1B-4

形式手法の開発現場での適用事例

山崎　雄大 [1]　　向山　輝 [2]　　橋本　祐介 [3]
日本電気株式会社 [1]　日本電気株式会社 [2]　日本電気株式会社 [3]

1. はじめに

システム開発における設計の信頼性を向上する技術として、形式手法 [1]という数学を基盤とした仕様記述、設計、検証の技術およびツールが知られている。形式手法には、数学的な記法による曖昧さの排除、数学的な検証による整合性の確保といった効果がある。

しかし、形式手法が開発現場に広く普及しているかといえば、そうとは言えない。これは、多くの開発者にとって不慣れな数学的手法への抵抗や、形式手法の適用効果についての不明瞭さなどのためと考えられる [2]。

形式手法の適用効果については近年になって、IPA/SEC による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 [3]などにより、現実的に説得力のある成果が得られつつある。本発表では、数学的手法への抵抗を軽減した形式手法の適用事例の一つとして、状態遷移モデルを用いた事例を紹介する。

2. 形式手法「Event-B」

筆者らは、採用する形式手法を Event-B [4]とし、その統合開発環境に Rodin Platform [5]を利用することを考えている。Rodin Platform を使った Event-B では、確認（validation）、不具合発見（falsification）、検証（verification）という三つの目的 [6]に対して、ProB [7]による仕様アニメーション [8]とモデル検査 [9]、Atelier B Provers [5]と SMT ソルバ [10]による定理証明という手段をとることができる。目的ごとに別々の記述を用意する必要はなく、Event-B の記述だけで全ての目的を達成できることが特徴である。

3. Event-B 採用の課題とアプローチ

Event-B の採用においては、仕様の記述に数学記号を多用することと、定理証明の自動証明率が低い場合に人手での証明を多く行う必要があることの二つが課題になると、筆者らは考えている。本章では、この二つの課題に対して筆者らがとったアプローチを紹介する。

3.1. 状態遷移モデルによる数学記号の隠ぺい

Event-B は集合論に基づく手法であるため、仕様の記述には集合演算を利用する。集合演算で使う数学記号には、帰属を表す∈や、包含を表す⊆などがある。

筆者らは、集合論における集合を、状態遷移モデルにおける状態に対応させ、集合演算を書く代わりに状態遷移モデルを書くアプローチをとった。図 1 にその対応例を示す。このように対応付けることで、状態遷移モデルから単純な変換規則によって Event-B の記述に変換することができる。

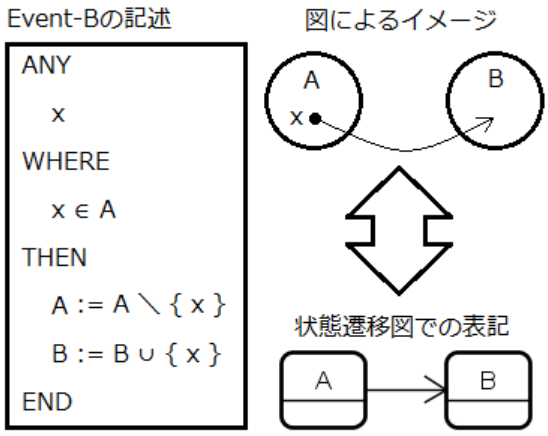

図 1 Event-B の集合演算と状態遷移モデルの対応

3.2. Alt-Ergo による自動証明率の向上

Rodin Platform を利用した Event-B の定理証明では、はじめに自動定理証明器による自動証明が試みられる。自動証明器が証明できなかった定理は、次に人手による証明が行われる。この人手による証明には、数学的な知識が必要になる。

筆者らは、人手による証明は行わず、レビューで対応することとした。しかし証明できない定理が多くなると、信憑性の低下やレビューの手間が懸念されるため、できるだけ自動証明率を向上させたい。Rodin Platform ではサードパーティー製の SMT ソルバを利用できるため、筆者らは経験的な観点から Alt-Ergo [11]を採用することとした。

A Case Study of Formal Methods in Industrial Development
1 YAMAZAKI Yudai, NEC Corporation
2 MUKAIYAMA Akira, NEC Corporation
3 HASHIMOTO Yuusuke, NEC Corporation

4. 事例

筆者らは、第3章にあげたアプローチを、弊社で開発しているサーバ管理ソフトウェア ESMPRO/ServerManager [12]の仕様策定段階で適用し、アプローチの妥当性を確認した。

