効果を得る新しいソフトウェア開発法の確立が緊急の課題になっています。本研究では、形式手法と呼ぶ技術をどのように使えば効果的であるかをあきらかにします。

どんな研究？

形式手法は設計仕様の厳密な表現の技術と自動検証の技術からなります。特に後者の代表であるロジック・モデル検査は実用的な方法として産業界でも関心が高まっています。本研究では、エンタープライズ系から組込みソフトウェアまでの多様なソフトウェアにモデル検査法を適用する方法を多面的に進めています。

内容

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

Correctness by Construction（CxC）技術　ー　数理論理に基礎をおくソフトウェア開発手法

産学連携フォーラム

「基盤ソフトウェア技術戦略の産官学協力委員会」提言

技術貢献

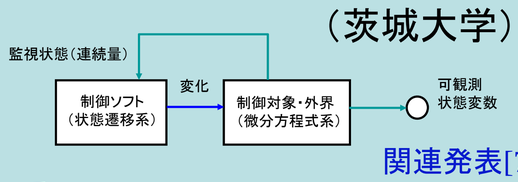
要求仕様の解析
- ー形式手法Event-B
- ーリファインメントによるモデリング（ナント大学）
- ー振る舞い仕様の検査：ランキング抽象

関連発表[2]

組込みソフトウェア適用ガイドライン
- ー経産省受託研究開発（三菱総研、他: 2008-）
- ー事例を通して適用ガイドラインを整理
- ー知識集積　→「SPINクックブック」へ

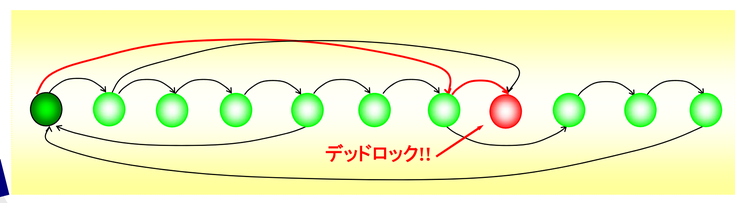
関連発表[8][9]

ハイブリッド系の表現と解析
- ー常微分方程式系との統合（茨城大学）



関連発表[7]

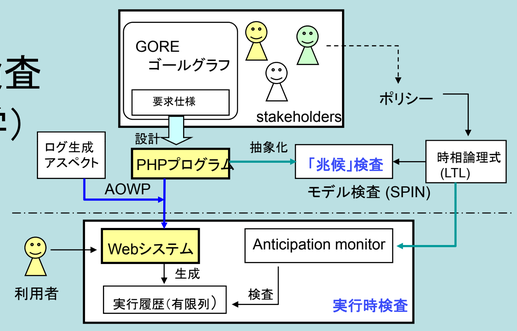
「モデル検査法」の展開



プログラム検査
- ーSpecification-based Testing (SBT)：事前・事後条件からのテスト生成（法政大学）
- ーModular Verification：DbCとモデル検査の組み合わせ（総研大中島研究室）

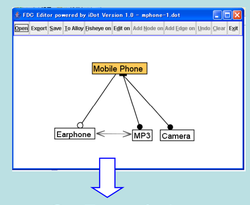
関連発表[3][5]

ポリシーの実行時監視
- ー要求ポリシーの2段階検査（オレゴン大学、東京大学）
- ーアスペクト指向AOWP（九工大）



関連発表[1][4]

形式手法＋SPLE
- ーFODAフィーチャダイアラグラム
- ーFD-Checker



形式定義　G : Formula in Propositional Logic

自動解析　$M \models G \wedge p$ Satisfiability Checking

関連発表[6][10]

最近の発表

研究論文

[1] K. Hokamura, N. Ubayashi, and S. Nakajima:: Aspect-oriented Programming for Web Controller Layer, APSEC'08, 2008年12月
[2] S. Nakajima and H. Kuruma:: Abstraction Aided Model Checking of Event-B Descriptions, IM_FMT'09, 2009年2月.
[3] S. Liu, T. Tamai and S. Nakajima:: Integration of Formal Specification, Review, and Testing for Software Component Quality Assurance、SAC 2009, 2009年3月.
[4] S. Nakajima, N. Ubayashi, and K. Hokamura：Runtime Monitoring of Cross-cutting Policy, Early Aspects at ICSE'09, 2009年5月.
[5] Y. Hashimoto and S. Nakajima：Modular Checking with Model Checking, SSV'09, 2009年6月, (to appear in ENTCS).
[6] S. Nakajima:: Constructing FODA Feature Diagrams with a GUI-based Editor, SEKE 2009, 2009年7月

解説・セミナー講演

[7] 中島震：形式手法の潮流ーアーキテクチャへの関心, システム/制御/情報, 9月号、2008年9月.
[8] 中島震：ソフトウェア工学からみたモデル検査法、回路とシステム軽井沢ワークショップ、2009年4月
[9] 中島震、石黒正揮：形式手法の概要とモデル検査法の応用、ESEC2009、2009年5月
[10] 中島震、鵜林尚靖：Alloy - 自動解析可能なモデル規範形式仕様言語、コンピュータソフトウェア、8月号掲載予定

NII　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