

工業高等専門学校に対する 形式手法 B-Method の学生実験の実践

大西 孝臣^{1,a)} 吉村 斎¹ 阿部 司¹ 稲川 清¹ 山本 椋太² 堀 武司³

受付日 2019年7月31日, 採録日 2020年1月16日

概要: 本稿では, ソフトウェア技術者の素養としての形式手法の体験を目標に, 工業高等専門学校 (工業高専) の本科 4 年生のクラス全員に対して形式手法 B-Method の学生実験を実践した. 当実験は, 形式仕様記述・定理証明とモデル検査の双方を実施項目に含有しており, 「フォーマルメソッド利用のレベル」におけるレベル 0 よりレベル 2 までの手順をひとつとって体験させることを目指す. 結果, 受講学生より, ツールの使用手順の理解度や B-Method への親近感について一定の評価を得ており, ツールを導入したいという希望が出ているなどの一定の関心を得ており, 学生の形式手法に対する敷居を下げることに成功しており, 目標を達成するものであり, 人材の養成確保の問題解決に向けて寄与するものと考え.

キーワード: 形式手法, B-Method, 学生実験, 工業高等専門学校

A Practice of Student Experiments of the Formal Method, B-Method Applied for Students of Institute of Technology

TAKAOMI OHNISHI^{1,a)} HITOSHI YOSHIMURA¹ TSUKASA ABE¹
KIYOSHI INAGAWA¹ RYOTA YAMAMOTO² TAKESHI HORI³

Received: July 31, 2019, Accepted: January 16, 2020

Abstract: This paper presents our design and launching of student experiments of the formal method, B-Method applied for the whole members of the 4th-grade class of an Institute of Technology with the aim of giving opportunities to commit a formal method as the software engineer's fundamental knowledge. Our experiments include both the tasks of formal description, theoretical proving, and the task of model checking. These tasks challenge to give students the opportunities to commit evenly from level-0 to level-2 according to "the levels of formal method usage." As the results, we got some certain evaluations from students about the understanding how to use the tools, and about the familiarity to the B-Method. We got some students' interesting with the requests to install the tools to their own PCs. Our practice succeeded to render students friendlier with the formal methods. Therefore, we have achieved our aim mentioned above. We think our practice contributes for the challenge to train and grow the human resource talented in formal methods.

Keywords: formal method, B-method, student experiment, institute of technology

1. はじめに

ソフトウェアシステムの開発現場において, 自然言語記述による仕様には曖昧な表現が含有されているという理由

から内容の矛盾や誤りの指摘が困難になる場合があるため, 仕様の記述が厳密で曖昧性を排除できる形式手法が注目されている [1]. 一方, 形式手法の普及は進んでいるが初歩的な技術利用にとどまる場合が多く, 普及推進のための技術教育が求められており [2], 以前よりその導入コストの高さと並行して人材の養成確保の問題が課題にあげられている [3].

文献 [1] によると, モデル検査ツールを使いこなすには数学や論理学の知識が必要になってくるが, そのつど勉強すればよいとあり, 文献 [4] によると, 形式手法の導入は簡単ではなく "難しい" が, 初めからすべてを先に学ぶ必要は

¹ 苫小牧工業高等専門学校
National Institute of Technology, Tomakomai College,
Tomakomai, Hokkaido 059-1275, Japan
² 名古屋大学
Nagoya University, Nagoya, Aichi 464-8601, Japan
³ 北海道立総合研究機構
Hokkaido Research Organization, Sapporo, Hokkaido 060-0819, Japan
^{a)} ohnishi@tomakomai-ct.ac.jp

なく、ツールの使い方の基礎を学習して仕様を記述し始める試みでもよく、“難しさ”とされるものの本質は形式手法の使用の是非とは無関係なところにあるとの立場もある。

海外においては形式手法の教育に関する研究は多数存在しており [5], 例をあげると, 米国には大学学部レベルや高等学校・中学校レベルも含め, ソフトウェア科学の教育課程に数学的論理思考 (mathematical reasoning) の導入を試みるコミュニティが存在する [6].

