B-009

参照変数の定数化による形式的派生部品生成手法

A Method for Generating Derived Formal Components by Making Reference Variables Constants

原野 和貴† 織田 健†
Kazuki Harano Takeshi Oda

1 はじめに

近年、ソフトウェアの複雑化により開発コストの増大や信頼性の低下が問題である。それに対し、形式手法や部品再利用が研究されている。我々は、形式手法の 1 つの B メソッドで記述されたモデルと実装の組の部品の再利用による、新規要求を満たすソフトウェアの合成手法を提案している [1]。この手法では要求と等価な仕様を持つ部品が再利用され、同じ定数や変数を持つ異なる操作の部品群が多いと要求に対する網羅性が高くなる。本手法では、生成された部品で状態が変化しない変数を定数化して派生部品を生成する手法を提案する。

2 研究背景

2.1 B メソッド

B メソッドは数学的基盤に基づく形式手法の 1 つで、仕様記述からコード生成まで支援する [2]。また、段階的詳細化により仕様から実装への記述が可能で、機械的な検証で各段階の無矛盾性と整合性を保障する。B メソッドには、定数や変数などを制約条件を用いて記述する部分とそれらを用いて操作を記述する部分がある。

B メソッドの定数には識別子を持つ宣言定数があり、宣言定数には実装に応じて型が制限された具象定数と型が制限されてなく実装には記述不可な抽象定数が存在する。B メソッドの型は集合論に基づきスカラー値、集合、関数等が存在する。仕様実装間における定数の詳細化では、抽象定数から具象定数への詳細化でも同じ型を持つ。

2.2 モデル充足ソフトウェア合成手法

モデル充足ソフトウェア合成 (MSSS) 手法は B メソッドの仕様と実装の部品を再利用して、新規要求を満たす無矛盾なソフトウェアを合成する [1]。この手法では、細分化要求と部品の仕様の等価性を文字列一致で判定し、要求を満たす部品が再利用される。

3 課題と解決方針

先の MSSS 手法の部品取得では、部品内の定数や変数と操作がともに要求と等価なものが再利用される。そのため、部品の種類が少ないと部品群の網羅性が低いという課題が生じる。特に変数の型が複雑な部品を再利用する場合、仮に変数の型が同じ部品群があっても操作が適合しないと不足部品が生じる (図 1)。

この課題に対し、既存ソフトウェアから生成された部品から操作で状態が変化しない変数 (参照変数) を定数化することで派生部品を生成する。これにより、同じ変数の型を持つ異なる操作の部品を生成し、部品群の網羅性の向上を図る。

†電気通信大学大学院情報理工学研究科情報学専攻

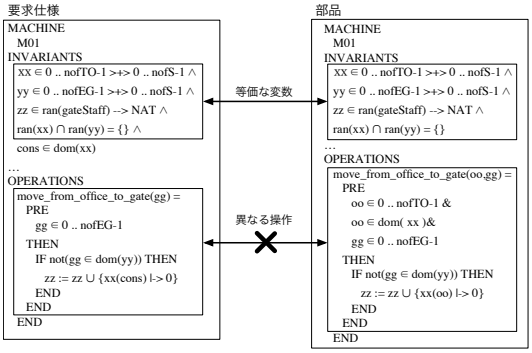

図 1: 同じ変数の型を持つ部品の再利用不可

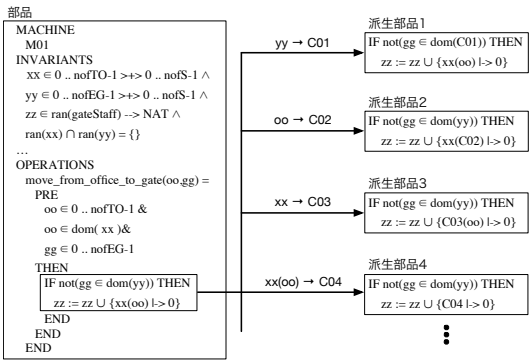

図 2: 参照変数の定数化による派生部品生成

4 参照変数の定数化による派生部品生成手法

本章では、先の方針に従い派生部品を生成する手法を説明する。本手法で対象とする参照変数とは、代入によって値が変化しない、着目する部品内では値の参照しか行われない変数である。この変数は操作の実行時に値が変化せず、部品内で定数と等価と考えることが可能である。本手法では、部品内の操作に含まれる参照変数を宣言定数に置換することで異なる操作を持つ新たな部品を生成する。図 2 では、部品内の各変数を COX の識別子の宣言定数に置換している。以降では、参照変数の具体的な定義を述べ、その後部品生成の具体的な手順を説明する。

4.1 参照変数の定義

まず、本手法で定数化の対象とする参照変数の定義について説明する。参照変数は、操作内の IF 文の条件分岐の条件などの制約条件や代入文に含まれる変数を対象としており、次の定義を満たす。

