様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１８　日現在

機関番号：　１２６０８
研究種目：　基盤研究(C)（一般）
研究期間：　2012～2017
課題番号：　２４５００００９

研究課題名（和文）故障の計算モデルと解析手法

研究課題名（英文）Computational Model of Failure and Its Analysing

研究代表者
西崎　真也（Nishizaki, Shin-ya）

東京工業大学・学術国際情報センター・教授

研究者番号：９０２６３６１５

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：システム故障時（ハードウェア故障、ネットワーク不調等）における、ソフトウェアシステムの挙動を解析するためのソフトウェア検証技術・形式的開発手法の確立を研究目的とした。故障という現象をとらえた計算モデルを研究し、その計算モデルに基づき、モデル検査を応用することにより、故障時におけるシステムの挙動解析を研究し以下のような事項に取り組んだ。
①システム故障の計算モデル②その計算モデルから従来の計算モデルへの変換に基づく故障時の振る舞いの解析手法の提案③その解析手法を支援する検証システムの開発④計算モデルの定理証明システム上での形式化

研究成果の概要（英文）：The purpose of this research is development of formal method including system verification in order to analyze behavior of software systems in case of system faults. We studied formal computational model of system faults and its application using model checking, which enables us to analyze behavior of software systems in case of faults. Especially, our research was focused on the following points: (1) computational model of system faults; (2) formal analysis of behavior in case of system faults based on a translation of our fault model into a traditional computation model; (3) verification system supporting our analyzing method; (4) formalization using theorem proving.

研究分野：　プログラム言語理論

キーワード：　モデル検査　システム検証

１．研究開始当初の背景

数理論理学の枠組みを用いたソフトウェア検証・形式的開発手法は、長年にわたり研究が進められ近年では実用化され、産業界で利用される段階となった。特に、状態遷移図の網羅的な解析をおこなうモデル検査は研究が進み、目覚しい発展を遂げた。申請者はモデル検査の適用範囲を広げる研究を行ってきた。例えば下記のものがある。

（１）ブロードキャスト通信への応用

（２）CPU の速度に依存するシステム誤動作の解析

（３）情報システムにおけるコンプライアンス解析

（４）サービス拒否攻撃耐性の解析

（５）モデル検査を用いたソフトウェアの破壊検査

（５）「モデル検査を用いたソフトウェアの破壊検査」では、システムの一部を意図的に“破壊”して、全体の挙動をモデル検査により解析し、システムの頑強性を分析した。

また研究（２）では CPU 速度低下のような非正常動作の挙動の分析をおこなった。これらの経験から、ソフトウェアのバグや安全性上の脆弱性の発見のみならず、システムの故障時における挙動の解析の実現可能性に一定の見通しを得た。ただ、故障というものは、ハードウェアの停止の他に、ネットワークの障害などの外的要因や、停止にまでは至らないハードウェアの不調などもある。故障をシステム設計時に想定し、モデル化し従来のモデル検査システムを適用するには限界がある。故障というものをより網羅的にとらえるためには、モデル検査システムがもつ計算モデルが故障という挙動をとらえたものでなくてはならないという知見をえた。

２．研究の目的

故障の計算モデルの提案とそれに基づく故障に関するソフトウェア検証技術の確立を本研究の目的とした。具体的には次の項目に取り組んだ。

（ア）システムにおける故障に対して、計算モデルを与えた。
さまざまな種類の故障を分類し、それらをとらえるような計算モデルを与えた。

（イ）その計算モデルに基づく、故障時の振る舞いの解析手法の提案をおこなった。
前項で与えた計算モデルに対して、従来、モデル検査で用いられてきた有限オートマトン等の計算モデルへの変換を研究した。

（ウ）さらにその解析手法を支援する検証システムを開発することに取り組んだ。
前項で提案した解析手法に基づき、検証システムの開発に取り組んだ。具体的には、既存のモデル検査システムへのモデル変換システムを作成し、モデル検査の結果を、変換前のモデルに対する言明に逆変換するシステムを作成することを試みた。

