形式仕様記述（Event-B 編）

平成２６年度シラバス

２０１４年1月１０日

国立情報学研究所

トップエスイープロジェクト

代表者　本位田　真一

1. 科目名

形式仕様記述（Event-B 編）

2. 担当者

來間 啓伸

3. 本科目の目的

本科目では、ソフトウェア開発の上流工程における対象のモデル化と検証に関する問題を扱います。形式手法（Formal Methods）は、構文規則と意味規則が厳密に定められた形式仕様記述言語をデザイン記法として用いることで、曖昧性なく解釈できる記述（形式仕様）を構築します。形式仕様言語の意味規則に照らし合わせて、記述に不整合がないか、要求された性質を満たしているか、などを厳密に検証できることが長所です。また、抽象的な記述を出発点として正しさを検証しながら実装に近い記述を構築する、段階的詳細化と呼ばれる方法も提供されます。このような特徴から、形式手法はまずソフトウェア開発の下流工程、すなわち設計工程から実装工程で用いられてきました。本講座の科目である形式仕様記述（B メソッド編）では、上流工程で作成した分析モデルをもとに設計から実装へと進む過程を扱っています。これに対して近年、分析モデルを作成する段階でも形式手法を用いる動きが出てきました。

上流工程で形式手法を使うことのメリットは、システムとそれを取り巻く環境の境界を明確にし、システムが環境の中で整合的に機能することを検証によって確認できる点にあります。形式手法のこのような利用法は、高い安全性が求められるシステムの開発において有効であると期待されていますが、そのようなシステムに限らず、一般にシステム開発の初期段階で要求を明確にする手法として有効である可能性を持っています。

本科目では、上流工程に適合する形式手法として Event-B を取り上げます。Event-B は B メソッドを提案した J.-R. Abrial 氏によって提案された形式手法であり、記法の多くの部分が B メソッドと共通しています。B メソッドの目的は、分析モデルによって明確にされたシステム化部分について、整合性が検証された設計モデルを作成し、その内容に違反しないことを検証しつつ詳細化してプログラムを作成することにあります。一方、Event-B の目的はシステム分析であり、システムとそれを取り巻く環境を一体的にモデル化して、両者の間に不整合がないことを検証します。Event-B でも詳細化は重要な役割を果たしますが、B メソッドとは異なり、複雑な分析モデルを漸進的に記述し検証する手段として使われます。本科目は形式仕様記述（B メソッド編）と連携し、システム分析からソフトウェア開発までの流れを、形式的な記述と検証を基盤として解説します。

本科目では Event-B を通じて形式的なシステム分析手法、すなわちシステム分析段階では何をどのように書くか、それによってどのような検証が行えるか、について考えます。

また、Event-B と B メソッドの違いを通じて、ソフトウェア開発の上流工程と下流工程の役割の違いについて学びます。

4. 本科目のオリジナリティ

本科目では、形式手法を使ったシステム分析について、Event-B と支援ツールを使って一貫して学ぶことができます。この中には、イベントとアクションの考え方に基づく対象の形式的なモデル化、定理証明手法を使ったモデルの整合性の検証、複雑なモデルを構成するための段階的詳細化の利用を含みます。本科目で利用する支援ツールは、これらのモデル化、検証、詳細化を一貫して支援するため、モデル化と分析を系統的に進めることができます。

本科目の特徴は形式仕様記述（B メソッド編）との連携にあり、B メソッドと Event-B を学ぶことで、システム分析とソフトウェア設計、実装の位置付けの違いを、同じ基盤を持つ２つの形式手法を対比させて理解することができます。

表１　従来の教材の問題点と、本科目における解

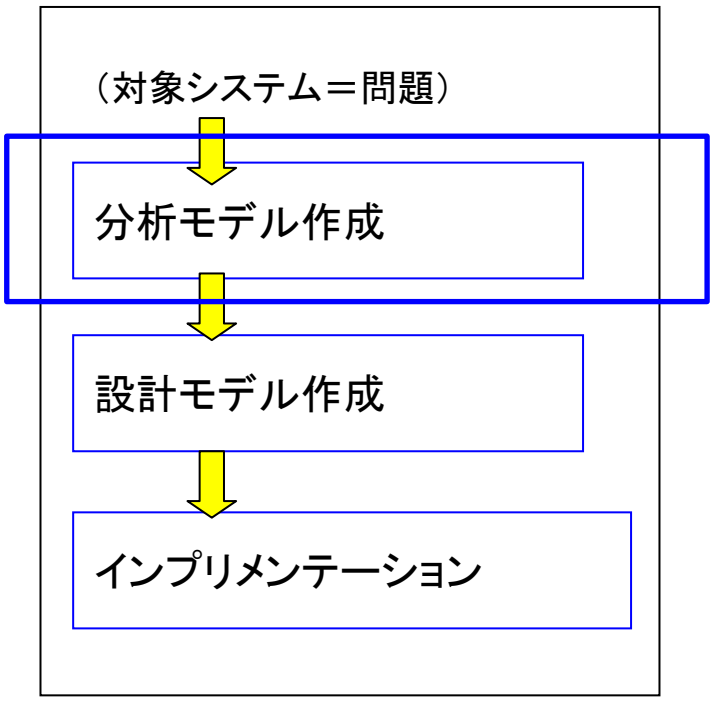
従来の教材の問題点	本科目における解
システムの機能が明確になっており形式的に記述し得ることを形式仕様記述の前提としているため、学んだ内容と現実のソフトウェア開発の間にギャップがある。	システム分析をサポートする形式手法を学ぶことにより、従来の形式仕様記述の前の段階における対象のモデル化と分析についての基本的な考え方を習得する。

