様式 C-7-2

自己評価報告書

平成２３年３月３１日現在

機関番号：１２１０２
研究種目：基盤研究（Ｂ）
研究期間：2008～2011
課題番号：20300001
研究課題名（和文）　記号計算の理論を駆使したウェブソフトウェアのモデル化と検証

研究課題名（英文）　Modeling and verification of web software based on theories of symbolic computation

研究代表者　井田　哲雄（IDA TETSUO）
筑波大学・大学院システム情報工学研究科・教授
研究者番号：70100047

研究分野：情報科学
科研費の分科・細目：情報科学・ソフトウェア
キーワード：ソフトウェア検証，記号計算，ウェブ

１．研究計画の概要

ウェブソフトウェアには従来にない高い信頼性が要求される．単に誤りなく動作するだけでなく，頑健である，悪用・誤用されないといった性質がウェブソフトウェアに求められる．このような「健全性」を保証するには従来の開発手法やデバッグ手法だけでは不十分であり，産業界や学術研究機関で新たな方法論の構築や方法論を支援する言語やツールの開発が進められている．

本研究では，記号計算の理論，形式言語・オートマトン理論をはじめとする，コンピュテーションやソフトウェアを形式化する様々な理論を駆使して，上記問題の解決に取り組んでいる．具体的には，定理証明支援系やモデル検査系を用いた方法論の高度化と広範な展開が重要課題であると考え，これまで定理証明支援系を用いたソフトウェアや幾何オブジェクト設計の正当性証明の研究を推進してきた．それと同時に，記号計算を支援するウェブサービスのシステムやサーバーサイドの記号計算アルゴリズムをクライアント（ブラウザー）から対話的にアクセスするウェブソフトウェアを構築してきた．

これらの先行するあるいは同時に進展させている研究で私達が得てきた知見や経験及び記号計算の研究コミュニティーが蓄積してきた多くの知見をウェブソフトウェアの「健全性」の検証に活用して，新たな計算理論，方法論，および方法論を支援するツール群を構築している．

２．研究の進捗状況

ウェブソフトウェアのモデル化と検証に様々な角度から取り組んでいるが，研究活動は次の３点に集約することができる．以下に，研究の進捗状況の概要を述べる．具体的な成果は，公表した論文を参照されたい．

（1）プログラムの性質を表す論理式を動的に生成し，生成された論理式の正しさを証明する研究を推進している．特に，シリンダー代数分解やグレブナ基底計算法の応用研究を行った．グレブナ基底計算の単項順序を工夫することにより，幾何学的な証明問題が効率よく行われることが判明したので，多くの実例についてこれを実証するとともに，ウェブプログラムに対して，応用の方策を検討した．現在，これらの方法を安全面でクリティカルなコード内に存在するループや，文字列探索のプログラムの検証に適用するとともに，定理証明支援系との連携を試みている．

（2）ウェブソフトウェアの開発で用いられる代表的スクリプト言語である PHP および Ruby の意味論の研究を行った．PHP については，その特徴となる参照代入に注目し，その意味論をグラフ書換として定式化し，現行の実装の問題点を明らかにした．また，Ruby については，そのオブジェクト言語機能を表現する操作的意味論を構築した．この操作的意味論に基づき，プログラムの制御フローを識別するコントロールフロー解析手法を開発した．

（3）文字列解析によるウェブプログラム検証の実用性を高める研究に取り組んでいる．特に，スクリプト言語のプログラムにおいて重要な役割を果たす正則表現マッチングの研究を重点的に行った．多くのスクリプト言語が採用している欲張り戦略による実装の意味をモナド

の概念を用いて定式化し,マッチングに精密に対応する出力付きオートマトンを構成する方法を与えた.出力付きオートマトンを用いることで,文字列解析の精度を高めることができた.

（4） XML 文書の効率的な文書変換に関する研究を推進した． XML 文書と変換規則との効率の良いマッチングアルゴリズムを,より広いクラスの変換規則に適用することを目指している.ヘッジではなくシーケンスに関する正規表現から検討を開始し，POSIX 準拠のマッチング及び欲張りマッチングの両方について,効率的なマッチングアルゴリズムの設計を完了している.現在は,欲張りマッチングに対するアルゴリズムの正当性の検証を行っている.

３．現在までの達成度

概要に示した研究活動について，着実な研究成果が生み出され，権威ある国際雑誌と国際会議において公表されている．また，研究活動の進展とともに，ソフトウェアツールが製作され，その成果が目に見える形で蓄積されている．以上のことから，本研究は,「おおむね順調に進展している」と評価できる.

４．今後の研究の推進方策

本研究が目標とするのは深い理論に基づくウェブソフトウェアの解析である．理論の展開には，あらかじめ設定した目標はあるものの，短期に完結できる性質のものではない．また，国際的な研究の広がりを持つために，研究目標は常に見直しが必要である．対象とするウェブソフトウェアそのものも，技術革新がめざましいため，研究対象が，広がる傾向がある．本研究が４年間の計画の基に推進されていることに鑑みて，次年度末に達成できる目標を再度明確にし，研究全体として，当該分野の学術の進展にどのような形で貢献ができているのかを確認する作業を行うとともに，分担者相互の連携を高め，分担者が個々に行っている研究を総合的にまとめる作業も行っていく.

５． 代表的な研究成果

〔雑誌論文〕（計４件）

① Ida. T, Kasem. A, Ghourabi. F, Takahashi. H, Morley's theorem revisited: Origami construction and automated proof, Journal of Symbolic Computation, vol. 46, pp. 162-170, 2011, 査読有

② Tetsuo Ida and Hidekazu Takahashi. Origami Fold as Algebraic Graph Rewriting. Journal of Symbolic Computation, 45(4):393 - 413, 2010.

③ 松本宗太郎, 南出靖彦, Ruby プログラムの制御フロー解析とその健全性の証明, 3 巻, pp. 9-25,2010.査読有

④ Taro Suzuki, Staoshi Okui, Product Drivatives of Regular Expressions, IPSJ Online Transactions, 1 巻, pp.53-65,2008, 査読有

〔学会発表〕（計５件）

① Kasem. A, Ghourabi. F, Ida. T, Origami Axioms and Circle Extension, Proceedings of the 26th Symposium on Applied Computing (SAC 2011),pp. 1106-1111, March 23, 2011, Tunghai University Taiwan

② Tozawa, M. Tatsubori, T. Onodera, Y. Minamide, Copy-on-Write in the PHP Langauge,Proc.of the 13th International Conference on Programming Languages, pp.200-212, Aug 23, 2009,Lyon, France

③ Tetsuo Ida. Symbolic and Algebraic Methods in Computational Origami: Invited Talk. In Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation (ISSAC 2009), pages 3-4. ACM, December 16-18, 2009,Hawaii, USA.

④ Tetsuo Ida, Hidekaza Takahashi, Origami Fold as Algebraic Graph Rewriting, Proc. of 24th annual ACM Symposium on Applied Computing, pp. 1132-1138, March 12, 2009, Hawaii, USA

⑤ T. Nishiyama, Y. Minamide, A Translation from the HTML DTD into a Regular Hedge Grammar, Proc. of 13th International Conference on Implementation and Application of Automata, pp. 122-131, July 21, 2008, California, USA