論文の内容の要旨

Assume-guarantee 検証手法は，モデル検査によるコンポーネントベースソフトウェアの検証に有望なアプローチとして認識されている．Assume-guarantee 検証手法は，コンポーネントベースソフトウェアの検証に適しているだけではなく，モデル検査における状態爆発問題の解決への可能性を持つ．Assume-guarantee 検証手法を使うことで，検証の対象をコンポーネントに分解し，検証の対象を別々にモデル検査することが可能となる．一般的なモデルベース検証手法，特にシステムの assume-guarantee 検証手法は，システムの振る舞いを記述するモデルに対して行われる．そのため，検証手法を適用する前にシステムの振る舞いの正確なモデルを得る必要がある．しかし，これらの手法はモデルとモデルの正当性を得る方法が利用可能であることを一般に仮定している．これは，モデルベース検証手法が研究中のシステムの振る舞いを記述するモデルの有用性と正当性を仮定することを意味する．それにもかかわらず，この仮定はモデル化の誤りやバグ修正のために常に成立するわけではない．加えて，既存 CBS のコンポーネントの進化は，ソフトウェアライフサイクルの中で避けることのできないタスクであるとされている．したがって，仮定が成立しても，振る舞いの追加や削除によりソフトウェアが進化するとき，モデルは無効になるかもしれない．不幸なことに，これらのタスクの結果，進化したソフトウェアは，全体を再度検査されなければならない．

本研究の目的は，コンポーネント進化におけるコンポーネントベースソフトウェア進化のモジュラー検証への効果的なアプローチを提供することである．改良が適応されてコンポーネントが進化したとき，提案フレームワークはモデルの更新と進化したシステム全体の再検査のために進化したコンポーネントとモデルに焦点を合わせる．本フレームワークでは，モデルの更新とモジュラー検証のプロセスで必要となる手順の数を減らすため，進化したコンポーネントの以前のモデルと検証結果を再利用する．

本論文には，三つの主な貢献がある．一つ目の貢献は，コンポーネントベースソフトウェアの assume-guarantee 検証のための最小仮定を生成する手法の提案である．本提案手法は，L*-based 仮定生成手法を改良したものである．本手法の重要なアイディアは候補となる仮定の検索空間から，最小の仮定を見つけることにある．これらの仮定は，コンポーネントが性質を充足し，システムの他の部分が充足されるために必要となる環境と見なされる．提案手法により生成される最小仮定は，より少ない計算コストでシステム全体の再検査に利用することができる．

二つ目の貢献は，設計段階のコンポーネントの進化におけるコンポーネントベースソフトウェアの assume-guarantee 検証のための効果的なフレームワークの提案である．本フレームワークでは，あるコンポーネントのモデルが進化するとき，既存コンポーネントの多くのモデルと進化したコンポーネントのモデルを再度検査する必要がない．フレームワークでは，進化したモデルが進化前システムの仮定を満たすかを検査すれば良い．進化したモデルが仮定を満たすとき，進化したコンポーネントベースソフトウェアは性質を満たしている．一方，進化したモデルが満たすには仮定が強すぎる場合，新しい仮定が生成される．我々は新しい仮定の生成に「assumption regeneration」と「minimized assumption regeneration」の二つの手法を提案する．これら手法では，より低い計算コストで新しい仮定を再生成するために以前の検証結果として現在の仮定を再利用する．

本研究の三つ目の貢献は，ソースコードレベルでのコンポーネント進化におけるモジュール適合テストとコンポーネントベースソフトウェアの assume-guarantee 検証のフレームワークの提案である．このフレームワークには，進化したコンポーネントの不確かな更新したモデルのモジュール適合テストと進化したコンポーネントベースソフトウェアの assume-guarantee 検証の二つの段階がある．コンポーネントが進化したとき，提案フレーワークはモデルを更新して進化したシステム全体を再検査するため，コンポーネントとモデルに着目する．また，本フレームワークはモデルの更新と assume-guarantee 検証のプロセスに必要となる手順の数を減らすため，進化したコンポーネントの以前の検証結果と以前のモデルを再利用する．

キーワード: 検証，モデル検査，assume-guarantee reasoning，assume-guarantee 検証，モジュール検証，コンポーネント進化，適合テスト，learning algorithm，仮定，コンポーネントベースソフトウェア.