形式手法現場適用への取り組み

山崎　雄大†

形式手法を現場で適用するため，筆者らは状態遷移モデルを Event-B の記述に自動変換し，整合性を自動検証する方法での適用支援を行っている．状態遷移モデルの記法と自動変換のツールは独自に作成した．整合性の検証はモデル検査器と自動定理証明器の利用を主とし，対話証明は任意とした．これらの施策により，現場が無理なく形式手法を適用できると考えている．

Activities for Applications of Formal Methods

Yamazaki Yudai†

In order for developers to utilize formal methods, we devised a way of transforming a state transition model to Event-B description and automatically verifying it. To make it realized, we developed a notation for state transition models and a transformation tool of a state transition model which is written by this notation. Consistency of the model is verified by model checking and automatic theorem proving and optionally by interactive proving.

1. はじめに

筆者らは，IPA の実験[1]や社内の製品開発への適用経験[2]から，形式手法 Event-B[3]の現場適用を目的として技術開発と適用支援を行っている．筆者らが現場適用しようとしている Event-B は，リファインメントに基づく形式手法であり，豊富な機能を備えた統合開発環境 Rodin Platform[4]が存在することが特徴である．Event-B のリファインメントでは，上位の記述と整合するように下位の記述を作成する．この考え方は，前工程の成果物と整合するように後工程の成果物を作成するという典型的なシステム開発の進め方と似ており，現場になじみやすい．また，Rodin Platform は Event-B の記述の編集だけでなく，プラグイン機能により確認(validation)，不具合発見(falsification)，検証(verification)の三つ[5]をサポートしており，その利用価値は大きい．

このような特徴を持つ Event-B だが，その記述は集合論を基礎としており，システムを集合として表現することになじみのない現場にとっては読むことも書くことも難しい．そこで筆者らは，システムを明に集合として表現することなく Event-B の記述を作成する方法として，状態遷移モデルを Event-B の記述に自動変換する方法をとることとした．状態遷移モデルは現状の現場で作成している成果物であり，状態を集合ととらえれば集合論が適用できる．

本稿では，筆者らが状態遷移モデルを用いた Event-B の現場適用支援活動で行った工夫について紹介する．

† 日本電気株式会社 ソフトウェア生産革新本部
Software Process Innovation and Standardization Division, NEC Corporation

2. 状態遷移モデルから Event-B に変換

状態遷移モデルを Event-B に自動変換する手段には，Rodin Platform 用のプラグインに iUML-B[6]という UML ライクな記法によるツールがある．しかし iUML-B は，いくらかは Event-B の文法に沿った集合の式を書かなければならず，明に集合として表現することの緩和効果には不足があった．そこで筆者らは，状態遷移モデルの記法と Event-B への自動変換ツールを新たに作成することとした．

3. 状態遷移モデルの記法

筆者らの考案する記法は，現場が求める表現力を広くサポートするために，現在も改善強化中である．現在までに分かっている主な要求には，例えば次のような表現のサポートがあった．

- リファインメント
  前工程で書いた状態遷移モデルとの整合性を検証するための対応関係の表現
- 状態の階層的な表現や並行状態
  UML ステートマシン図のコンポジット状態や領域のような表現

- 一つの状態遷移モデルを複数の記述に分割して作成可能なこと
  UML ステートマシン図のサブマシンのような表現
- 条件式や代入文の平易な記法
  例えば「a < b ∧ b <= c」という式を「a < b <= c」と書けるようにするなど

現在は，後述の自動変換ツールを作成する手間の都合上，状態遷移モデルの書式を状態遷移表に限定している．将来的には UML ステートマシン図のような書式，延いては状態遷移モデル以外もサポートしたいと考えている．

4. Event-B への自動変換ツール

筆者らの作成する Event-B への自動変換ツールは，状態を集合に，状態遷移を集合の操作に対応させて変換する．例えば，状態 A，状態 B の定義は，次のように変換する．

```
VARIABLES
    状態 A
    状態 B
INVARIANTS
    partition(キャリアセット，状態 A，状態 B)
```

また，状態 A から状態 B への遷移は，次のように変換する．

```
EVENTS
    状態 A から状態 B への遷移 =
    ANY
        x
    WHERE
        x ∈ 状態 A
    THEN
        状態 A := 状態 A ＼ { x }
        状態 B := 状態 B ∪ { x }
    END
```

5. 自動検証の活用

筆者らは，Event-B を適用する際の不具合発見・検証のプロセスを，次のように定めた．

(1) はじめに変換ツールで文法チェックを行う
(2) 文法チェックに通ったら，モデル検査機能で不具合発見を行う
(3) モデル検査で不具合が見つからなくなったら，自動定理証明機能で証明条件の検証を行う
(4) 自動で証明できなかった証明条件に対しては，対話的証明を行う(オプショナル)
(5) 対話的に証明できなかった証明条件に対しては，レビューを行う

(2)のモデル検査機能は，Rodin Platform 用プラグインの ProB for Rodin[7]を使用する．また，(3)の自動定理証明機能は，同じく Rodin Platform 用プラグインの Atelier B Provers[8], SMT Solvers(veriT)[9]を使用する．

6. おわりに

筆者らの方法では，状態遷移モデルに限定したうえで，Event-B 及び Rodin Platform の機能を活用した形式手法を，現場が無理なく適用できると考える．このことを示すために現在は，過去のプロジェクトと進行中のプロジェクトを対象に，いくつかの実証実験を行っている．実証実験で得た知見をもとに，今後も記法の改善や検証能力の向上を進めるつもりである．

参考文献

[1] IPA/SEC，情報系の実稼働システムを対象とした形式手法適用実験報告書，2012.
[2] 山崎雄大，向山輝，橋本祐介，形式手法の開発現場での適用事例，情報処理学会 第 76 回全国大会，2014.
[3] J. R. Abrial, Modeling in Event-B: System and Software Engineering, Cambridge University Press, 2010.
[4] Event-B.org, http://www.event-b.org/
[5] 中島震，「形式手法」の「適用」について，ソフトウェアシンポジウム 2009 形式手法適用 WG.
[6] IUML-B, http://wiki.event-b.org/index.php/IUML-B
[7] The ProB Animator and Model Checker, https://www3.hhu.de/stups/prob/index.php/Main_Page
[8] Rodin User's Handbook v.2.8: Provers, http://handbook.event-b.org/current/html/atelier_b_provers.html
[9] SMT Solvers Plug-in, http://wiki.event-b.org/index.php/SMT_Plug-in