様式 C-19

科学研究費補助金研究成果報告書

平成２１年５月２１日現在

研究種目：基盤研究　（C）
研究期間：２００７～２００８
課題番号：１９５００２１
研究課題名（和文）　コード言語の最適化技術と検証技術を統合する証明システムの研究

研究課題名（英文）　A Study on Proof System That Combines Verification and Optimization Technologies

研究代表者 大堀　淳（OHORI ATSUSHI）
東北大学・電気通信研究所・教授
研究者番号：60252532

研究成果の概要：直観主義的論理学の自然演繹証明システムとラムダ計算との同型関係を拡張・一般化し，機械語コードの証明論を完成し，コードの最適化やコードの検証をより体系的に行う基礎を構築した。この証明論では，機械語コードは，左規則のみからなるある種のシーケント計算として表現され，その操作的意味，すなわち，コードを実行する機械の状態遷移規則は，シーケント計算のカット除去定理の証明から系統的に抽出することができる。さらに，この証明システムは，低レベルコードのアクセス権限の検証や制御フロー遷移の最適化などの基礎となることが示された。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	600,000	180,000	780,000
２００８年度	2,600,000	780,000	3,380,000
年度			
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウエア
キーワード：プログラミング言語，コード最適化，コード検証，証明論

１．研究開始当初の背景

プログラミング言語技術から見た今日の情報システムの際立った特徴は，インターネットを介した実行コードの動的な取り込みと利用である．この機能によって，通信網の壁を越え，インターネット上の資源を動的に共有し連携することが可能となっている．しかしながら，その基礎をなすコードの動的なリンクと実行の基礎は十分に確立しされているとは言えず，その結果，インターネットを介したプログラムの多くは，最適化や効率化が不十分でかつ種々の脆弱性を含む信頼性の低いものとなっているのが現状である．種々の言語が併存する環境下でのコードの効率的な利用と安全性の検証を系統的に行う基盤技術の確立は，安全で効率よいユビキタスコンピューティングを実現する上での鍵である．しかしながら，そのような基盤技術は，従来の単一言語を仮定して積み重ねられてきたプログラミング言語処理系の実装技術やプログラムの検証技術では十分に実現できない．

この問題は，近年，プログラミング言語の研究者の関心を集め，コード共有に関する安全性検証の研究が盛んに行われている．代表的なものにＮｅｃｕｌａとＬｅｅによるＰｒｏｏｆ－Ｃａｒｒｙｉｎｇ－Ｃｏｄｅ，Ｓｔａｔａ とＡｂａｄｉによるＪａｖａバイ

トコードの型の検証システム，Ｍｏｒｒｉｓｅｔｔ等によるＴｙｐｅｄ　Ａｓｓｅｍｂｌｙ　Ｌａｎｇｕａｇｅなどがある．これらの研究は，プログラム理論や型理論の考えを用いて，既存のコードが満たすべき安全性の性質を書き下し検証する試みである．このアプローチは，個々のコードに関する検証システムの構築としては有効であるが，低レベルのコードの効率的な利用と安全性の検証に関する系統的な枠組みを与えるには至っていない．

本研究では，コードの最適化と検証を統一的に扱う論理学的枠組みの確立とそれに基づく最適化と検証技術の構築を目指す．そのような論理学的枠組みが構築されるならば，Ｃｕｒｒｙ－Ｈｏｗａｒｄ同型関係に基づくラムダ計算の型理論が高信頼言語の設計や型主導コンパイルを通じた効率化の実現に大きく貢献したように，低レベルコードに対しても，その安全性の検証やより効率的なコードへの最適化などを系統的に行う技術の確立が可能になると期待される．