（エ）FMEA や FTA のような信頼性工学の開発手法の形式化
FMEA（故障モード解析と影響解析）や FTA（フォールトツリー解析）のような信頼性工学の手法を、本研究課題で提唱する計算モデルに基づき、どのように形式化しうるのかということを考察した。

（オ）故障をとらえる計算モデルの定理証明システム上での形式化

３．研究の方法

・故障をとらえた計算モデルの確立

故障をとらえた計算モデルの確立に取り組んだ。計算モデルの基盤として、pi 計算や ACP(Algebra of Communicating Processes) のようなプロセス代数と多くのモデル検査システムで用いられている有限状態オートマトンの２つの枠組みを取り上げた。

・故障をとらえた計算モデルに基づく故障時の振る舞いの解析手法の提案

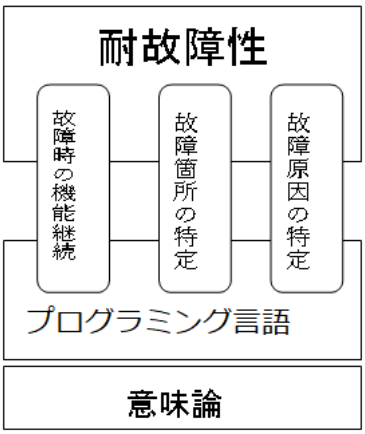
・解析手法を支援する検証システムの開発

前項の振る舞いの解析手法に基づき検証システムの開発をおこなう。プロセス代数ベースの計算モデル・有限状態オートマトンベースの計算モデルのいずれにおいても、バックエンドの推論システムとして、既存のモデル検査システムを位置づけ、フロントエンドには、前項の成果である計算モデルの変換システムを据える。そして、前項の成果を用いてバックエンドから出力される（モデル検査の）解析結果をフロントエンドで逆方向に変換し、ユーザーに表示する。
また、前項の成果を踏まえて実装する他に、Web ベースの対話的インターフェースを実現することにより、使いやすさについても配慮する。

・故障をとらえる計算モデルの定理証明システム上での形式化

主として、プロセス代数ベースの計算モデルについて、定理証明システム（例えば

Isabelle/HOL など）を用いて形式化する。定理証明システムによる形式化は、故障に関する形式的仕様記述の基盤技術となる。さらに、最近、定理証明システムは SAT などの推論エンジンを搭載しており、モデル検査システムで行うような網羅的探索を用いることが可能となっている。このことをふまえて、前項までで研究しているモデル検査における手法と定理証明システムを用いた形式化を統合するような検証手法についても研究をおこなう。



４．研究成果

・故障をとらえた計算モデル

故障をとらえた計算モデルを確立することができた。

・解析手法を支援する検証システムの開発

モデル検査を用いた検証システムのプロトタイプ段階のシステムについて一定の成果を得た。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計４件）

(1) Typed and Untyped Object Calculi with First-class Continuations, S. Nishizaki, R.Ikeda, International Journal of Software Engineering, 査読有 Vol. 1, pp.1-10, 2012

(2) Applying Model Checking to Destructive Testing and Analysis of Software System, H. Kumamoto,T. Mizuno, K.Narita, S.Nishizaki, Journal of Software, 査読有 Vol.8, No. 5, pp.1254-1261, 2013

(3) Let-Binding with Regular Expressions in Lambda Calculus, Takuya Ohata and Shin-ya Nishizaki, Journal of Software, 査読有, Vol.11, No.2, 220－229, 2016

(4) Simplification of Abstract Machine for Functional Language and Its Theoretical Investigation, S.Nishizaki, K.Narita, T.Ueda, Journal of Software, 査読有, Vol.10, No. 10, 1148-1159,2015

〔学会発表〕（計１９件）

(1) DoS Attack-resistant Framework for Client/Server Intelligent Computing, Shintaro Tabata, Shin-ya Nishizaki, ITC2012, LNEE, Springer, Vol.150, pp.47-53, 2012,

