H20/B11 推論エンジンを用いたプログラム自動検証法の研究(1節 共同プロジェクト研究の理念と概要, 第4章 共同プロジェクト研究)

雑誌名	東北大学電気通信研究所研究活動報告
巻	15
ページ	260-262
発行年	2009-08
URL	http://hdl.handle.net/10097/48440

共同プロジェクト研究

課題番号　Ｈ２０／Ｂ１１

採択回数	①	２	３

推論エンジンを用いたプログラム自動検証法の研究

［1］組織

代表者：小川　瑞史
（北陸先端科学技術大学院大学）
対応者：大堀　淳
（東北大学電気通信研究所）
分担者：岩沼　宏治（山梨大学）
鍋島　英知（山梨大学）
関　浩之（奈良先端科学技術大学院大学）
浅井　健一（お茶の水女子大学）
岩崎　英哉（電気通信大学）
高橋　孝一（産業技術総合研究所）
広川　直（北陸先端科学技術大学院大学）
Li Xin（北陸先端科学技術大学院大学）

研究費：物件費０円、旅費 25 万円

［2］研究経過

プログラムの高信頼化の研究・開発は、近年ますますその重要性を増している。本プロジェクトでは自動推論技術や推論エンジンの実装を用いてプログラム検証に適用することを目的として研究を行った。

本プロジェクトは、本年度が第１年度であり、以下、研究活動状況の概要を記す。主な活動は研究集会ならびに共同研究（代表者と対応者間）のための研究セミナーを各１回行った。なお参考文献は査読付（またはそれに準じるもの）のみをあげる。

A. H21 年１月８日（木）～9 日（金）に研究集会を東北大学電気通信研究所で開催した。発表リストならびに概要は以下の通りである。

１月８日（木）

1. 岩沼宏治（山梨大）Towards Efficient Equality Computation in SOLAR

概要：結論発見システム SOLAR における効率的な等号推論の実現の考察と提案を行なった。まず初めにボトムアップ型定理証明における等号調整法と、その順序制約と Basic 法による効率化について概説し、次にトップダウン型定理証明法における効率的な等号計算の困難さを考察した。SOLAR はトップダウン型定理証明法の一種である Connection Tableaux を基礎としているため、等号計算に関して同様な難しさを内在する。トップダウン型定理証明の等式計算の効率化法として、Brand の Modification 法、Bachmair 他による weak ordering 制約をもつ Modfication 法が有名である。Modification 法は、前処理によって証明対象となる節論理式を変型することで、等式の各種の性質を予め埋め込む手法である。Paskevich は weak ordering 制約付き Modfification 法を、Connection Tableaux に効果的に埋め込んだトップダウン型等号計算体系を提案している。しかし、modification 法は等号対称律を論理式に埋め込むため、一つの論理式から一部のみが違う複数の式を生成する必要があり、変換生成した式は一般に巨大になる。殆どが重複した複数の論理式は、様々な冗長計算を発生させ好ましくない。本講演では、等号対称律を論理式に埋め込まず新しい推論規則を導入して、等号対称性の保証が行なえる計算体系の提案を行なった。

2. 広川直（北陸先端大） KBO Orientability

概要：Knuth-Bendix 順序は関数記号の優先順位と実数上の重み付けをパラメータとする順序である。本発表ではこの順序による停止性問題が有限の命題論理式で記述可能であることを示した。さらにこの順序を用いた停止性の自動検証ツールは、SMT ソルバを用いることで極めて容易に実装でき、実行速度も既存のアルゴリズムに比べ優れていることを実験により示した。（論文投稿中）

3. 岩崎英哉（電通大）遅延評価型関数プログラムにおける再帰データ構造の Thunk の再利用

概要：遅延評価では、関数適用式の評価時に各引数の評価を遅延させるため、Thunk と呼ばれるデータ構造がヒープ内に割りあてられる。実行時オーバーヘッドが大きい Thunk の量を減らすことは、関数プログラムの効率化に極めて重要である。本発表では、すでに割りあてられた Thunk の再利用のための静的解析を提案する。具体的には、リストの tail 部にある Thunk への参照を単一とするプログラム変換を施し、 Thunk の安全な破壊的更新による再利用を行う。提案アルゴリズムを Glasgow Haskell Compiler（GHC）に試験的実装し nofib ベンチマークにより評価した。その結果、メモリ消費量と実行時間について有望な結果を得ることができた。

[1] 田村知博、高野保真、岩崎英哉: 純関数型言語の処理系における効率的な枝刈り機構の実装、情処学会論文誌プログラミング、1(2), pp.28--41, 2008.