本研究が確立を目指すコードの証明論的基礎とそれに基づくコードの最適化やコードの検証の理論は，それ自身，これまでの考え方とは異なる新しいアイデアに基づく独創性の高いものである．さらに，本研究では，これら基礎理論を通じて得られるコード言語に対する一般的な証明システムを基礎とし，より実用的で強力なコード生成や検証の実現を目指す．それによって達成されるコード処理系の安全性と効率を高める処理系構築技術は，大量で大規模な情報システムを安定・安全に運用するための新しいサステナブルな技術の一つの核となりうるものである．さらに，本研究が確立を目指すコード言語の論理学的基礎は，コードの検証や最適化にとどまらず，システムの自律技術，ソフトウエア安全化技術，ソフトウエア構成技術，モニタリング技術等と深い関連を持っており，システムレベルでの，一般的で強力な論理学的な枠組みへの幅広い研究へと発展する可能性を持つ．

２．研究の目的

本研究の一般的な目的は，機械語コードそのものの論理学的解釈を基礎とし，コードの利用や，最適化，検証などを統一的に行うことを可能にする系統的な枠組みを構築することである．特に，コンパイラが行うコード生成の最適化とコードリンク時に必要とされる検証を統一的に扱う論理学的枠組みの確立と，それに基づく最適化と検証技術の構築を目指す．そのような論理学的枠組みが構築されるならば，Ｃｕｒｒｙ－Ｈｏｗａｒｄ同型関係に基づくラムダ計算の型理論が高信頼言語の設計や型主導コンパイルを通じた効率化の実現に大きく貢献したように，低レベルコードに対しても，その安全性の検証やより効率的なコードへの最適化などを系統的に行う技術の確立が可能になると期待される．

この一般的な目的を達成する第一歩として，本研究実施期間では，機械語コードの証明論を完成させ，それを基礎として，コードの利用や，最適化，検証などを統一的に行うことを可能にする系統的な枠組みの構築を目指す．さらに，構築されたコードの証明論を基礎とし，コード生成やコード最適化技術およびそれらの正しさの検証技術の構築を試みる．これらは，ラムダ計算の型理論が果たしたと同様に，低レベルコードに対しても，より効率的なコードへの最適化やその正しさの検証などを系統的に行うことを可能にすると期待される．この目的を達成するために，本研究では，まず機械語コードに対するシーケントスタイルの証明システムの完成とその諸性質を確認し，それに基づきコード生成や，コード検証，コード最適化の系統的方法を分析する．

３．研究の方法

本研究の目指す論理学的アプローチの技術的根拠および見通しを，機械語コードのための論理学的解釈に求めることができる．この解釈によって，Ｃｕｒｒｙ－Ｈｏｗａｒｄ同型関係の考え方を機械語コードに適用し，機械語コードそのものを論理学の証明システムとして表現することが可能となる．この研究の過程で，論理学の証明論の枠組みを用いてコードの最適化およびその動作の検証を行うことが可能である，との洞察を得た．報告者はさらに，この洞察の下に，コードの生成・最適化およびコードの検証の一連の研究を行い，以下のような結果を得た．

- 機械語コードの証明システムの証明変換により新しいレジスタ割り付け方式を構築できる．
- 機械語コードの証明論的解釈の考え方を用いることによって，コード最適化の基礎として使われている SSA 変換を型として表現可能である．
- Java バイトコードに対する証明システムを構築することにより Java バイトコードの静的なアクセス制御が実現可能である．

これら研究の過程で，本研究が目指す研究につながる以下の重要な洞察を得た．

- 検証と最適化は相補的であり，これらを統合することにより，より強力な枠組みを構築可能である．
- コードの証明論的解釈はコード最適化と検証の双方を表現可能である．

本研究は，これまでの研究成果を，以上の

新しい見方で洗練・発展させ，コードの検証と最適化という従来はまったく違ったものと捉えられていたものを統合することにより，コード操作のためのより一般的な枠組みの構築を目指す新しい試みである．

