3J-07

形式的ソフトウェア合成手法 MSSS の妥当性評価実験

岡野 純平[†]
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専攻

1 はじめに

近年ソフトウェア開発では、信頼性の確保が課題となっている。そこで我々は形式手法 B-Method を用い、ソフトウェア部品の再利用により高信頼ソフトウェアを自動合成する MSSS 手法を提案した [1]。MSSS 手法は各行程の部分的な検証しかしておらず、全体の検証が行われていなかった。そこで本研究では MSSS 手法の妥当性を検証するため、全体を通した評価実験を行う。

2 背景と目的

2.1 MSSS 手法

MSSS 手法とは、B-Method で記述されたモデルに対してソフトウェアを自動合成する手法である (図 1)。

MSSS では最初にモデル細分化を行う (詳細は 3.1 節)。その後細分化モデルをキーとして同じモデルを持つ部品をリポジトリから検索する。この時、一つの細分化モデルに複数の部品が得られる。次に各部品が他の細分化モデルの部品と結合可能かを型情報の利用により判定し、結合可能な部品を結合しソフトウェアを出力する。

2.2 本研究の目的

MSSS では各行程に対してその手順が個々に提案されたが、それぞれの手順に対して小さな例題を用いた個別の検証しかしておらず、MSSS 全体を通した実験が行われてなかった。本研究の目的は MSSS が全体において妥当かどうか網羅的に検証することである。

3 MSSS

3.1 モデル細分化の手法

B-Method のモデルは大まかに ‘制約条件部’ と ‘操作部’ の二つに分けることができる。モデル細分化では入力されたモデルが操作部の代入文一つとなるような細分化モデルを複数個出力する [2]。

3.1.1 プリミティブ化と簡約化

プリミティブ化とは演算子に対してその定義にあたる数学的等価な表現への書き換えを行い、演算子の限定を行うことである。例を挙げると $s \in t$ をプリミティブとするならば $s \notin t$ は $\neg(s \in t)$ と表す。簡約化は冗長な表現を解消する方法で、いくつかのルールを用いることで制約条件内の式の書き換えを行う。

3.1.2 推論

それぞれの細分化モデルの ‘制約条件部’ は元の制約条件では明示されない暗黙の条件を含む。このような暗黙の条件を細分化モデルに含めるため, 推論を行う。推論では制約条件から任意の二つの式を選択し、そこから導かれる新しい条件式を制約条件として追加する。

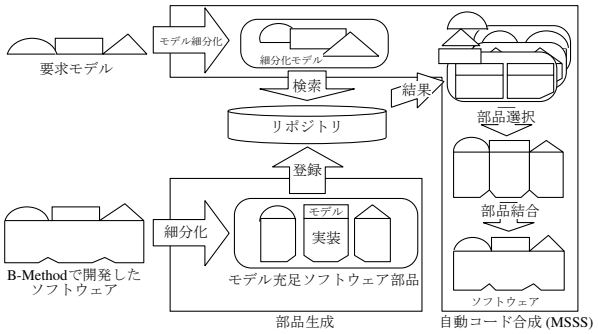

図 1: MSSS の概略図

3.1.3 制約条件抽出

推論により制約条件展開をした後 ‘操作部’ を一代入文毎に分割し、その代入文毎に必要な制約条件を抽出する。その方法は、操作内に存在する変数のみを持つ制約条件を推論した式の中から抽出することである。

3.2 変数名の変更

細分化モデル内の集合、変数名を登場順に書き換える。これにより数学的等価なモデルは全て同じ字面となる。

3.3 部品検索

部品検索は細分化モデルを入力としてそれを満たした部品を出力する。部品のモデルを細分化モデルの要求モデルと比較して事前条件以外は字面の一致、事前条件は包含関係 (細分化モデル $\subseteq$ 部品のモデル) が成り立つとき検索結果として出力される。

3.4 部品の選択と部品結合

検索された部品を結合する際、どの部品同士が結合できるかを選択可否判定で判定する。選択可否判定は部品間の同じモデル変数を表す部品の実装変数の型情報が一致したときその部品同士は結合可能と判定する。部品結合では選択可否判定が真となる部品同士を結合しソフトウェアを出力する [3]。

4 評価実験

MSSS の振る舞いが全体として妥当かどうかを評価するため、本研究では MSSS に対して以下の四つの評価軸を用意し、実際に MSSS に対して要求モデルを入力して、最終的に出力されたソフトウェアが評価軸を満たしているかどうかで評価を行う。

- 入力に対して必ず出力がある。
- 入力されたモデルと出力されたソフトウェアの整合性がとれる。
- 入力されたモデルが数学的に等価なら同じソフト

formal

[†]Jumpei Okano, The University of Electro-Communications department school of Informatics
[‡]Takeshi Oda, The University of Electro-Communications graduate school of Informatics

Copyright ©2016 Information Processing Society of Japan.
All Rights Reserved.