4.1. 対象機能の概要

対象とした機能は ESMPRO/ServerManager の障害管理機能である。この機能の概要は次の通りである。

- 被管理サーバの温度・電圧などが警告域にある場合に警告を記録する。
- 被管理サーバの温度・電圧などが異常域にある場合に異常を記録する。このときユーザは、被管理サーバを停止させるか、稼働を継続するかを選択できる。
- 被管理サーバの温度・電圧などが警告域から正常域に回復した場合に警告回復を記録する。
- 被管理サーバの温度・電圧などが異常域から警告域、または正常域に回復した場合に異常回復を記録する。

4.2. 状態遷移モデル

表1に対象機能の状態遷移モデルを示す。

表1 対象機能の状態遷移モデル

状態 / 要因		初期	異常	警告	正常	停止
異常検出	停止	記録 = { 警告, 異常 } / 停止		記録 = { 異常 } / 停止	記録 = { 警告, 異常 } / 停止	
	継続	記録 = { 警告, 異常 } / 異常	記録 = {} / 異常	記録 = { 異常 } / 異常	記録 = { 警告, 異常 } / 異常	
警告検出		記録 = { 警告 } / 警告	記録 = { 異常回復 } / 警告	記録 = {} / 警告	記録 = { 警告 } / 警告	
正常検出		記録 = {} / 正常	記録 = { 異常回復, 警告回復 } / 正常	記録 = { 警告回復 } / 正常	記録 = {} / 正常	

この他に、この状態遷移モデルが満たすべき性質を列挙した。以下は、その抜粋である。

- 状態に変化が無いのであれば、何も記録されてはならない。
- 前の状態が「異常」であり、かつ状態が「異常」以外に遷移するのであれば、「異常回復」が記録されていなければならない。

本事例では、これらの満たすべき性質は、直接 Event-B の記述で表現した。

4.3. 形式手法の適用

本事例では、表1に至るまでの途中の版での確認と不具合発見、および最終成果物の検証に形式手法を適用し、形式手法の効果を得た。

4.4. 自動証明率

本事例では Alt-Ergo の利用により、自動証明率が100%に達した。参考までに、Atelier B Provers だけを利用した場合の自動証明率は約21%であった。

5. おわりに

本事例により、次の二つのことを確認できた。

- 状態遷移モデルで数学記号を隠ぺいした場合においても、形式手法の効果が得られたこと
- Alt-Ergo により、自動証明率が著しく向上したこと

本事例では、状態遷移モデルが満たすべき性質については数学記号を隠ぺいすることができなかった。これは今後の課題である。

謝辞

本発表の事例を創出するにあたり、多大なるご助力を頂きました ESMPRO 開発グループの方々に、心から感謝いたします。

参考文献

[1] NASA, What Is Formal Methods?, http://shemesh.larc.nasa.gov/fm/fm-what.html

[2] 株式会社三菱総合研究所, 形式手法入門： 利点・期待と欠点・限界, http://formal.mri.co.jp/outline/fm-introduction-2.html

[3] IPA 独立行政法人 情報処理推進機構, 「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」の公開, http://www.ipa.go.jp/sec/softwareengineering/reports/20120420.html

[4] J. R. Abrial, Modeling in Event-B: System and Software Engineering, Cambridge University Press, 2010.

[5] Event-B.org, Event-B.org, http://www.event-b.org/

[6] 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.

[7] M. Leuschel, The ProB Animator and Model Checker, http://www.stups.uni-duesseldorf.de/ProB/index.php5/Main_Page

[8] 植木雅幸 , @IT MONOist, ライトウェイトな形式手法で高品質な仕様をこの手に！, http://monoist.atmarkit.co.jp/mn/articles/0809/17/news125.html

[9] E. M. Clarke, O. Grumberg , D. Peled, Model Checking, MIT Press, 1999.

[10] C. Barrett , C. Tinelli, SMT-LIB, http://www.smtlib.org/

[11] OCamlPro SAS, The Alt-Ergo SMT Solver, http://alt-ergo.ocamlpro.com/

[12] NEC Corporation, サーバ管理ソフトウェア ESMPRO/ServerManager,ESMPRO/ServerAgent, http://www.nec.co.jp/pfsoft/smsa/