5. 本科目で扱う難しさ

Bメソッドでは、ソフトウェアの仕様を形式的に記述して整合性を検証するとともに、段階的詳細化によってプログラムを作成します。このような手法は、整合性が確認された仕様からはじめて、詳細化の正しさを確認しながらプログラムを作成する点で、ソフトウェアの信頼性の向上に有効であることが期待されます。その一方、システムとしての正しさは、最初の仕様に依存しています。Bメソッドでは、最初の仕様を形式的に記述した設計モデルが整合していることは検証しますが、システムの観点から仕様が妥当な機能を提供しているかどうかについては、検証対象ではありません。

最初の仕様がシステムの観点から妥当なものであることを確認するためには、システムについて考慮するだけでは十分ではありません。システムとしての妥当性は、システムを取り巻く環境との整合性によって決まるからです。Event-Bは、システムとそれを取り巻く環境を形式的に記述して整合性を検証するためにデザインされた形式手法で、Bメソッドよりも上流の工程を対象としています。ここで、システムだけでなく環境も合わせて記述し検証するためには、Bメソッドとは異なるモデル化の考え方が必要になります。

開発過程



6. 本科目で習得する技術

本科目では、形式手法 Event-B によるシステム分析について学びます。Event-B の大きな特徴は、イベントとアクションの概念に基づく対象のモデル化と、複雑なモデルの作成における段階的詳細化の利用にあります。段階的詳細化とは、妥当性が確認しやすい抽象的なモデルをもとに、少しずつ段階的に、モデルの内容を複雑化・詳細化していくモデル作成方法です。Event-B では、この詳細化の各段階でモデルの正しさを、定理証明手法を使って検証します。正しいとは、モデルが矛盾していないことを意味する整合性と、下位のモデルが上位のモデルにしたがっていることを意味する詳細化の正当性の両方を含みます。このため、妥当性を容易に確認できる抽象的なモデルから開始して、正しさを検証しながら複雑なモデルを作成します。詳細化の各段階で正しさを確認しているので、不整合を起こすことなく複雑なモデルを分割して記述できる、と期待できます。

Event-B は多様な分野のシステムについて適用評価が進められていますが、分析したい性質は分野によって異なります。本科目では Event-B を通じて、様々なシステムのモデル化と性質の分析を行うための基本的な技術を習得します。

習得項目

１．モデル化手法

　　１．１　アクションシステム

　　１．２　ガーディッド　コマンド

２．詳細化手法

　　２．１　データ詳細化

　　２．２　重ね合わせ

7. 前提知識

本科目で扱う Event-B は B メソッドを発展させた形式手法であり、受講生に B メソッドの基礎知識があることを前提として講義を進めます。したがって、本科目の受講生は次の科目を既に受講済みであるか、受講と同等の基礎知識を有していることが必要です。

- 形式仕様記述（B メソッド編）

次の科目を受講済みであることは、理解を深める助けになります。

- 基礎理論
- 形式仕様記述（基礎編）

また、以下の分野に関する知識を有していることが望まれます。

1. プログラミング言語論
2. ソフトウェア工学

8. 講義計画

第１回　Event-B 概論

- Event-BとBメソッド
- ツールの基本的な使い方

第２回　Event-B 実習

- Event-Bの構文と情報構造の表現

第３回　Event-B 実習

- リファインメント

第４回　Event-B 実習

- リアクティブシステムの記述と検証

第５回　Event-B 実習

- 通信プロトコルの記述と検証

第６回　Event-B による事例演習

- リファインメントを使ったシステム分析

第７回　Event-B による事例演習

- リファインメントを使ったシステム分析

9. 教育効果

本科目を受講することにより、システム開発において形式仕様記述を利用するための基本ノウハウを習得できます。これらのノウハウを各々の開発現場の特性に合わせて適用することで、信頼性の高いシステムを効率的に開発することができます。

10. 使用ツール

本科目では、以下のツールを使います。

- Rodin Platform
  Event-B のための統合支援ツールであり、編集、構文検査、型検査、証明責務生成、証明支援などの機能を提供する
  http://www.event-b.org/

11. 評価

講義中に出題する課題レポートと事例演習レポートならびにグループ発表の評点、出席状況を総合して評価します。課題レポートと事例演習レポートでは、一人一人の受講者について評点を与えます。これにグループ発表の評点を加算し、出席状況と合わせて総合的に各受講者の評価を決定します。

12.参考書

（１）J.-R. Abrial: “Modeling in Event-B,” Cambridge University Press, 2010.
（２）J.-R. Abrial: “The B-Book,” Cambridge University Press, 1996.
（３）J.-R. Abrial: Formal Methods in Industry: Achievements, Problems, Future, Proceedings of ICSE2006, 2006.
（４）A. Romanovsky and M. Thomas (eds.): “Industrial Deployment of System Engineering Methods,” Springar, 2013.
（５）来間：B メソッドによる形式仕様記述, 近代科学社, 2007.

その他、必要に応じて研究論文を紹介します。