形式仕様記述（Bメソッド編）

平成２４年度シラバス

２０１２年1月１３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. 講座名

形式仕様記述（B メソッド編）

2. 担当者

來間　啓伸

3. 本講座の目的

本講座では、形式仕様言語を用いた設計に関する問題を扱います。ソフトウェア開発の設計工程では、上流工程で作成した分析モデルをもとに、プログラムとして実装するために必要な情報を加えた、設計モデルを作成します。設計段階で使われる代表的なデザイン記法である UML（Unified Modeling Language）では、多様なダイアグラム記法によって様々な設計情報を表現することができます。ダイアグラムは直感的に理解しやすいため、UML は産業界で標準的に使われてきました。その反面、UML はダイアグラム記法の意味規則を、モデル間の関連を解析するのに十分な厳密さで規定してはいません。すなわち、設計工程で作られるモデルは相互に整合していなければなりませんが、モデル間の整合性が正確に議論できるほどには、UML の意味規則は厳密ではありません。

一方、厳密さに重きを置き、数学的な概念を基礎とした、形式手法の研究も進んできました。形式手法では、構文規則と意味規則が厳密に定められた形式仕様言語をデザイン言語として用いることで、曖昧性なく解釈できるモデル（形式仕様）を構築します。設計段階で作られるモデルの間に不整合がないことを、形式仕様言語の意味規則に照らし合わせて厳密に検証できることが特徴です。形式手法には様々な手法がありますが、B メソッドは特にソフトウェア設計段階での利用を指向した手法であり、設計工程における一連の作業過程を規定して、各過程での記法と検証方法を提供するとともに、それをツールによって支援します。

本講座では、分析モデルから実装までの間の設計工程を対象として、B メソッドを使った系統的なソフトウェア開発の方法を学習します。形式仕様言語を使ったモデルの記述と整合性の検証を学び、形式手法を通じて設計工程を捉え直すことが本講座の目的です。

4. 本講座のオリジナリティ

本講座では、対象システムのモデル化からプログラムの構成に至る一連のソフトウェア開発過程を、B メソッド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、設計の各段階に対応する複数のモデルの形式仕様記述、モデルの内部に矛盾がないことの検証、モデル間に不整合がないことの検証を含みます。本講座で利用する支援ツールは、これらの記述ならびに検証を統合的に支援するので、演習を通じて形式手法によるソフトウェア開発を一連の流れとして学習できます。また、形式仕様記述（セキュリティ編）で学ぶ Event-B は上流工程での分析モデル作成を指向した形式手法であり、本講座は

Event-B の講座と連携している点にも特徴があります。

表１　従来の教材の問題点と、本講座における解

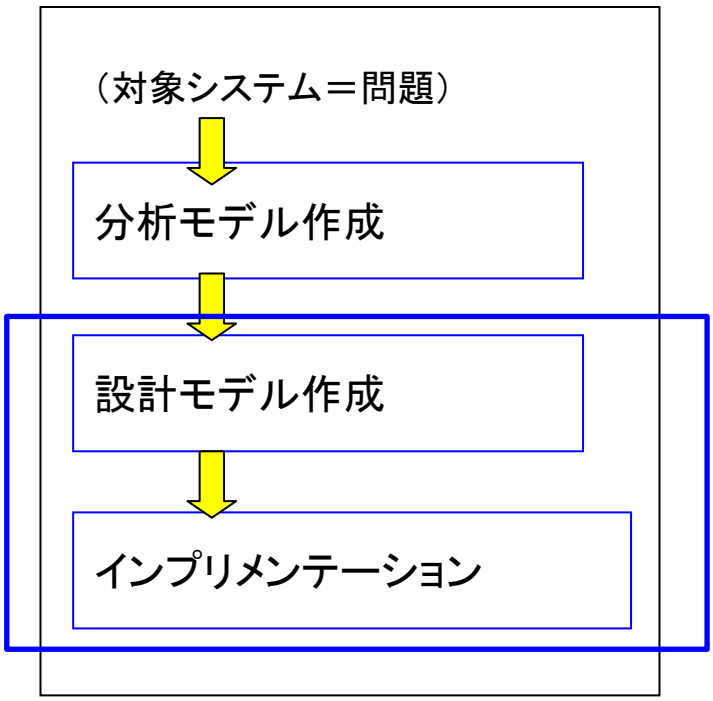
従来の教材の問題点	本講座における解
仕様記述、検証、プログラムの構成が、それぞれの側面で取り上げられており、ソフトウェア開発の一連の流れとして理解することが困難	仕様記述からプログラム構成に至る過程の中で、各段階で何を記述し何を検証すべきかを B メソッドにしたがって示すとともに、統合支援ツールを使って一連の流れを実習する

