B-009

抽象データ型に対応した不足部品の自動生成手法

Automatic Implementation Generation Method Corresponding to Abstract Data Type

大久保 稜† **織田 健**†
Ryo Okubo **Takeshi Oda**

1 はじめに

ソフトウェア開発の大規模化による信頼性低下やコスト増大が問題になっている。我々は問題解決のため形式手法を用いた既存ソフトウェアを部品化し、新規ソフトウェアを自動合成する手法を提案している [1]。不足部品が生じた場合は可能な限り自動生成する手法が提案されていたが、その対象範囲の狭さが課題であった。本研究では従来手法で対象外であったデータ型に対応する手法を提案し、その妥当性を実験により検証することで、自動生成の対象範囲を拡張することを目的とする。

2 背景

2.1 形式手法と B メソッド

形式手法は数学的基盤に基づく形式仕様記述言語により、自然言語の曖昧さを排除しシステムの正しさを機械的に検証できる [2]。B メソッドは集合論に基づく形式手法であり、段階的詳細化により一連の開発工程を支援する。モデルでは抽象的なデータ型の変数とそれに対する操作が記述されており、実装ではそれをより具体的な変数と操作に詳細化する。モデル変数と実装変数はリンク不変条件によって関係付けられる。B メソッドでは各段階の無矛盾性と段階間の整合性を機械的に検証できる。

2.2 MSSS 手法

我々は B メソッドを用いたソフトウェア自動合成手法である MSSS（モデル充足ソフトウェア合成）手法を提案している。MSSS 手法は大きく MSFC（モデル充足最粒度部品）生成と MSSS の 2 つの処理に分けられる。MSFC 生成は B メソッドで作られた既存ソフトウェアを細分化することで部品を生成し部品リポジトリに登録する。モデルを細分化し、各細分化モデルとそれに対応するように元の実装から抽出された細分化実装の組を部品としてリポジトリに登録する。MSSS は新規ソフトウェアのモデルを入力し実装を出力する処理である。この処理では入力されたモデルを細分化し、細分化モデルに合致する部品をリポジトリから検索する。部品間には結合の可否があるため、取得された部品から結合可能な組み合わせを調べ、利用者の負担が最も軽くなる組み合わせを選択する。不足部品が生じた場合は可能な限り自動生成をするが、自動生成不可能な部品は利用者が記述する。

2.3 具象データ型と抽象データ型

本研究ではモデル変数を詳細化した変数のデータ型を‘具象データ型’と‘抽象データ型’に分類する。具象データ型は実装で直接宣言されている変数へ詳細化された場合のデータ型を指し、抽象データ型は実装で他のモデルを輸入した場合のデータ型を指す。一般に抽象データ型とはデータとそれに対する操作が外部インターフェイスとして備わっているオブジェクトを指している。B メソッドの抽象機械も同様の性質を有しており、詳細化の際に用いられるケースも多々ある。

2.4 従来手法と研究目的

同一のモデル変数を含む部品同士はその変数の詳細化方法が一致しなければ結合ができない。従来の自動生成手法ではこの制約を考慮して、取得された部品のデータ型から情報を抽出し、生成する部品のデータ型を他部品に揃え、あらかじめ用意されていた生成規則からデータ型とモデルの操作から実装の操作を決定する手法が提案された [3]。しかし、従来手法ではモデル変数が特定の具象データ型に詳細化されている場合のみ適用可能であり、抽象データ型には対応していなかった。

本研究は利用者の負担低減のため、自動生成手法を抽象データ型に対応できるよう拡張することを目的とする。

3 解決方針

抽象データ型に手法を拡張する場合も従来手法と同様に他部品とデータ型を揃え、結合できるように部品を生成しなければならない。しかし抽象データ型に詳細化されている場合、従来手法のように生成規則から操作を決定することは不可能である。なぜなら従来の生成規則は変数を直接処理するものであったことに対し、抽象データ型内の変数は直接参照・代入することは許可されていないためである。抽象データ型内の変数を処理するためには内部に備わっている操作を呼び出すしか方法はない。そこで本研究ではモデルの操作を満たすような操作を抽象データ型内を探索することで決定し、それを実装に記述することで操作を生成する方針を取る。

4 抽象データ型に対応した自動生成手法

4.1 手法の概要

抽象データ型の操作がモデルの操作を満たすための条件は 2 つある。1 つはモデルの操作の事前条件が満たされているとき抽象データ型の操作の事前条件を満たすこと。もう 1 つはリンク不変条件を通してモデルの事後状態と抽象データ型の事後状態が一致することである。B メソッドの開発環境である Atelier B の定理証明器を用いてこれらを検証し、両方の条件を満たした抽象データ型の操作をモデルの操作を満たすものとして選択する。証明はいくつかのコマンドを組み合わせることで行うことができ、最も汎用的なコマンドとして pr が挙げられる。なお本手法の対象は “モデル変数と抽象データ型の変数は 1 対 1 に対応している”、“1 回の操作呼び出しでモデルの操作を満たせる”、“証明は pr コマンドだけで

