3J-05

形式的ソフトウェア部品生成のための実装抽出手法

叶野 英俊 †
電気通信大学情報理工学部総合情報学科

織田 健 ‡
電気通信大学情報理工学研究科総合情報学専攻

1 はじめに

形式手法の１つとして、B Method がある。B Method のモデルと実装を細分化し部品として整備することで再利用性を高めることができ、高信頼な新規ソフトウェアを低コストで作成することが可能となる。しかし、細分化されたモデルに対応する実装の部品の機械的な抽出手法は提案されていない。本研究では、モデルと実装間の制約から変数の対応関係を特定することで、細分化モデルを満たす実装の操作の機械的な抽出手法を提案する。

2 研究背景

2.1 形式手法 B Method

形式手法は数学的基盤に基づく記述によりソフトウェアの仕様記述、開発、検証などを行う手法である。B Method は形式手法の１つであり、仕様記述からコード生成までの一連の過程を支援する [1]。B Method は仕様を抽象的に記述したモデルと、モデルとの整合性を保ちながら詳細化した実装を用いる。モデルと実装の変数の関係はリンク不変条件として実装上に記述される。

2.2 先行研究

ソフトウェアの開発コストの増大や信頼性の低下という問題の解決法の１つとして既存ソフトウェアを部品化し再利用するという方法が研究されている。B Method のソフトウェア部品生成の概念図を図１に示す。部品化に関して、三鍋らはモデルの一部を一定の基準により切り分け部品として整備するモデル細分化手法を提案している [2]。また、中村はモデル細分化により作られた細分化モデルのふるまいと等価な部分を実装から抽出し細分化実装を作る、実装抽出を提案している [3]。

2.3 先行研究の実装抽出における課題

2.3.1 手順の曖昧さ

先行研究では実装抽出の方針は記述されているが、「代入文を手がかりに式を特定する」などの曖昧な記述が多く、機械的な実装抽出には至っていない。

2.3.2 複雑な制約条件を持つ実装の実装抽出

実装はモデルとの整合性が保たれる限りどのような書き方をしても許される。モデルの変数が集合や数値である場合、リンク不変条件は複雑にはならないが、変数が写像である場合、リンク不変条件は複雑な形になる場合が存在する。先行研究ではリンク不変条件が単純な形のみしか扱っておらず、複雑な記述に対応できていない。

An Implementation Extraction Method for Formal Software Components Generation

†Hidetoshi Kano, The University of Electro-Communications Department of Informatics

‡Takeshi Oda, The University of Electro-Communications Graduate school of Informatics

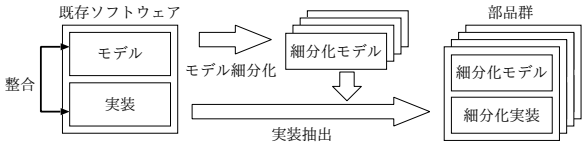

図 1: 部品生成概念図

2.3.3 モデルと実装の条件分岐の対応

モデルと実装の操作で用いる IF 文等の条件分岐の構造は、モデルと実装で異なった構造をとることがある。しかし先行研究ではモデルと実装で条件分岐の構造が一致している場合にしか対応していない。

3 機械的抽出を考慮した実装抽出手法

前述の課題を解決した実装抽出手法を説明する。

3.1 変数の対応付け

まずリンク不変条件によりモデルと実装の変数の関係を特定する。ここで特定したモデルの変数に対応する実装の変数群をリンク変数と呼ぶ。

具体的な手順は以下の通りである。

1. モデルの変数を１つ選択し、リンク不変条件から選択したモデルの変数を含む条件を全て抽出する。
2. リンク不変条件から定義域、値域の制限、減算の部分を取り除く。
3. モデル変数を複数含むリンク不変条件を除去する。
4. 最終的に残ったリンク不変条件に出てくる実装変数群がリンク変数となる。

3.2 条件分岐の対応特定

モデルと実装の操作に条件分岐が含まれる場合、モデルの代入文に対応する実装の代入文が実装のどの条件分岐に存在するかの情報が必要となる。ここで、モデルと実装の条件式の形が異なる場合を考慮し、リンク変数を利用し条件分岐内の代入文の対応をとることでモデルと実装の条件分岐の対応関係を特定し、モデルの代入文が実装のどの条件分岐に存在するかを特定する。

3.2.1 条件代入文群の探索

条件分岐の条件 P が真のとき、その条件に対し１回の操作で実行される一連の代入文群を P の条件代入文群と定義する。モデルと実装の全ての条件分岐パターンに対して条件代入文群を作成する。

図 2 を例とすると、このモデル操作 op の条件分岐パターンは P と not(P) の 2 パターン存在するため、これらの 2 つの条件に対して条件代入文群を作成する。

3.2.2 対応特定

3.2.1 節で作成したモデルの条件代入文群が実装のどの条件代入文群に対応しているかを特定し、その対応からモデルの代入文が実装の条件分岐のどこに存在するかを特定する (図 3)。具体的な手順は以下の通りである。

Copyright ©2018 Information Processing Society of Japan.
All Rights Reserved.