(2) Blog-Based Distributed Computation, Takayuki Sasajima, Shin-ya Nishizaki, LNCS, Springer, Vol.7473, pp.461-467, 2012,

(3) Formal Approach to Reliability Improvement with Model Checker, K.Yamada, S.Nishizaki, Proceedings, of ITC2012, LNEE, Springer, Vol.150, pp.15-24, 2012

(4) Formal Framework for Cost Analysis Based on Process Algebra, Shin-ya Nishizaki, Hiroki Kiyoto, ICCIP2012, CCIS, Springer, Vol.288, pp.110-117, 2012,

(5) Model Checking Approach to Real-time Aspects of Denial-of-Service Attack, Tatsuya Arai, Shin-ya Nishizaki, ICCIP2012, CCIS, Springer, Vol.288, pp.86-94, 2012,

(6) Model Checking of Broadcast Communication via Process Calculus, Ritsuya Ikeda, Shin-ya Nishizaki, AISS, Vol.4, No.17, pp.373-379, 2012,

(7) Modifiable Continuation in Object Calculus, Emiko Kuma, Shin-ya Nishizaki, WCTP2012, PICT, Springer, Vol.5, pp.150-173,2012

(8) Design of Open Equation Archive Server Resistant Against Denial-of-Service Attacks, Shin-ya Nishizaki , Hiroshi Tamano, AIM2012, CCIS, Springer, Vol. 296, pp.62-69, 2013

(9) Event-Driven Implementation of Layer-7 Load Balancer, Takayuki Sasajima, Shin-ya Nishizaki, Proceedings of IAIT2013, CCIS, Springer, Vol. 409, 162-172, 2013

(10) Formal Model of Time for Analyzing Denial-of-Service Attacks, S.Nishizaki, R.Ikeda, Intl. J. of Advancements in Computing Technology, Vol.5,No.7, pp. 580-588, 2013

(11) Process Calculus for Cost Analysis of Process Creation, Shin-ya Nishizaki, Mizuki Fujii, Ritsuya Ikeda, ITSE2012, LNEE, Springer, Vol.210, pp.33-44,2013

(12) Real-Time Model Checking for Regulatory Compliance, Shin-ya Nishizaki, Takuya Ohata, Proceedings of AIM2012, CCIS, Springer, Vol. 296, pp.70-77, 2013

(13) Strong Reduction for Typed Lambda Calculus with First-Class Environments, S. Nishizaki , Mizuki Fujii, Information Computing and Applications,LNCS,Springer,Vol. 7473, pp. 632-639, 2013

(14) Distributed Online Judge System for Interactive Theorem Provers, Takahisa Mizuno, S. Nishizaki, Proc. of ICASCE 2013, EPJ Sciences, Vol.68, Article No.:00016, 2014

(15) Formalization of Signaling System by Process Calculus, Yasuaki Ibayashi, Shin-ya Nishizaki, IERI Procedia, Elsevier, 160-168, 2014

(16) Incorporating First-order Unification into Functional Language via First-class Environments, Shin-ya Nishizaki, LNICST, Springer, Vol.117, pp.19-25, 2014

(17) Effect system with control capturing, Shohei Matsumoto, Shin-ya Nishizaki, Computer Science and Application (Proc.of CSA 2014),CRC Press, 219-223, 2015

(18) Translation Style Semantics and Type System of Control Capturing, Shohei Matsumoto, Shin-ya Nishizaki, Proc of ISRME 2015, Atlantis Press, 1271-1278, 2015

(19) Formal Performance Analysis of Web Servers using an SMT Solver and a Web Framework, T. Kimura and S. Nishizaki, Proceedings of CSA 2016,De Gruyter,195－204, 2016

〔図書〕（計０件）

〔産業財産権〕

○出願状況（計０件）

○取得状況（計０件）

〔その他〕
特になし

６．研究組織
(1)研究代表者
西崎　真也（NISHIZAKI, Shin-ya）
東京工業大学・学術国際情報センター・教授
研究者番号：９０２６３６１５

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者

なし