4L-03

抽象データ型を考慮した不足部品の自動生成手法

大久保 稜[†]
電気通信大学大学院情報学専攻

織田 健[‡]
電気通信大学大学院情報学専攻

1 はじめに

ソフトウェア開発の大規模化に伴いコスト増大と信頼性低下が問題となっている。その解決策として形式手法と部品再利用がある。我々は形式手法Bメソッドを用いた既存ソフトウェアを部品化し、それらを再利用することで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]。この手法では不足部品が生じた場合は極力自動生成をしていたが、適用可能範囲の狭さが課題であった。本研究では適用範囲を拡張する手法を提案する。

2 研究背景

2.1 形式手法とBメソッド

形式手法とは数学的基盤に基づく形式仕様記述言語により、自然言語の曖昧性を排除し仕様の機械的検証を可能にする [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仕様からコード生成までの一連の開発過程を支援する。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メソッドを利用したMSSS（モデル充足ソフトウェア合成）手法を提案している。MSSS手法は部品を生成するMSFC（モデル充足細粒度部品）生成と新規ソフトウェアを合成するMSSSから構成される。

MSFC生成はBメソッドで作成されたソフトウェアを入力として部品を生成する処理である。入力ソフトウェアのモデルを細分化し、細分化モデルに対応した細分化実装を抽出することで、それらを組とした部品が生成される。生成された部品は部品リポジトリに登録されるが、同一の細分化モデルを含む部品が既に登録されている場合、既存部品の細分化モデルに対して新規部品の細分化実装が紐付けられる形で登録される。

MSSSは要求モデルを入力とし、部品を再利用・合成することで新規ソフトウェアを作成する処理である。要求モデルを細分化し、細分化モデルを検索キーとして部品リポジトリを検索する。検索で得られた部品を取得部品と呼ぶ。部品間には結合の可否が存在するため、結合可能な部品の組み合わせから要求を最も網羅できる組み合わせを選択し、それらを合成することで新規ソフトウェアを得る。細分化モデルを満たす部品が存在しない場合は可能な限り自動生成をするが、自動生成できないものは人の手で記述する。

2.3 具象データ型と抽象データ型

Bメソッドでは集合や写像などを用いた数学的なモデルを実行可能なコードに落とし込むために詳細化が行われる。モデルを詳細化する際に、モデル内の変数と実装内の変数の関係を表すリンク不変条件という制約を記述する。本稿では詳細化される変数が実装内で宣言・定義されていた場合には、それらを‘具象データ型’と呼ぶ。対して実装内で他のモデルを輸入して、そのモデル内の変数とのリンク不変条件が記されていた場合、‘抽象データ型’に詳細化されたと呼ぶ。一般に抽象データ型とは内部的なデータとそれに対する操作がインターフェイスとして備わったデータ型のことをいう。Bメソッドの抽象機械は抽象データ型としても利用される。内部の実装はカプセル化されているため複雑なモデル変数を詳細化する場合に抽象データ型を用いるケースは多々ある。

2.4 従来の自動生成手法

部品間で同じモデル変数が含まれている場合、結合時の不整合を回避するためそれらは同じデータ型に詳細化されていなければならない。この性質を利用して、従来手法では不足部品の細分化モデルに含まれる各変数に対して同様の変数を含む取得部品から‘自動生成に関する詳細化情報’と呼ばれる情報を抽出していた。これは詳細化先のデータ型やリンク不変条件に関する情報の集合である。従来の自動生成手法では不足部品の細分化モデルに含まれる変数が特定の具象データ型の変数に詳細化されている場合を対象としていた。抽出した自動生成に関する詳細化情報とあらかじめ用意しておいた生成規則を基に自動生成を行う手法であった [3]。しかし、従来手法は適用範囲が狭く抽象データ型には対応していなかった。

2.5 研究の目的

上述の課題を受けて、本研究では自動生成手法に抽象データ型への対応手法を取り入れ、自動生成可能な部品を増やすことで人の負担を従来より低減することを目的とする。なお本研究では自動生成手法を考慮した部品選択手法の提案も検討しているが、本稿では割愛する。

3 解決方針

従来手法では図1右上のように細分化実装の雛形を取得部品から抽出し、細分化実装の操作を変数の型の情報・細分化モデルの操作・生成規則の3つから生成した。実装変数の状態を直接操作する生成規則を定め、リンク不変条件を通してモデル変数との状態が一致するように操作を生成することが可能であった。しかし、抽象データ型では内部の変数を直接操作できず、用意されている操作を呼び出すことでしか変数の状態を変えられない。そこで本研究では図1右下のように要求の操作と抽象データ型の全ての操作との整合性をBメソッドの開発環境の1つであるAtelier Bに備わっている定理証明器により検証し、呼び出すべき操作を決定する手法を提案する。

Automatic implementation generation method considering abstract data type

[†]Ryo Okubo, The University of Electro-Communications, Graduate School of Infomation and Communication Engineering

[‡]Takeshi Oda, The University of Electro-Communications, Graduate School of Infomation and Communication Engineering

