審 査 の 結 果 の 要 旨

氏　　名　　小 林　 努

ソフトウェアシステムの信頼性向上という目標のためにソフトウェア工学で広く研究されているのが,形式的モデルによる仕様記述及びその段階的詳細化によるソフトウェア実装である．ここでは，(1) 詳細化の各段階の正しさ（主に模倣関係の構築によって保証される），及び (2) 最初に用いる形式的モデルの正しさ，これら2つのことを証明することで,段階的詳細化の結果として得られるプログラムコードの正しさが結論される.以上のアプローチは B-method 等の形式仕様記述手法として具現化され産業界においても広く用いられるが，一方で仕様として用いる形式的モデルの構築の難しさ（対象とするソフトウェアシステムのすべての側面を表現する包括的なモデルでなければならない）が課題として認識されている．ゆえに最近は（前述のモデルからコードへの詳細化に加えて）抽象的なモデルからより具体的なモデルへの詳細化の過程にも注目が集まっており，そのようなモデルの詳細化をサポートする形式仕様記述手法として Event-B が提案され，研究及び応用が進みつつある．本論文の貢献はこの Event-B に関するものである.

Event-B に関する既存研究の多くは,抽象的モデルを詳細化して包括的モデルを得ることを目的とするものであった．これに対する本論文の新奇な着眼点は，詳細化の過程それ自体（「詳細化構造」）の再利用及び保守が応用上重要であるというものである．たとえば語彙の大幅な増大をもたらす詳細化の一ステップは,可読性を損なうばかりか模倣関係による正しさの証明を難しくし，さらに（システムの一コンポーネントを切り出して他のシステムの一部として用いるといったような）モデルの再利用の際の障害にもなりうる.プログラムコードの保守の分野において研究される諸手法に着想を得た本論文では，上記の課題に対して (1) Event-B モデルの詳細化構造のリファクタリング手法，(2) Event-B モデルの詳細化構造の計画の計算機支援，(3) 上記2つの手法の適用のために必要な情報の獲得のための方策，これら3つの貢献がなされる.

以下，論文の構成に即して，本論文の貢献についてより詳細に述べる.

第1章では形式仕様記述手法という背景とモデル詳細化構造の再利用・保守という課題,

及びリファクタリングと計画という本論文のアプローチについて概説がなされる．第2章では Event-B のフォーマリズムを手短に導入したのち，第3章では Event-B における変数と述語が明示的なものと非明示的なものに分類できることを示して，この分類を用いて本論文の技術的貢献（すなわちリファクタリングと計画）のアイデアを説明している．

第4章では本論文の主な貢献の一つである詳細化構造のリファクタリング手法が導入される．ここでは詳細化構造 $M_n, M_{n+1}, \ldots, M_m$（$M_i$ と M_{i+1} の間に一段階の詳細化が施されている）と変数の集合の列 $E_s, E_{s+1}, \ldots, E_t$ を入力として，後者のように変数を用いるような新たな詳細化構造 $M'_s, M'_{s+1}, \ldots, M'_t$ を得ることが目的となる．詳細化の各段階でどの変数を用いるべきかは所与であるため，それに応じてスライシングによって用いる述語を取捨選択するが，この際にもともとの詳細化構造において各段階の詳細化の正しさの証明に必要な非明示的な述語が失われてしまいかねない．本論文ではこのような述語を補完的述語と呼び，これを論理学における Craig 補間によって求める手法を提案している．

第5章では詳細化構造の事前計画の計算機支援に関する本論文の貢献が述べられる．ここでは（詳細化構造の最終到達点たる）包括的モデルに現れるべき述語と変数（及び変数同士の相互関係）を入力とし，目的のモデルに至る詳細化構造の候補を生成することが目的となる．このような候補は一般に多数考えられるが，(1) （経験的に）良い詳細化構造が満たすべき性質によるフィルタリング，(2) 生成した詳細化構造の候補の適切な可視化，(3) ユーザーが候補を取捨選択する対話的ワークフロー，これらの方策によって有用な詳細化構造の獲得を支援する手法が本章で提案される．

第6章では以上の2つの手法についてケーススタディが示され，手法の有効性が主張される．特にリファクタリングについては，詳細化の大きな一段階を複数の小さな段階に分割することで詳細化の正しさの証明が容易になる例と，リファクタリングによってモデルの一部の再利用が可能になる例，これら2つの例が示される．

第7章では第4-5章の2つの手法について，その入力の一部，具体的には変数や述語の間の相互関係について（これはモデル自体に直接は記述されない情報である），これらをどのようにモデルから抽出するかが議論され，いくつかの方策が提案されて，ケーススタディが示される．これが本論文の主要な貢献の3つ目である．

以降，第8章では本論文の貢献について，特にその利点と限界について再度検討が行われ，第9章でさらに関連研究が議論されたのち，第10章で結論と将来の研究課題が述べ

られる.

以上のように Event-B における詳細化構造の保守・再利用という新たな課題を特定し，そのための手法を提案して，その有効性を実装・ケーススタディによって確認した本論文は，日々大規模化するソフトウェアの高信頼化という社会的課題（及び既存のソフトウェア資産の再利用というパラダイム）に対してその貢献が大であると評価できる.

以上により本論文は博士（情報理工学）の学位請求論文として合格と認められる.