振舞仕様の検証方法に関する研究

松本 充広

北陸先端科学技術大学院大学 情報科学研究科

1998 年 2 月 13 日

キーワード： 並行分散システム，代数仕様，検証法，詳細化，項書換えシステム.

本研究の目的は，並行分散システムに対する，従来の検証方法の問題点を明らかにし，その問題を解決した検証方法を提案することである．

並行分散システムは，複数の計算主体がお互いに通信しあうことで計算が実行されるシステムである．このようなシステムは，可能な状態，状態遷移が膨大で，信頼性を確保するためのテスト数は膨大になる．論理検証は，論理レベルのバグを発見でき，テストに比べ，コストが低い．従って，テストの一部を論理検証に置き換えることで，開発コストの削減を期待できる．このため，プロセス代数の分野で，この論理検証の方法が盛んに研究されている．しかし，大抵のプロセス代数は，抽象データ型を記述できないため，データフロー解析を行なえない．代数仕様の一分野に，プロセス代数を，抽象データ型を扱えるように一般化した，振舞意味論がある．本研究では，この振舞意味論に基づく従来の検証方法の問題点を明らかにし，その問題を解消した検証方法を提案する．なお，振舞仕様は，振舞意味論に基づいて記述した仕様のことである．

振舞意味論では，並行分散システムをブラックボックスと見なす．そして，システムの状態を取得するオペレータ（属性）と，システムの状態を変更するオペレータ（操作）とを使って，システムの振舞いを記述する．システムはブラックボックスなので，何回かの操作で変更した状態を，属性で取得することでしか，内部状態を認識できない．この操作と属性の実行が，観測である．なお，内部状態が等しいかどうか（振舞等価）は，全ての観測結果が等しいかどうかで決める．

この振舞等価の検証方法として，余帰納法と，文脈長帰納法とがある．余帰納法は，検証する時に，人間が隠蔽合同という関係を与えなければならない．しかし，この関係を用いることで，大抵の場合，文脈長帰納法より効率的に検証を行なえる．なお，従来は，隠蔽合同の性質が明らかでなかったため，常に余帰納法が効率的だと信じられていた．

振舞等価の検証は，項書換えシステムに基づく検証系で行なう．本研究では，まず，検証系で扱える隠蔽合同で，検証に役立つものは，振舞等価しかないことを示した．

観測手段の間には，観測結果が必ず等しい等の関係を持つものがある．つまり，冗長な観測手段がある．検証に使われる隠蔽合同は振舞等価なので，従来の隠蔽合同の選択は，実は，冗長な観測手段を除去することで得られる観測手段の集合の選択に，他ならない．本研究では，振舞仕様の等式を，観測手段間の等式と見なすことで，この冗長な観測手段を見つけだし，適切な観測手段の集合の選択を機械的に構成する方法，テスト集合余帰納法を提案する．なお，テスト集合余帰納法で，全ての冗長な観測手段が除去される振舞仕様の十分条件も，明らかにする．同時に，必要な観測手段が可算無限個になり，余帰納法と文脈帰納法とが一致する振舞仕様の例も構成する．

振舞等価検証の応用として，振舞仕様間の段階的詳細化がある．これを，振舞仕様を満たす実装の制限と捉えた研究に，Goguen 博士，Malcolm 博士の研究がある．しかし，彼らの研究は十分ではない．彼らの方法を，スタックを，アレイとポインタを使って構成したスタックへ詳細化する例で説明する．彼らは，まず元になるスタックの振舞仕様を与える．次に，アレイとポインタの振舞仕様を元に，その合成方法を振舞仕様で記述する．最後に，この合成方法を記述した振舞仕様が，スタックの振舞仕様を満たすことを検証する．振舞意味論では，振舞仕様の記述を，ブラックボックスの記述と考える．しかし，彼らは，最後の検証の所で，振舞仕様の記述を，データ構造の記述として扱っている．つまり，合成した振舞仕様に対応するブラックボックスの状態に，必ず，アレイやポインタの状態が対応すると仮定している．しかし，合成した振舞仕様に対応するブラックボックスの状態の中に，アレイやポインタの状態と対応づけられない状態が存在する．実際，振舞等価の定義に基づいて検証すると，合成した振舞仕様は，スタックの詳細化になっていないことが示せる．

本研究では，射影オペレータを導入し，これを用いて振舞仕様の合成を記述する方法を提案する．なお，この方法で記述した振舞仕様のことを，オブジェクト指向仕様と呼ぶ．オブジェクト指向仕様では，射影オペレータを用い，合成した振舞仕様の状態と，合成する振舞仕様の状態とが対応するように仕様を記述する．このため，彼らの方法の問題は，生じない．

射影オペレータの研究は，二木研の飯田等との擬射影オペレータの研究（共同研究では，これを射影オペレータと呼んでいる）が基になっている．共同研究では，擬射影オペレータを用いた，動的システムの仕様記述，検証方法の研究を行なった．なお，本論文では，私の行なった，擬射影オペレータの定義，検証方法についてのみ記述する．

射影オペレータは，擬射影オペレータとは異なり，振舞仕様を合成する時に，観測手段を制限することが出来る．例えば，擬射影オペレータを使って，アレイとポインタとを合成すると，単に合成したものが出来るが，射影オペレータを使って合成すると，スタックが出来る．これは，射影オペレータが，ポインタより下のセルの中見しか見えないように，観測手段を制限するからである．このように，段階的詳細化のために仕様を合成する時には，射影オペレータの観測手段を制限する性質は，重要な働きをする．

以上まとめると，本研究で提案した方法で，従来の検証方法の問題点を解消することが出来た．