4. 増子萌、浅井健一(お茶の水女子大) MinCaml コンパイラにおける shift/reset の実装

概要:限定継続を扱う命令である shift と reset を Power PC の機械語レベルで実装法を提案し、実際に MinCaml コンパイラに組み込んでベンチマークを実行したときの状況について発表した。

[2] 増子萌、浅井健一: MinCaml コンパイラにおける shift/reset の実装、第 11 回プログラミングおよびプログラミング言語ワークショップ論文集 pp. 163-177, 2009.

5. 山本雅洋、大堀淳(東北大) 変数の生存区間解析のため SAT ソルバを用いた型推論アルゴリズム

概要:コード最適化問題の一つである最適レジスタ割付け問題は、レジスタを変数に割付けるのではなく、変数の生存区間に対し割付ける必要がある。従来の枠組みでは、生存期間はフローグラフに対する彩色問題などグラフ論的な手続きにより定義されていた。本発表では、生存区間の宣言的記述となる型システムと型推論アルゴリズムを報告する。この型システムは、変数型はプログラム中の変数定義の部分集合、型推論規則は変数定義の到達可能性の推論規則を表現する。このとき各変数の生存区間は論理制約を満たす最小解に対応し、SAT の最適化問題である MIN-ONE に帰着する。最後に、提案手法と OptSAT アルゴリズムを用いた実装を報告する。

[3] 山本 雅洋、大堀 淳: 変数の生存区間解析のための SAT ソルバを用いた型推論アルゴリズム、第 11 回プログラミングおよびプログラミング言語ワークショップ PPL2009.

[4] 上野雄大、大堀淳:制御フローの合流のための計算系、情報処理学会論文誌 プログラミング(PRO), 1(3), pp. 19–33, 2008.

6. 高橋孝一(産総研) マーキングアルゴリズムの抽象化による検証について

概要:Deutsch-Schorr-Waite マーキングアルゴリズムはポインタを操作するプログラムであり、正しさが自明ではない。我々は、μ計算を用いた抽象化を行うことによって、比較的コンパクトかつ高速に検証することに成功した。検証は、Agda を使った対話的証明と、我々が開発したμ計算の充足可能性の自動決定器の両方を組み合わせて行った。

[5] Yoshinori Tanabe, Toshifusa Sekizawa, Yoshifumi Yuasa, Koichi Takahashi: Pre- and Post-conditions Expressed in Variants of the Modal mu-calculus, IEICE Trans. on Information and Systems, Special Section on Formal Approach, Vol.E92-D, No.5, pp.995-1002, May. 2009.

[6] Toshifusa Sekizawa, Yoshinori Tanabe, Yoshifumi Yuasa, Koichi Takahashi. MLAT: A Tool for Heap Analysis based on Predicate Abstraction by Modal Logic. The IASTED International Conference on Software Engineering (SE 2008).

[7] Yoshifumi Yuasa, Yoshinori Tanabe, Toshifusa Sekizawa, Koichi Takahashi: Verification of the Deutsch-Schorr-Waite Marking Algorithm with Modal Logic. 2nd Int. Conf., Verified Software: Theories, Tools, Experiments (VSTTE 2008), LNCS 5295, pp.115–129, 2008.

1 月 9 日(金)

7. 関浩之(奈良先端大) Multiple Context-Free Grammar and Its Application

概要 : Multiple Context-Free Grammar(MCFG)は、CFG の自然な拡張であり、CFG より真に大きく、CSG より真に小さいクラスである。MCFG は、空判定問題や所属問題の判定可能性、言語演算に対する閉包性など、CFG の良い性質を保存している。本発表では、MCFG の定義と諸性質を概観した後、M モデル検査への応用について述べる。具体的に、LTL モデル検査が可能となるよう、MCFG の無限系列言語の生成モデルへの拡張について考察する。

[8] 高田喜朗、王静、関浩之: 実行履歴に基づくアクセス制御の形式モデルと検証、電子情報通信学会論文誌 J91-D (4), pp.847-858, 2008.

[9] Yuki Kato, Tatsuya Akutsu, Hiroyuki Seki: A Grammatical Approach to RNA-RNA Interaction Prediction, Pattern Recognition, 42, pp.531-538, 2009.

[10] Yoshiaki Takata, Hiroyuki Seki: Formal Language Theoretic Approach to the Disclosure Tree Strategy in Trust Management, IEICE Trans. Information and Systems, E92-D, 2, 2009.

[11] Yuki Kato, Tatsuya Akutsu, Hiroyuki Seki: Dynamic Programming Algorithms and Grammatical Modeling for Protein Beta-Sheet Prediction, J. Computational Biology, to appear.