5. 本講座で扱う難しさ

情報システムは多様な側面を持ちますが、情報の管理という共通性があります。このため、設計の初期段階では、情報の流れを整理し、管理する情報の構造を明確化することが重要です。その上で、情報を管理し加工する処理を設計してゆきます。ここで、後者が前者を満たしているか、すなわち、ある処理の結果、意図通りの情報になっているか、大域的な制約を常に満たしているか、については、設計者によるレビューによって確認されるのが一般的です。ところが、人手によるレビューでは、誤りや漏れを除ききれません。殊に、設計が変更される度に確実にレビューし直すことは、大変困難です。仕様を形式的に記述する目的の一つは、大域的な制約と処理の双方を機械処理可能な言語で表し、レビューを機械化することにあります。

このような目的で作成した形式仕様は、システムの本質を端的に表す役割を担っており、設計者が重要と考えた要件が盛り込まれる一方で、重要でないと考えた要件は省略されています。一般に、このような形式仕様は計算機による実行が不可能であるか、実行可能であっても実行効率が悪く、目的プログラムを得るためにはさらにいくつかの工程を経る必要があります。この工程では、計算機で実行するための詳細が付け加えられ、計算機上での実行効率を上げるための書き換えが行われて、仕様は複雑になり記述量も多くなります。この時、最初の形式仕様に表現されていたシステムの本質が失われてしまっては、意味がありません。最初の形式仕様と整合性を保ちつつ、複雑かつ記述量の多い仕様を得るための、系統的なアプローチが必要です。

開発過程



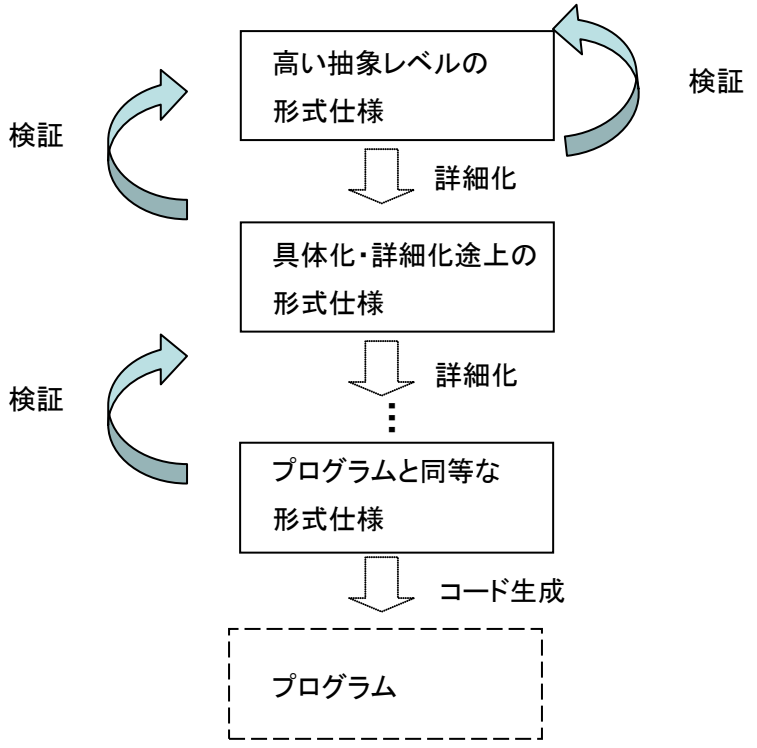
6. 本講座で習得する技術

本講座の前半では、抽象度の高い形式仕様の記述と、定理証明を使った形式仕様の検証について学習します。後半では、抽象度の高い形式仕様から、段階的な詳細化により、計算機での実行効率が良い具体的な形式仕様を構成する方法を学習します。

