B-023

形式的ソフトウェア部品の検証を兼ねた自動生成手法の改善と評価

Improvement and Evaluation of the Method of Automatic Generation with Verification of Formal Software Parts

佐々木孝紘† 織田 健†
Takahiro Sasaki Takeshi Oda

1 はじめに

ソフトウェアの大規模化や複雑化に伴う開発コストの増大や信頼性の低下に対し、我々は形式手法を用いた既存ソフトウェアから部品を生成、再利用してソフトウェアを合成する MSSS 手法 [1] を提案している。MSSS 手法において不足部品を自動生成する手法 [2] が提案されたが、生成された部品の信頼性に課題があった。そこで、整合性を検証しながら部品を自動生成する手法 [3] が提案されたが信頼性向上を確認する実験が不足していた。また、検証に時間がかかる課題もあった。本研究では、新たな自動生成手法の信頼性向上の確認のために行った実験の報告と検証時間を短縮させる方法の提案を行う。

2 研究背景

2.1 B Method

B Method[4] は形式手法の一つで、集合論と一階述語論理に基づいて仕様が記述されるモデルと、これを段階的に詳細化するリファインメントや実装による開発手法である。各段階における無矛盾性と整合性を証明することで信頼性の高いソフトウェアを開発できる。

2.2 MSSS 手法

MSSS 手法は、B Method によって開発されたソフトウェアから部品を生成してリポジトリに登録し、新規要求を細分化したモデルと同じモデルを持つ部品をリポジトリ内から検索して得た部品を合成することで、新規要求を満たすソフトウェアを合成する手法である。部品の検索時に、新規要求の細分化モデルと同じモデルを持つ部品が無かったり、他の部品と実装のデータ構造が異なる等の理由で部品が不足することがある。不足した部品は極力自動生成し、できないときは人が記述する。

2.3 大久保の自動生成手法

大久保はモデルの変数の詳細化のために、実装内で新たに変数を定義する具象データ型と他のモデルを輸入する抽象データ型にそれぞれ対応する自動生成手法を提案した [2]。具象データ型に詳細化されている場合は取得した他部品の実装におけるデータ型等の情報とモデルの代入文から実装の操作を導く生成規則を整備することで操作を生成していた。また複数の演算が絡み合った代入文は単純な代入文に分解することで生成規則の適用範囲を広げていた。抽象データ型に詳細化されている場合は輸入されたモデル内の操作の中から細分化モデルの代入文を満たす操作を定理証明器を用いた整合性検証によって見つけ出すことで操作を生成していた。しかし、具象データ型を用いた操作の整合性が検証されておらず、誤りを含む実装を生成する可能性があった。

†電気通信大学大学院情報理工学研究科情報学専攻

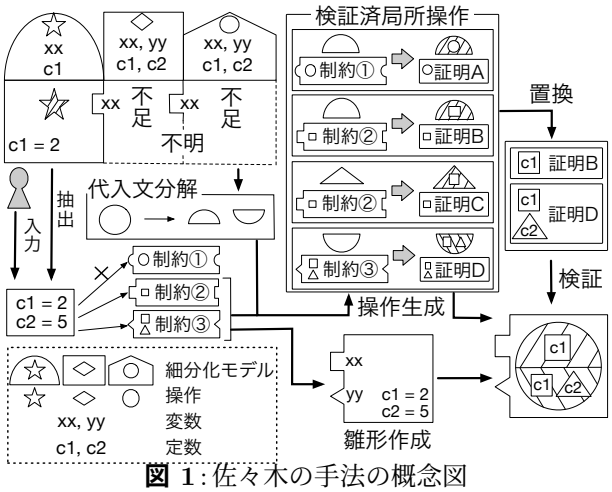

図 1: 佐々木の手法の概念図

2.4 佐々木の自動生成手法

筆者らは生成規則ごとに事前に整合性の検証が可能な局所操作を用意し、それらの一部をモデルの変数に関連する集合や定数に置換して再利用することで操作を生成する手法を提案した [3](佐々木の手法と呼ぶ)。この手法では置換後の局所操作の整合性のために集合や定数が満たすべき制約を実装のデータ構造ごとに設定し、置換する集合や定数がそれらを満たすか検証することで生成する操作の正しさを保証する (図 1)。また、モデルの変数に関連する集合や定数が満たすような制約が設定されている実装のデータ構造を探し出し、採用することで実装中のデータ型が不明な変数を含む部品の自動生成にも対応する。自動生成した実装は、局所操作の整備時に定理証明器へ入力したコマンド列を局所操作と同様に置換して再利用することで整合性を検証する。実験により大久保の手法に対して適用範囲の優位性は確認されたが、誤りを含む実装を生成しうる場合について実験を行っておらず信頼性の向上は確認されていなかった。また、部品単体の証明に長い時間がかかることも課題であった。

2.5 研究の目的

これまでは誤りを含む実装を生成しうる場合について両手法を比較していなかった。そこで、本研究ではそのような場合となる部品と要求を用意して両手法を比較し、信頼性の向上の有無を検証する。また、佐々木の手法の課題であった検証時間を短縮させる方法を提案する。

3 信頼性向上を確かめる追加実験

新たに部品用のソフトウェアと合成するソフトウェアの要求を作成し、2 つの手法によって不足部品を自動生成する実験を行った。実験の結果を表 1 に示す。大久保の手法で生成された一部の部品は取得部品から抽出した配列の長さが十分でない等の理由で操作に誤りを含んでい