[12] Yuki Kato, Tatsuya Akutsu, Hiroyuki Seki: Prediction of Protein Beta-Sheets: Dynamic Programming versus Grammatical Approach, 3rd IAPR Int. Conf. on Pattern Recognition in Bioinformatics (PRIB 2008), 2008.

8. 南出靖彦(筑波大) Checking the Balancedness of a Context-Free Language in Polynomial Time

概要 : 括弧から成る文字列を生成する文脈自由文法

が与えられたとき、その文法が生成する文字列で括弧のバランスがとれているかを判定する問題は、ソフトウェア検証などにも応用されている基礎的な問題である。既存のアルゴリズムが指数関数時間であったのに対し、本研究ではPlandowskiによるSLPと呼ばれる特殊な文脈自由文法の等価性を多項式時間で判定するアルゴリズムを応用することで、この問題に対して多項式時間判定アルゴリズムを与えた。

[13] T. Nishiyama, Y. Minamide: Translation from the HTML DTD into a Regular Hedge Grammar, 13th Int. Conf. on Implementation and Applications of Automata, LNCS 5148, pp. 122-131, 2008.

9. 小川瑞史（北陸先端大）Antichain for VPA model checking

概要：Visibly Pushdown Automaton (VPA) は括弧言語を受理可能な有限オートマトンの拡張であり、しかも有限オートマトン同様なブール演算の閉包性をもつため、包含問題（モデル検査）が決定可能である。しかしその計算量は $O(2^{n^2})$ と困難であり、過去において数状態以上を解く実装は存在しなかった。本発表では、計算の融合と極小化のアイデアを用いたantichainアルゴリズムをP-オートマトンの手法を用いてVPAに対し拡張した。その実装・実験により従来手法に比べ劇的な改善を示し、実用的な有効性の可能性を示した。（論文投稿中）

B. H21年2月27日（金）に研究セミナーを東北大学電気通信研究所で行った。セミナーの内容は以下の通りである。

Li Xin（北陸先端大）A Scalable Stacking-based Context-Sensitive Points-to Analysis for Java

概要：Javaは動的なメソッド呼出をもつため、文脈依存解析の基礎となるメソッド呼出グラフの生成自体が自明ではなく、points-to解析が必要となる。本発表では、on-the-flyな重み付プッシュダウンモデル検査によるJavaのpoints-to解析の定式化、およびその実装・実験について述べる。実装は、Javaの前処理としてSOOT（中間言語Jimpleへの変換系）、バックエンドモデル検査エンジンとしてWeighted PDSライブラリを用いるが、単純な実装では2000メソッド以上の処理は困難であった。本実装では分割モデル検査を組み合わせることで10000メソッド超のWebアプリケーションの処理が可能となることを報告する。（論文準備中）

なお、このセミナー（午前）をもとに同日午後においては、SML# コンパイラへの適用可能性を主に活発な討論を行った。

［3］成果

（3－1）研究成果

初年度であり、本研究プロジェクトの直接の研究成果はないが、本プロジェクト参加メンバーによる近年（本年度を含む）の研究成果について研究集会と研究セミナーと行い、それぞれの研究成果を用いた共同研究の可能性についてキックオフを行った。

その結果、通研側対応者の大堀研で進めているSML#コンパイラにおける最適化の定式化や実装において、プッシュダウンモデル検査を用いる検討を開始している。従来のプッシュダウンモデル検査は主に手続きに対し適用させており、関数型言語であるSMLに適用するには高階関数のプッシュダウンモデルなどの検討が必要である。当面、既に解法が知られているreference解析を対象として、適用可能性を評価する。

（3－2）波及効果と発展性など

本プロジェクトの研究成果はいまだではあるが、組織横断的・分野横断的な研究メンバーによる研究集会により、具体的な共同研究課題が討議された。これにより、現在のstate-of-the-artの手法、ならびに分野横断的な問題の交換がなされ、新しい研究領域の開拓（萌芽的研究の発見）に結びつき、今後の発展が期待されている。

特に、形式言語における理論的成果であるプッシュダウンオーマトンの拡張・決定アルゴリズム等をツール実装を含め、現実のSMLなどプログラミング言語の高信頼化・最適化に応用については、研究集会後、さらに研究セミナーを開催し、具体的な共同研究の可能性をさらに深く探索した。

また開催した研究集会・研究セミナーにおいては、大堀研学生（東北大）、浅井研学生（御茶ノ水女子大）、小川研助教・ポスドク（北陸先端大）など若手研究者の発表が半数を占め今後の進歩が期待されている。

［4］成果資料

初年度であり、直接的な研究成果はないが、研究集会・研究セミナーにおける研究交流のもととなる資料を［1］の報告にあげた。