段階的な詳細化とは、自明な、あるいは、その妥当性が確認しやすい抽象的な記述をもとに、少しずつ、段階的に、記述の内容を具体化・詳細化していく手法です。特に、形式仕様言語を用いることで、この詳細化の各段階で、詳細化が正しいことを検証します。すなわち、正しい抽象的な記述から開始して、正しさを検証しながら具体的なデザインを得る、という手法です。詳細化の各段階で正しさを確認しているため、不具合が混入することがない、と期待できます。

本講座の習得項目は、以下のものです。

１．設計検証
　１．１　形式仕様記述
　１．２　整合性の検証
２．段階的詳細化
　２．１　データ詳細化
　２．２　詳細化の正当性の検証



7. 前提知識

本講座の受講生には、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。

- プログラミング言語論
- ソフトウェア工学

また、基礎知識として次の項目に関する初歩的知識を有しているか、「基礎理論」講座を受講していることが期待されます。

- 集合論
- 命題論理、述語論理

8. 講義計画

第１回　イントロダクション

- 形式手法の特徴と課題

第２回　Ｂメソッドの概要

- 基本概念とツールの使い方

第３回　仕様記述段階（１）

- B 抽象機械記法

第４回　仕様の整合性検証

- 最弱事前条件
- 証明責務と証明

第５回　データ構造の表現

- 関係と関数

第６回　仕様記述段階（２）

- B 抽象機械記法
- 証明責務と証明

第７回　グループ演習（仕様記述）

- 問題設定
- グループ議論

第８回　グループ演習（仕様記述）

- グループ発表・議論
- 仕様記述のまとめ

第９回　詳細化段階（１）

- データの詳細化と処理の詳細化

第１０回　詳細化段階（２）

- リファインメントの記法

第１１回　詳細化の正当性の検証

- 証明責務と検証

第１２回　実装段階（１）

- インプリメンテーションの記法

第１３回　実装段階（２）

- ライブラリ
- 証明責務と証明

第１４回　グループ演習（データ詳細化）

- 問題設定
- グループ議論

第１５回　グループ演習（データ詳細化）

- グループ発表・議論
- Bメソッドのまとめ

9. 教育効果

本講座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

本講座では、次のツールを使います。

- AtelierB
  B メソッドのための統合支援ツールであり、編集系、型チェッカ、証明責務生成系、証明支援系を含む。

11. 実験及び演習

第２回から第６回

Ｂメソッド演習

（第８回までに課題レポート提出）

第７回から第８回

仕様記述の事例演習

演習進捗のグループ発表

（事例演習レポートを作成、提出期限は後日通知）

第９回から第１３回

Ｂメソッド演習

（第１５回までに課題レポート提出）

第１４回から第１５回

データ詳細化の事例演習

演習進捗のグループ発表

（事例演習レポートを作成、提出期限は後日通知）

事例演習は、グループ学習によって行います。受講者は、グループに分かれて以下を行っていただきます。

- 題材仕様の理解
- モデル化方針の検討
- 形式仕様記述
- 結果の報告
- 事例演習レポートの作成

事例演習では、以下の資料を配付します.

- 題材仕様に関する資料
- モデル化の指針
- 題材仕様の基本部分に関する形式仕様記述例

12. 評価

以下の４つのレポートならびにグループ発表の評点と出席状況を総合して評価します。

- ２つの課題レポート
- ２つの事例演習レポート
- 第８回と第１５回のグループ発表

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。

13.教科書

- 来間啓伸：B メソッドによる形式仕様記述，近代科学社，2007.

14.参考書

- S. Schneider ：“the b-method: an introduction,” palgrave, 2001.
- J.-R. Abrial ：“The B-Book,” Cambridge University Press, 1996.
- 玉井哲雄：ソフトウェア工学の基礎，岩波書店 2004.
- B Language Reference Manual, ClearSy, http://www.b4free.com

その他、必要に応じて研究論文を紹介します。