ウェアが出力される。
- 条件にあった部品があるならば必ず検索される。

4.1 出力の有無

実験は6つのモデルに対し、モデル細分化、部品検索、選択可否判定、部品結合の手順を実際に行った。その流れでモデル細分化の際に推論の停止性についてはツール及び、手計算による確認を行った。また部品検索ではあらかじめ検索出来る部品を用意した。

実験の結果として、全てのモデルで推論は停止し、出力が存在した。

4.2 モデルと実装の整合性

MSSSで出力されたソフトウェアは、高信頼である必要があり、モデルと異る振る舞いがあってはならない。モデルと実装の整合性がとれなくなる原因として、モデル細分化の際情報が欠落すること、選択可否判定が真でも証明責務が偽となる部品の結合が挙げられる。実験では出力されたソフトウェアのモデルと実装間の証明責務が真となるか確認した。

4.3 数学的等価な入力に対する出力

数学的に等価な入力に対する出力は以下のことを考慮して実験を行った。

- 全ての関数、関係においてプリミティブ化、簡約化の合流性があるかどうか
- 全ての述語論理においてプリミティブ化、簡約化の合流性があるかどうか

数学的に等価な入力に対して出力結果が一致するかどうかは等価な入力に対して出力された細分化モデルが完全に一致するかどうかに依存する。よって評価方法は数学的等価な入力を行い細分化モデルが一致するかで行う。

実験はモデルに部分全単射、部分単射、部分全射、全射を用いたモデル、またいくつかの集合演算子を使ったモデルとそれぞれの関数、集合に対してそれと等価な表現の記述をした2つのモデル(1つのモデルに対して8つの操作)を準備しMSSSに入力することで行った。

実験結果は8個の操作に対して7つの操作は等価な表現になり1つの操作は異る表現となった。

4.4 検索の信頼性

MSSSでは利用出来る部品は全て検索されるべきある。

実験は一つの要求モデルと複数の部品の仕様となる細分化モデルを十分な数を用意し行った。これらの部品のうち、入力したモデルの細分化モデルと任意の部品のモデルのPROPERTIES節、INVARIANT節の字面の一致、事前条件の包含関係を比較することによって元の入力モデルから検索出来るものを集めた。

実験結果はどの細分化モデルも必ず一つは部品を検索することができたが、こちらの意図した部品が必ず検索出来たとはいえなかった。

5 考察

5.1 出力の有無

MSSSは全ての入力に対して出力が存在しなければならない。出力がされない最たる原因としては推論が終了しないことが挙げられる。

今回の実験では推論が無限に続くといったことはなかった。よってMSSSの推論は停止し、出力が存在するということは十分に期待できる。

5.2 モデルの整合性

モデルの整合性の検証は部品の実装の整備が現時点で十分でないためまだ検証が終わってない。

5.3 数学的等価な入力に対する出力

数学的等価な表現の入力に対する出力に関しては以下のことが分かった。

- 関数、集合、論理演算、関係において数学的に等価ならば出力は一致する。
- 関数を論理演算で記述すると出力は一致しない

実験結果として細分化モデルの出力が一致しない場合が存在した。しかし字面が一致しなくとも出力されたソフトウェアの振る舞いが同じであればMSSSとして問題はないと考られるため、MSSSは充分にこの評価軸を満たしているといえる。

5.4 検索の信頼性

部品検索はモデル細分化において自明な条件(例えば $a = a$ のような)が出現することによって数学的に等価な部品であっても検索が行えない場合が存在した。

これは利用出来る部品が存在しても検索されないことを示し、MSSSの振る舞いとしては正しいとはいえない。よってモデル細分化をした後、検索を行う前に細分化モデルに存在する自明な条件を削除する手順が必要であると考えられる。

また検索において事前条件の包含関係は数にのみ依存していて、集合単位では考慮されていない。よって入力側の事前条件が $a : \{1, 2, 3\}$ という入力に対して部品の事前条件が $a : \{1, 2, 3, 4\}$ の場合異る条件と解釈され検索されない。これを解決するために集合の包含関係を考慮した検索方法を開発することが望まれる。

6 おわりに

今回の実験ではMSSSにおいてモデルに関連した問題点がいくつか見つかった。特に数学的に等価な部品が検索されないことについては今後新たに考えるべき課題である。これらの課題に対してMSSSが解決を行うためいくつかの手法を今後考える必要がある。

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, 博士論文 電気通信大学,(2014.02)

[2] 三鍋 孝介, 織田 健 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, 第12回情報科学技術フォーラム論文集,vo1.1 pp.271-272, (2013.09)

[3] 熊谷 恒, 形式的ソフトウェア合成手法における部品の充足を考慮した合成手順, 第77回情報処理学会全国大会講演論文集,vo1.1 pp.351-352,(2015.03)

Copyright ©2016 Information Processing Society of Japan.
All Rights Reserved.