定義 1 操作内の変数 (宣言された変数、引数、返り値、一時変数) の内、宣言された変数と引数である。

定義 2 代入文内に含まれる変数は次のいずれかを満たすとき参照変数である。

- 代入文の右辺にのみ記述されている。

Copyright © 2021 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

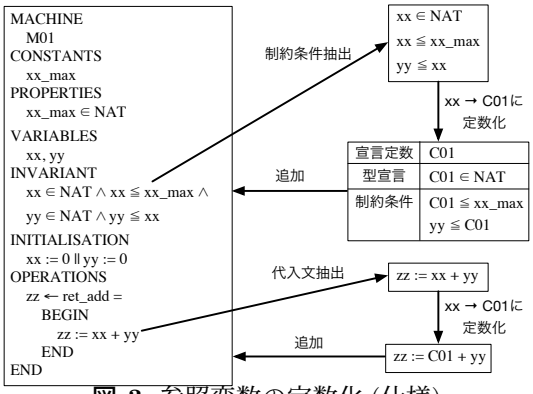

図 3: 参照変数の定数化 (仕様)

- 代入文の左辺で参照用途 (関数の定義域指定など) で記述されている。

定義 3 制約条件内に含まれる変数。ただし、代入文にも含まれるときは定義 2 を満たす。

定義 4 変数の型がスカラー値、集合、関数である。ただし集合、関数は具象定数で制限される型であり、実装で輸入機械 (ライブラリなど) を使用していない。

定義 5 関数の変数の場合、`dom(func)`、`ran(func)`、`func(idx)` などの定義域または値域に制限される記述をまとめて 1 つの参照変数とすることができる。

4.2 派生部品生成手法の手順

次に、既存ソフトウェアから生成された部品から派生部品を生成する手順について述べる。

4.2.1 参照変数の特定

まず、操作内の変数から参照変数を特定し列挙する。参照変数を上記の定義に従ってまとめて 1 つの参照変数とする場合も含めて、全て列挙する。

4.2.2 定数化する参照変数群の決定

次に、特定された参照変数群から派生部品で定数化する参照変数群を決定する。本手法で生成される派生部品は定数化が可能な全ての組み合わせで定数化する。

また、これらの決定では 2 つ制限を設ける。まず 1 つ目は、IF 文の一意の条件分岐のように定数のみで構成される代入文や制約条件が発生するような組み合わせを禁止とする。次に 2 つ目は、定義 5 を満たす参照変数が組み合わせに含まれる時、同時にその構成変数を含むことを禁止とする。例えば、`func(idx)` という参照変数が含まれる場合はその構成変数の `func`、`idx` は含まれない。

4.2.3 部品の制約条件・操作抽出と削除

次に、定数化する参照変数についてそれらが含まれる部品内の制約条件や操作を抽出・削除する。この時、定数化する参照変数は削除されるため、変数の宣言部と初期化を削除する。

4.2.4 新たな宣言定数の決定

次に、得られた制約条件の情報から、新たな宣言定数を決定する (図 3 右上)。宣言定数の決定では新たな宣言定数の宣言、宣言定数の制約条件 (型宣言) の決定、参照変数が含まれる制約条件の更新を行う。

まず、新たな宣言定数の宣言では、スカラー値の場合は仕様実装ともに具象定数で宣言し、集合と関数の場合は仕様では抽象定数、実装では具象定数で決定する。

次に、宣言定数の制約条件の決定では新たな宣言定数の型宣言を決定する。新たな宣言定数の型は、スカラー値と関数では仕様と実装それぞれの参照変数の型を持つ。対して集合では、詳細化で型が変更できないため実装の宣言定数も仕様と同じ型を持つ。なお、定義 5 の参照変数は関数の定義域または値域の一方を型として持つ。

最後に、参照変数が含まれる制約条件の更新では、他の宣言定数や変数との関係を示す制約条件を新たな宣言定数で置換する。この時、定義 5 の型を一方に制限された時など、部品に関係しない制約条件は削除する。

4.2.5 操作の決定

次に、抽出した操作から定数化後の新たな操作を決定する (図 3 右下)。スカラー値の場合は、仕様と実装の操作内の参照変数を新たな宣言定数で置換することで決定する。また、集合や関数の場合は、仕様実装間の変数の関係を示す制約条件を元に操作を決定する。

4.2.6 制約条件・操作の追加

最後に、上記で決定した宣言定数の制約条件と操作を部品に追加し構文の並び替え等を行い部品生成する。

5 評価実験

本手法で生成される部品が無矛盾性であるか検証した。実験では、簡単な部品を複数用意し本手法を適用すると無矛盾性が保たれていることを確認した。

6 考察

実験から、単純な部品について派生部品を生成することが可能であることが示された。しかし、集合や定義 5 を満たす制約条件など完全に手法が決定されていないため、手法の決定および検証が課題の 1 つである。

本手法では、派生部品の生成による部品群の網羅性の向上が利点である。それに加え、派生部品は我々が提案した定数に関する再利用性向上手法 [3] により再利用性が高いと考えられる。この手法では、スカラー値の定数の型を関係を持つ変数と同じ型に拡大することで再利用性を向上させる。スカラー値の参照変数の定数化では型が変数の型と同じになるため再利用性が高いと言える。これらの利点の検証も課題の 1 つである。

7 終わりに

本研究では、部品の操作内の参照変数を定数化し部品群の網羅性を向上させる手法を提案した。今後は、更なる手法の具体化や再利用性に関する検証等が課題である。

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] 原野和貴, 織田健 「定数値制約領域の拡大による形式的部品の再利用性向上手法」, 情報処理学会 第 83 回全国大会, vol.1 pp.259-260(2021, 3).

Copyright © 2021 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.