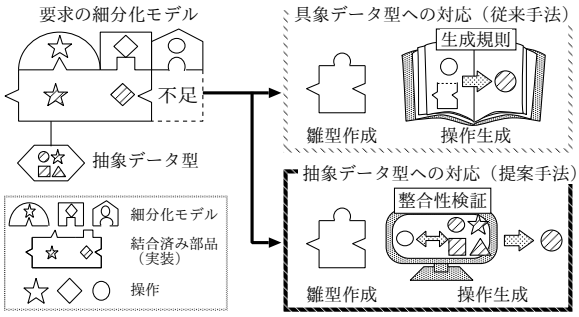

図 1: 提案手法の概念図

4 抽象データ型を考慮した自動生成手法

4.1 手法の概要

本稿では MSSS において部品検索を行い、部品の組み合わせの候補が揃っている状態からの処理を説明する。各組み合わせの取得部品から自動生成に関する詳細化情報を抽出し、これらを基に細分化実装の雛形を作成する。次に代入文を分解した後、具象データ型の変数のみからなる代入文は従来手法で生成し、抽象データ型の変数を含む代入文は提案手法で生成する。自動生成された部品を考慮して人の負担が最も少なくなる組み合わせを選択する。自動生成できない部品は人の手で記述し、それら全てを結合することで新規ソフトウェアの完成とする。

4.2 適用範囲

本手法では全ての不足部品を自動生成することは不可能であり、適用範囲は次の通りである。具象データ型の変数へ詳細化されているモデル変数の型においては従来手法の適用範囲であるスカラーと集合に加え、写像も取り入れる。なお、本稿では写像に対応する手法の詳細は割愛する。抽象データ型を利用しているものについての型の制限は設けないが、1 回の操作呼び出しで要求を満たせないもの、また整合性を自動証明できないものは自動生成不可能であると判断する。

4.3 自動生成の手順

4.3.1 情報の抽出と雛形作成

不足部品のモデル変数が取得部品で抽象データ型に詳細化されている場合、データ型を合わせるため取得部品から輸入している機械とリンク不変条件等の情報を抽出し、これを自動生成に関する詳細化情報とする。これらの情報の制約条件と細分化モデルの機械名・操作名を記述することで細分化実装の雛形を作成する。

4.3.2 代入文の分解

複数の演算が絡み合った代入文は自動生成が困難である。そこで複雑な代入文を複数の単純な代入文に分解する。例えば、$set := set \cup \{fun(xx)\}$ のような代入文は $l01 := fun(xx)$ と $set := set \cup \{l01\}$ のような代入文に分解することで自動生成を適用しやすくする。これらの分解規則はあらかじめ用意しておき、これ以上分解できなくなるまで適用する。

4.3.3 定理証明器の整合性検証による代入文生成

分解した各代入文に対して自動生成を行う。抽象データ型を利用する場合は呼び出すべき操作を見つけるため、

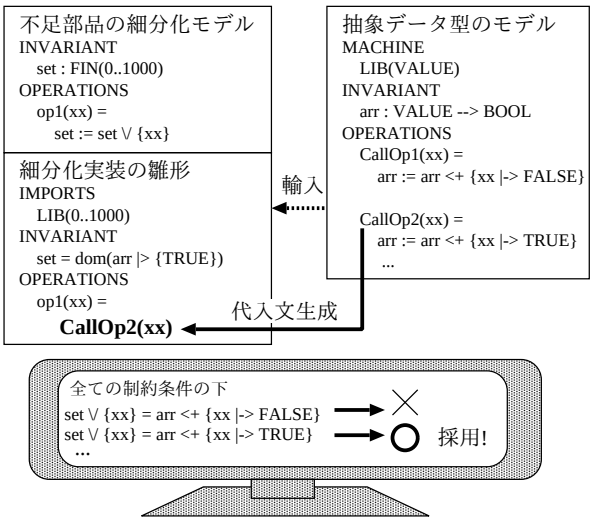

図 2: 定理証明器による整合性検証の例

抽象データ型の全ての操作と分解後の代入文の整合性を定理証明器を用いて検証し、証明が成功したものを細分化実装での代入とする。検証は要求の制約・抽象データ型内の制約・リンク不変条件を基に事前条件と事後状態の 2 つに対して行う。要求の操作の事前条件が成り立つ時に抽象データ型の操作の事前条件が成り立つことの検証と、全ての条件が成り立つ時に要求の操作の事後状態と抽象データ型の操作の事後状態が一致するかを検証する。図 2 は事後状態の整合性検証の例である。抽象データ型のモデルには操作が複数あるが、その全ての操作の事後状態と要求操作の事後状態の整合性を検証することで、モデルの代入文と $CallOp2$ が整合していることが分かる。これを細分化実装の雛形に記述することで代入文の生成が完了する。

5 考察

本手法は構想段階に留まっているため、今後実験をして妥当性を検証していく必要がある。定理証明器を用いて段階間の操作の整合性を検証し操作を生成するため、信頼性を保証されている生成規則を用いなくとも、信頼性の高い部品の生成が期待できる。一方、整合性を自動証明できなければ正しい操作と認めないため、本来整合性が成り立つはずの操作を取りこぼす可能性がある。

6 終わりに

本稿では自動生成手法において、定理証明器を用いた要求の操作と抽象データ型の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た。今後は実験による本手法の妥当性検証と判明した課題の検討を行う。

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)