表 1: 2 つの手法の比較実験の結果

不足部品	大久保の手法	佐々木の手法
abandon_2	○	矛盾検出
abandon_3	○	矛盾検出
finish_repair_1	誤り生成	矛盾検出
lend_1	誤り生成	矛盾検出
repair_2	誤り生成	○
return_1	誤り生成	○

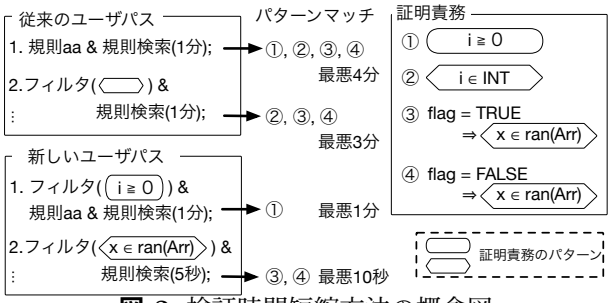

図 2: 検証時間短縮方法の概念図

た。佐々木の手法では取得部品から抽出した定数に対して置換前に満たすべき制約の検証を行った結果、自動生成する前に定数値と制約との間の矛盾が検出された。また、佐々木の手法では誤りを含む部品が生成されなかったが、大久保の手法では誤り無く生成できた部品を定数値の検証で矛盾を検出したことで生成できなかった。

4 検証時間の短縮

佐々木の手法中で検証のために再利用される定理証明器のコマンド列はユーザパスというファイルにまとめられ未証明の証明責務に対して上から順に適用される。また、一部のコマンドは規則の検索等をタイムアウトまで行う。検証時間が長かった理由としてタイムアウトがあるコマンドが想定されていない場面で呼び出されることが考えられる。ユーザパスにはコマンド列ごとに適用する証明責務の結論のパターンを指定できるフィルタと呼ばれる機能がある。これまではそもそもフィルタを指定していなかったり、指定されたパターンに対して複数の証明責務がマッチする状態になっていた (図 2)。そこでまずフィルタのパターンとして各証明責務の結論をそのまま指定し、同じ結論を持つ証明責務に対応するコマンド列はタイムアウトが設定されていればその時間を短く設定する方針を取る。これにより証明責務の結論ごとに適切なコマンド列を呼び出せるようになる。また、同じ結論を持つ証明責務には複数のコマンド列が呼び出されうるが、その時の実行時間を短くできる。

5 検証時間短縮の評価実験

検証時間短縮の効果を評価するために、従来のユーザパスと証明責務の結論をパターンに持つフィルタを設定したユーザパス、またそのフィルタを持ちコマンドのタイムアウト時間を短くしたユーザパスについて検証時間を比較した。実験の結果を表 2 に示す。各証明責務の結論をパターンに持つフィルタによって多くの部品の検証時間を短縮できた。また、タイムアウトの短縮によっても一部の部品の検証時間を更に短縮できた。

表 2: 検証時間の評価実験の結果

部品	従来	フィルタ (結論)	フィルタ (結論) タイムアウト短縮
add_2	559 秒	7 秒	7 秒
order_1	551 秒	10 秒	10 秒
sell_1	269 秒	5 秒	5 秒
sell_2	745 秒	9 秒	9 秒
highest_1	1966 秒	88 秒	28 秒

6 考察

6.1 信頼性の比較実験について

大久保の手法では誤りを含む部品が生成されたのに対して、佐々木の手法では生成された全ての部品に誤りが含まれていなかった。このことから今回の実験の範囲では生成される部品の信頼性が向上したと言える。また、MSSS 手法では結合後のソフトウェアの検証を人が行う。生成された部品が誤りを含んでいる場合、この検証時に誤りが発見されその部品を人が作り直すことになり開発の効率が下がるこのことからも MSSS 手法における自動生成手法としては佐々木の手法がより適していると考えられる。しかし、大久保の手法で誤り無く生成できた部品が佐々木の手法で生成されないことがあり、適用範囲の縮小が確認された。これは、定数値に課す制約を実装のデータ構造ごとに決定していることから、一部の局所操作の整合性のために必要無い制約も余分に課せられていることが原因だと考えられる。この問題は定数値に課す制約を実装のデータ構造と局所操作のペアごとに整備すれば解決できると思われる。

6.2 検証時間の短縮の評価について

実験により、証明責務の結論をパターンに持つフィルタによって検証時間を大幅に短縮できる事が分かった。また、タイムアウトの短縮も一部の部品の検証時間の短縮に寄与する事が分かった。

7 終わりに

本稿では新たに行った実験により大久保の手法に対して信頼性の向上は確認できたが自動生成の適用範囲が狭まっている事が分かった。また、検証時間を短縮する方法を提案し実験によって十分に検証時間を短縮できることを確認した。今後は、信頼性を保ったままできるだけ適用範囲を広げること、またモジュール構造を持つ部品への対応が課題となる。

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, 2013
[2] 大久保 稜, 織田 健. 抽象データ型に対応した不足部品の自動生成手法. 第 21 回情報科学技術フォーラム論文集. vol.1 pp.203-204. (2022.09)
[3] 佐々木 孝紘, 織田 健. 形式的ソフトウェア合成手法における部品検証を兼ねた不足部品の自動生成. 情報処理学会第 87 回全国大会講演論文集. vol.1 pp287-288. (2025.03)
[4] 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