ソフトウェア開発方法論

Software Development Methodology

（プロジェクト番号：JSPS-RFTF 96P00504）

プロジェクトリーダー
片山　卓也　　北陸先端科学技術大学院大学・情報科学研究科・教授
コアメンバー
二村　良彦　　早稲田大学・理工学部・教授
米崎　直樹　　東京工業大学・情報理工学研究科・教授
米澤　明憲　　東京大学大学・情報学環・教授

1. 研究目的

現代の社会は大規模で高度なソフトウェアによって支えられており、今後の社会の進展やIT 化などによりそのような社会基盤となるソフトウェアに対する要求が益々強くなると思われる。本プロジェクトでは計算機科学の最新の研究成果をとり入れ、科学的・形式的手法にもとづくソフトウェア開発方法論を、次の４点に焦点をあてて研究を行なうことである。

（１）発展的ソフトウェア開発方法論（片山グループ）
（２）ソフトウェア開発アルゴリズム（二村グループ）
（３）ソフトウェア開発における形式化技術と環境（米崎グループ）
（４）開放性をもつ並行・分散ソフトウェア（米澤グループ）

２．研究成果概要

（１）発展的ソフトウェア開発方法論

・オブジェクト指向ソフトウェア開発方法論の上流工程に焦点をあて、分析モデルを形式的に記述し、それらを統合・実行するシステム、統合モデルの一貫性を定理証明システムによって検証するためシステムなどからなるオブジェクト指向分析環境を実現した。このような一貫した開発環境は世界でも最初のものであり、複雑なソフトウェアを高信頼に構築するためには非常に有用なツールである。
・ソフトウェアの進化や発展はソフトウェアライフサイクルで最も困難かつコストのかかる過程であり、その合理的解決が望まれているが、その科学的な基礎が確立されていない。本研究では、代数的束による発展原理を発見すると共に、抽象解釈にもとづく新しい発展メカニズムを得た。これにより、ソフトウェアの進化・発展問題の科学的解決に大きな貢献をした。

（２）ソフトウェア開発アルゴリズム

プログラム自動生成のためのプログラム高速化実験システム WSDFU（Waseda Simplify-Distribute-Fold-Unfold，ウスドゥフ）を開発した。それは、実測値として最高１億倍以上の自動高速化を達成した。しかも、多くの場合、自動高速化はパソコンを用いても瞬時（1分以内）に行える。このような桁違いの高速化を自動的に行うソフトウェアの開発は世界初である。既存の他システムでは実行不可能な16 種類のベンチマークテストを行い、WSDFUの強力さを国際的にアッピールした。これにより、プログラム自動生成システムの実用化可能性を示すことができた。

（３）ソフトウェア開発における形式化技術と環境

多くのミッションクリティカルシステムでは、時間の扱いが極めて重要であるが、本研究では、時間に関する論理学の最新の成果を用いたシステムの仕様化の技術とそのための環境を構築した。すなわち、

・時間論理のクラスに対する検証系や、線形論理、適切さの論理について、仕様記述を目的として様々な体系を得た。
・仕様の差分と以前のステップでの検証結果から、差分を反映した仕様の検証結果を効率的に得る方法を得た。
・状態爆発を抑制した高速検証エンジンについては、プレステートと呼ばれる技術を発明し、状態展開の先読みを行うことにより、無駄な状態展開を押さえた効率的検証エンジンを構成した。
・入力制約式と呼ばれる、仕様が実現可能であるために必要なイベント入力に関する最弱前提条件を求める方法を部分計算として用いて、モジュール化された仕様に対する効率的な検証技術を開発した。
・これらの成果を集約して検証システムとして実現し、これまで検証不可能であった実際的システムの仕様について検証実験を行い有用性を示した。

（４）開放性をもつ並行・分散ソフトウェア

・安全なモバイルソフトウエアの構築基盤となる、２種類のプログラム言語系、JavaGo および MobileML を設計し、その処理系を実装した。JavaGo 言語系は、従来のモバイル計算記述用言語では難しかった、より現実的で柔軟なモバイル計算を可能にするために、「透明な移動」の機構および「移動する部分/しない部

分」の指定を行う機構を組み込んでいる。また、処理系は極めて性能が高く、ネットワーク上を移動しながらソフトウエアをインストールするシステムなど、有用性および新規性の高い応用プログラムの実現を可能にした。

・モバイルソフトウエアの理論的基盤をなすプロセス計算の枠組みにおいて、新規性の高い型システムを考案した。この型システムによって、プロセス間のメッセージのやりとりにおいて、デッドロックを少なくしたり、受け手プロセスが誤返答や二つ以上の返答により、送り手プロセスを混乱させるなどの現象を、静的な検査により防止することが可能となった。また、型システムに通信回数の情報を導入し、冗長な通信の除去などの最適化が可能となった。

３．結論

研究を行った４つの課題、（１）発展的ソフトウェア開発方法論、（２）ソフトウェア開発アルゴリズム、（３）ソフトウェア開発における形式化技術と環境、（４）開放性をもつ並行・分散ソフトウェア、のいづれに関しても、世界的に見ても一流の成果が得られた。本研究成果は、学術的にも大変良質のものであると同時に、実用的面からもソフトウェア開発を科学的ベースに乗せるための基盤になり得るものである。

主な発表論文

1. Takuya Katayama: Evolutionary Domain-A Sound Basis for Software Evolution, International Workshop on Principles of Software Evolution 2001, pp.1-6, 2001
2. 青木利晃,立石 孝彰,片山卓也,定理証明技術のオブジェクト指向分析への適用,コンピュータソフトウェア,18 巻 4 号,pp18-48, 2001
3. 二村良彦,小西善二郎,一般部分計算法に基づく自動プログラム変換実験システムの開発,コンピュータソフトウェア,18 巻 0 号,pp60‐77,2001
4. 萩原茂樹,友石正彦,米崎直樹,有限フレームを意味的基礎として持つ様相論理に対する分解証明法,コンピュータソフトウェア,１８巻０号,pp78‐91,2001
5. Tatsuro Sekiguchi, Hidehiko Masuhara, Akinori Yonezawa, A Simple Extension of Java Language for Controllable Transparent Migration and its Portable Implementation, Springer Lecture Notes in Computer Science, 1594 pp211‐226,1999
6. Naoki Kobayashi, Quasi-Linear Types, Proceedings of ACM Conference on Principles of Programming Languages (POPL'99), pp29‐42,1999