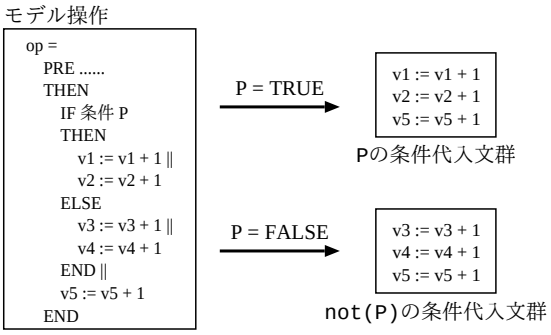

図 2: 条件代入文群の探索

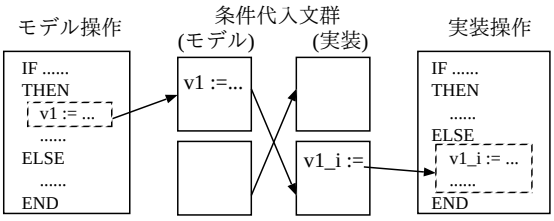

図 3: モデルの代入文と実装の条件分岐の対応

1. モデルの条件代入文群の左辺を見て、そのリンク変数を左辺に持つ実装の条件代入文群が対応する。
2. 手順１で対応が取れない場合、モデルの条件代入文群の右辺の変数、定数を見て、そのリンク変数や同じ定数を持つ実装の条件代入文群が対応する。
3. 条件代入文群の対応から、モデルの代入文が実装の条件分岐のどこに存在するのかを特定する。

3.3 非決定的値生成、参照操作の作成

モデルの操作に非決定的値が含まれる場合、モデル細分化の際に非決定的値を生成する操作 (非決定的値生成操作) と生成した値を用いて代入を行う操作 (非決定的値参照操作) の 2 つを作成する。ここでは、モデルの操作と同様に実装の値生成操作と値参照操作を作成する。

3.3.1 非決定的値に対応する実装の式の特定

モデルに非決定的値が存在する場合、まずは実装における非決定的値に対応する式を特定する。

モデルと実装でふるまいが同じであると証明できるためには、モデルの非決定的値と実装の式の対応が明示されている必要がある。多くの場合、その対応関係は戻り値への代入という形で記述されている。そのため、モデルで非決定的値が代入されている戻り値に実装で代入されている式が非決定的値に対応する実装の式となる。

3.3.2 非決定的値生成、参照操作の構築

次に、値生成操作と値参照操作を構築する (図 4)。

値生成操作では、操作名は元の実装操作と同様とし、モデルの非決定的値の数だけ戻り値を作る。この操作は、作った戻り値に非決定的値に対応する実装の式を代入する代入文と、元の実装操作のうち非決定的値に対応する実装の式が含む変数を定義する代入文を持つ。

値参照操作では、操作名は元の実装操作と同様とし、元の実装が持つ戻り値や引数を全て抽出する。また、モデルの非決定的値の数だけ引数を追加する。操作の中身は、元の実装操作の代入文のうち、値参照操作に含まな

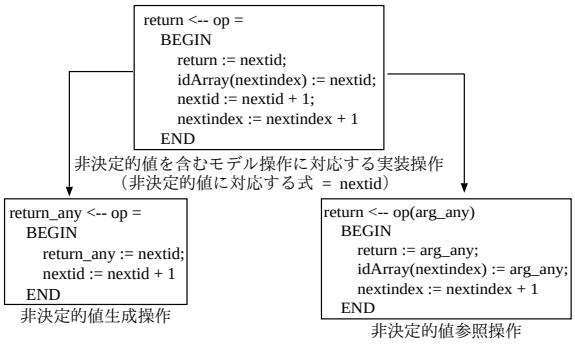

図 4: 非決定的値生成、参照操作の構築

かった代入文を持つ。この際、非決定的値に対応する実装の式の部分を、追加した引数に置き換える。

3.4 操作抽出

操作抽出では前の手順で作成した値生成操作、参照操作から、細分化モデルを満たす代入文を抽出し細分化実装操作を構築する。細分化モデルを満たすためには、細分化モデルの代入で変化する変数が実装においても変化すること、また細分化モデルで変化しない変数が実装においても変化しないことが重要である。そのため、変化しない実装の条件分岐を空にする、変化しないモデルの変数のリンク変数に関する代入文を抽出しないなどの工夫を行う。具体的な手順は以下の通りである。

1. 3.2 章で特定した条件分岐以外の代入文を削除する。
2. 細分化モデルの変数のリンク変数から、対応する実装の代入文を抽出する。ただし、他のモデル変数のリンク変数に関する代入文は抽出しない。
3. 抽出した代入文に関する代入文を再帰的に抽出する。
4. 最終的に抽出された代入文群が、細分化モデルの代入文に対応する。

以上の手順により、細分化モデルの代入文と等価な実装の代入文群を抽出することができる。

4 考察

小規模なソフトウェアを用いた実験から、細分化モデルに対応する実装操作を機械的に抽出できることを確認した。しかし、条件分岐の対応特定で各条件代入文群に含まれる変数、定数が同一である場合に正しく対応特定ができない、また一部の記述についてリンク変数による操作抽出が正しく行えないなどの課題がある。

5 おわりに

本研究では機械的抽出を考慮した実装抽出手法を提案した。今後は 4 章で述べた課題に対応していくとともに、モジュール構造への対応や制約条件の抽出を行っていく。

参考文献

[1] 来間 啓伸. *B* メソッドによる形式仕様記述, 近代科学社, 2007.

[2] 三鍋 孝介. 文字列一致による数学的等価性判定可能なモデル分割アルゴリズム, 情報科学技術フォーラム, Vol.12, pp.271-272, 2013

[3] 中村 丈洋. *B Method* における部品再利用によるソフトウェア合成と高信頼ソフトウェア部品の整備, 電気通信大学 電気通信学研究科 博士 (工学) 学位論文,2014.

Copyright ©2018 Information Processing Society of Japan.
All Rights Reserved.