本研究の実施期間では，この中長期的な研究の第一歩として，以下の具体的課題の解明を目指す．

① コードの最適化変換の証明論的解釈

コード最適化はコードの実行の効率化である．したがって，コード言語の証明論的解釈に従えば，カット除去プロセスの効率化と捉えられるはずである．そこで，まず，カット除去プロセスの静的分析を行い，コード最適化を，カット除去プロセスの複雑さを減少させる証明変換と捉え，この見方を基礎として，種々の最適化を表現可能な証明簡約関係の導出を試みる．

② コード検証機構の証明論的解釈

コード検証は，型システムなどのコードに対する静的な整合性解釈が不可能であることを通じて検出される．そこで，コード検証にて検出の対象とする``望ましくないコード''の緒性質を証明論的に特徴付ける証明図の静的解釈の枠組みの構築を目指す．

③ 両者を統合したより一般的なコードの証明論

コードの証明システムをオブジェクトレベル，コードの検証システムをメタレベルとしてもつ２階層からなるコードの証明論を構築し，前２者を統合した体系の構築を目指す．

④ コンパイラ等への応用のためのアルゴリズムとその実装方式

以上のコードの最適化と検証の証明論的な枠組みを実際のコード言語の最適化や検証に応用するためのアルゴリズムや実装方式の構築を目指す．

４．研究成果

2007 年度は，本研究の一般的な目的である機械語コードの論理学的解釈を基礎としたコードの利用や，最適化，検証などを統一的に行うことを可能にする系統的な枠組み構築の基礎となる機械語コードの証明論を完成させた．この証明論の枠組みでは，機械語コードは直感主義的論理学の証明論の一つである，ある種のシーケント計算系の証明とみなすことができ，機械語コードの実行はシーケント計算系のカット除去のプロセスに対応する．さらにこのカット除去プロセスは，カット除去定理の証明から系統的に抽出することができる．この対応から，高水準言語からの機械語コードへのコンパイルは，自然演繹システムからこの証明システムへの証明変換として系統的に与えられ，さらに，機械語コードに対応する証明を自然演繹システムの証明に変換することによって，機械語コードを，ソース言語を参照することなしに，高水準言語に変換する可能性が与えられる．これら結果は，コードの最適化やコードの検証の論理学的な基礎を与えるものである．これら結果の一部は，プログラミング言語の分野で最も権威と影響力のある国際論文誌ＡＣＭ　ＴＯＰＬＡＳに発表された．

2008 年度は，2007 年度に完成させた機械語コードの証明論及び以前の研究成果であるコンパイルの論理学的基礎を，コード生成システムに応用する研究を行い，制御フローの合流を取り扱うための計算系と，その計算系から導出される中間表現を構築した．従来の関数型言語の中間表現として使用される継続渡し形式や A-正規形などでは，条件分岐後に制御フローを合流する機構が含まれていないため，条件式などを機械的に翻訳すると，分岐の後に続く計算が各分岐に複製されてしまう．この問題は，それら中間表現に対応する計算系に，分岐後の制御フローの合流に相当する規則を追加することで解決できるはずである．本研究では，この洞察に基づき，論理和に関する規則を左規則が唯一の上式を持つように変更したシーケント計算を構築し，その結果から，制御フローの合流を取り扱うことができるコンパイラの中間表現とその型システム，およびラムダ計算からこの中間表現への効率の良いコンパイルアルゴリズムを導いた．この成果は関数型言語の実用的なコンパイラのより系統的な実現を可能にするものである．

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３件）

① 上野雄大，大堀淳，型代入を遅延する最適化型推論アルゴリズム，コンピュータソフトウェア，２５，１０１－１１３，２００８，（査読有）

② 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)，１，１９－３３，２００８，（査読有）

③ Atsushi Ohori，A Proof Theory for Machine Code，ACM Transactions on Programming Languages and Systems，29 (6)，２００７，(査読有)

〔学会発表〕（計０件）

６．研究組織

(1)研究代表者

大堀　淳（OHORI ATSUSHI）
東北大学・電気通信研究所・教授
研究者番号：60252532

(2)研究分担者

なし

(3)連携研究者

なし