P-75

情報通信技術

形式仕様記述を充たす ソフトウェアを合成するシステムの開発

■ 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し、再利用することでソフトウェアの合成を行うモデル充足ソフトウェア合成（MSSS）手法を提案している［1］。

B Methodは形式手法の1つで、集合論と一階述語論理に基づいた仕様記述言語を用いて抽象的な仕様を表すモデルと、これを段階的に詳細化したリファインメントや実装を記述することでソフトウェアを開発する手法である。MSSS手法では、このような整合性が保証されたモデルから実装までの組を部品とし、ユーザの記述する形式仕様を充たすように部品を組み合わせることで新規のソフトウェアを合成する。これまでに合成の手順について提案されてきたが実システムが開発されていなかった。本研究では各手法に含まれる曖昧さを取り除き、また手法間を連携させることで実際にソフトウェアを合成するシステムを開発した。

■ 活動内容

1. ソフトウェア合成手順の整理

① 要求を表すモデルを1代入文ごとに分割し、必要な制約条件を抽出することで細分化モデルを生成する。数学的に等価なモデルは文字列としても一致するようにする処理（字面統一）を含む。

② 文字列として一致する細分化モデルを持つ部品をリポジトリから検索する。

③ 同じモデルで異なる実装を持つ部品の中から他の部品と矛盾なく結合できるものを選択する。

④ 選択した部品をリファインメントの段数を揃えて結合することで要求を充たすソフトウェアを合成する。

手順を整理することで、明示されていなかったデータフローが明らかになった。

2. ソフトウェア合成システムのプロトタイプの構築

B Methodの記述を解析する必要のある細分化等の処理にはStandard ML、リポジトリにはMariaDBを用いた。そのほかの処理にはPythonを用いて部品をオブジェクトとして扱い、処理を順に適用する方針でソフトウェアを合成する。

システム構築にあたって各種データ構造や曖昧だった手順を厳密に定義する必要があった。特に部品の結合可否の判定はアルゴリズムとしての提案がされていなかった。

実装および手法の検証を行うために単純な要求モデルを用いて実際に合成を行う実験を行った。結果として手法の不足点や改善点が見つかったものの概ね合成に成功した。今後はよりデータを増やして実験を行う予定である。

3. モジュール構造を持つ要求モデルへの対応

先述のプロトタイプは要求が1つの状態機械として記述されている場合を対象としていた。B Methodでは複数のモデルに参照関係を持たせてモジュール構造を構築することができる。MSSS手法では参照先のモデルを展開することで1つのモデルの場合に帰着する手法が提案されているものの特別な場合にしか対応していない。現在、この手法を拡張して一般の入力に対応したシステムを構築している。

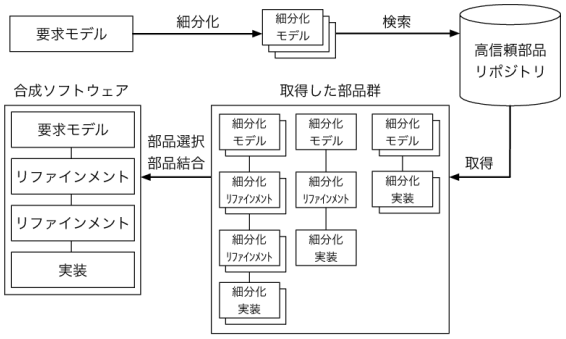

図1. ソフトウェア合成の概要

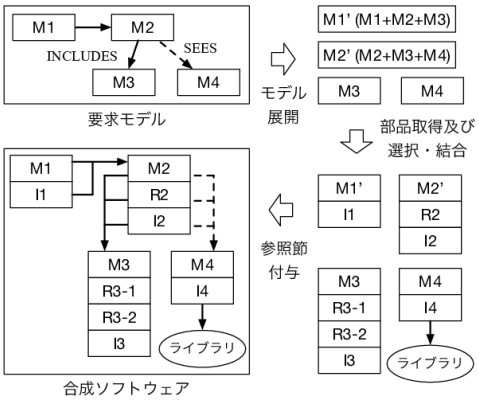

図2. モデルの展開を取り入れたソフトウェア合成の概要

■ 関連情報等

［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.

代表発表者 **田中 涼介（たなか りょうすけ）**
所 属 **電気通信大学大学院 情報理工学研究科 情報学専攻 織田研究室**
問合せ先 **〒182-8585 東京都調布市調布ヶ丘 1-5-1**
TEL: 042-443-5000（代表）
tanaka@tolab.inf.uec.ac.jp

■キーワード: (1) 形式手法
(2) 部品再利用
(3) リポジトリ
■共同研究者: 織田 健 （電気通信大学）