†電気通信大学大学院情報理工学研究科情報学専攻

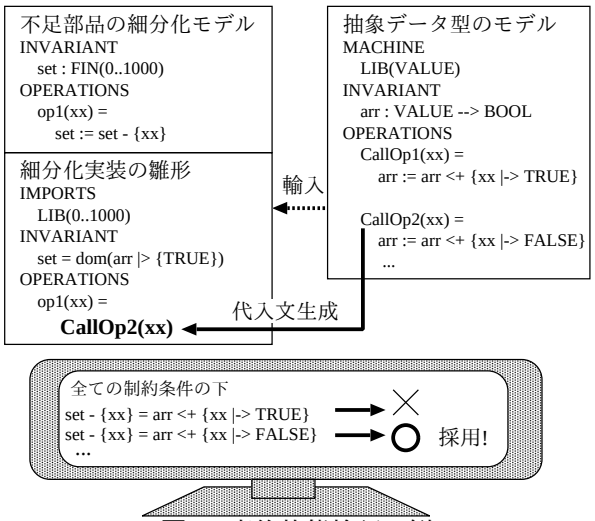

図 1: 事後状態検証の例

行う”、を条件とし、満たせないものは自動生成不可とする。手順は MSSS において部品リポジトリを検索し、候補となる部品の組み合わせが挙げられている段階から開始する。まずは不足部品の実装の雛形を作成する。次にモデルの代入文を単純な代入文に分解する。抽象データ型に詳細化されている変数を含む代入文は抽象データ型の操作から事前条件と事後状態を満たす操作を探索し、実装の雛形に呼び出す操作を記述して部品の生成が完了する。以降の節ではこれらの手順について説明する。

4.2 実装の雛形作成

これは従来手法と同様の手順になる。不足部品は他の部品と結合できるように生成する必要があるため、データ型を揃えなければならない。不足部品の細分化モデルに含まれる変数と同一の変数を含む細分化モデルで、既に部品を取得しているものからリンク不変条件とその変数の詳細化方法を特定し、データ型等の情報を不足部品の実装に書き込む。加えて不足部品のモデル名や操作の名前も書き込むことで実装の雛形は作成される。

4.3 代入文分解

1 つの代入文に 2 つ以上の異なるモデル変数が含まれている場合は自動生成が困難になるため、代入文を変数を 1 つのみ含むように分解する。具体的には $set := set \cup \{func(aa)\}$ のような代入文で、set と $func$ が変数の場合、$L01 := func(aa)$ と $set := set \cup \{L01\}$ のように分解して各代入文について自動生成する。

4.4 事前条件・事後状態の検証

抽象データ型の操作からモデルの操作を満たす操作を決定する。モデル操作の事前条件 P_M と抽象データ型の操作の事前条件 P_{Ai} に対して、$P_M \Rightarrow P_{Ai}$ を検証する。またモデル変数 x_M と抽象データ型の変数 x_A とのリンク不変条件 $x_M = L(x_A)$、モデルの操作の事後状態 V_M と抽象データ型の操作の事後状態 V_{Ai} に対して、$V_M = L(V_{Ai})$ を検証する。2 つの検証が真となればその操作の呼び出しを実装の雛形に記述して自動生成が完了となる。例えば、図 1 は事後状態の検証で 2 つの操作が検証されているが、操作 $CallOp2$ がモデル操作を満たすことが証明されたため、これを実装に記述している。

5 評価実験

本手法の妥当性を検証するために評価実験を行った。実験では 1 つの実験用モデルとそれを 3 通りに詳細化した 3 つの実験用実装を用意した。実験用モデルを細分化したところ 14 の細分化モデルが作成され、各細分化モデルと各実装について細分化実装を抽出すると、36 個の部品が作成されリポジトリに登録された。この実験用モデルを MSSS において再びソフトウェアを合成するのだが、現在のリポジトリの状況では全ての部品が揃っているため不足部品が生じない。そこで部品の存在確率を設定し、リポジトリの中身を調整した。存在確率は MSSS 手法が十分に活用されていることを想定し 90%に設定した。リポジトリの状態を上記の条件で変えて、5 回実験を行った。結果として対象範囲内の部品は全て生成でき、誤った部品を生成することはなかった。また、追加の実験としてモデル変数と抽象データ型の変数が 1 対多に対応している場合と証明のコマンドの追加を許可した状態で、同様の実験を行い結果を確認した。1 対多の変数間の対応は判定するアルゴリズムは存在しないため主観で判断した。結果として変数間が 1 対多に対応している場合は通常の証明コマンド pr のみでは証明することができず、追加の証明コマンドを実行した場合に証明ができ、部品を生成することができた。

6 考察

実験の結果から本手法の信頼性と妥当性が検証された。誤った操作は事前条件か事後状態のどちらかの検証で必ず失敗するため、誤った部品を生成することはなかった。対象範囲内の部品であれば全てを正しく生成することができたため、一連の手順は十分に妥当な手法であったと言える。自動生成の対象範囲が広がったことから利用者の負担を低減する目標も達成したと考える。ただし、部品の存在確率が妥当な設定であったかは確認できておらず、手法の柔軟性を検証するためにも様々な確率で実験を重ねる必要がある。対象範囲を狭めているため完全な手法ではないが、追加実験で手法を拡張する方針を立てることができた。変数間が 1 対多に対応している場合でもアルゴリズムさえ整備すれば部品を生成することが可能であるとわかった。また、複雑になった証明を行うための証明コマンドも追加する方針も立てることができた。今後は手法を改良し、部品の生成率上昇を目指す。

7 終わりに

本稿では不足部品の自動生成において、操作の整合性検証により抽象データ型に対応する手法を提案し、実験で手法の妥当性と改善点が確認された。今後は手法をより拡張し、さらなる利用者の負担低減を目標とする。

参考文献

[1] 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

[2] 来間 啓伸. B メソッドにおける形式仕様記述. 近代科学社. 2007

[3] 大久保 稜, 織田 健. 取得部品からの詳細化情報抽出による不足部品の自動生成手法. 第 20 回情報科学技術フォーラム論文集. vol.1 pp.143-144. (2021.09)