国内における形式手法の教育としては, 主に企業の若手エンジニア向けの取り組みとして, 国立情報学研究所のトップエスイープロジェクト [7] が 2004 年より 10 年超の実績 [8] をあげており, 大学と共同した普及活動も目指している。

同時に, 2004 年に, 産業技術総合研究所システム検証研究センターが組織され [9], 2006 年に形式手法のモデル検査分野の 4 日間の教程の入門書 [10] を発行している。2004 年に, 北陸先端科学技術大学院大学の 21 世紀 COE プログラム「検証進化可能電子社会」が採択され [11], 博士課程大学院生への教育実践を行っている。2010 年に, 情報処理推進機構のソフトウェア・エンジニアリング・センターが形式手法人材育成作業部会を発足させ [12], 人材の育成方法の開拓や入門書 [13] の作成を行っている。

大学における教育として, 情報処理学会による, 大学の情報系学科・コースの学士課程の教育における情報学分野の参照基準であるカリキュラム標準 J17-SE [14] において, 形式手法は学習対象たる知識体系を構築している項目である BOK (Body of Knowledge) として位置付けられているのと同時に, 情報基礎科目の上位としてソフトウェアエンジニアリング技術を扱う SE 科目として位置付けられている。

大学の情報系学科・コースと同じく工学系の高等教育機関であり, 筆者大西らが所属する工業高等専門学校 (以下, 工業高専と呼ぶ) の情報系の学科・コースにおいても, 情報技術教育の裾野を広げるべく形式手法の導入を検討している。しかし, 冒頭で述べたとおり, 形式手法には人材の養成確保の問題があり, そのうえ, 企業や大学などでの導入事例と比較して, 工業高専において形式手法を導入する際には, 以下の考慮すべき問題が存在する。

- 情報系においてもハードウェア分野の教授にも時間を使っているため [15], 形式手法の教授に費やすための講義・実験・実習そのものの時間数が不足している。
- 教養系で大学教養レベルの数理論理学を教授しておらず [16], 専門系でも教授する時間が少なく [15], 学生は, 形式手法に触れる時点で初見に近い状態である。
- 講義・実験・実習の時間数に収まる規模で, かつ, ソフトウェアシステムの開発現場で活かせる内容を備えた題材が普及しておらず, 実践例も少ない。

上記の問題については, 工業高専の学生 (以下, 工業高専

生と呼ぶ) に導入しようとする工夫や試みがなされていないかかったところにも起因するものと考ええる。また, 前述の文献 [1] や文献 [4] により見る立場をふまえば, まずツールに触れさせるアプローチで工業高専生への形式手法の導入を試みるべきであり, プログラミング言語での実習を行っている時分の工業高専生に対して, 形式手法のツールに触れさせることを通じて「ソフトウェア技術者の素養としての形式手法を体験させる」ところに学生の将来にとっての意義があるものと考ええる。

本稿では, 形式手法における人材の養成確保の問題への解決策の 1 つとして普及推進の技術教育の裾野を広げるべく, 筆者大西らが所属している苫小牧高専の創造工学科情報科学・工学系 4 年生 (以下, 学生と呼ぶ) のクラス全員に対して, 形式手法 B-Method (以下, B と呼ぶ) を手段として, 「ソフトウェア技術者の素養としての形式手法の体験」を目標に, 形式仕様記述・定理証明とモデル検査の双方を実施項目に含有する学生実験を実践した。

工業高専における形式手法の教育の実践については, 令和元年度よりの工業高専専攻科生向けの選択科目の講義の例 [17] があるが, 工業高専本科生のクラス全員に対する必修での実践例は皆無である。

教育実践による, 本稿の主な貢献の位置づけを次のとおりに考える。

- 形式手法の導入を容易にすることを目指した教育手順の提案・教育教材の開発および実践への適用
- 形式仕様記述・定理証明とモデル検査の双方を実施項目に含有する教育手順の提案および実践報告
- 形式手法の導入教育における, 学習者による自己評価項目の試行的提案および実施報告
- 教育実践の結果や成果をふまえた教育手順・教育教材の評価

本稿の次章以降は, 次のように構成されている。

2 章においては, 本稿における実験で採用する形式手法の特徴について述べ, 実践した学生実験の実施の背景・実施内容の詳細 (使用文書・実験の手順・手順ごとの学習目標) について述べ, 実践の教育効果を議論するための research question (以下, RQ と呼ぶ) を定義する。3 章においては, 学生実験の実施結果・実験実施後に行った学生アンケートの結果・実験実践を通じて得た知見を述べ, 2 章で定義した RQ への考察を行い, 本稿における教育実験の評価について述べる。4 章においては, 関連分野の先例となる教育実践との比較について述べる。5 章において, 本稿のまとめを述べる。

2. 学生実験の実施

2.1 形式手法 B-Method について

種々ある形式手法の中から, 本稿における実験においては B を採用した。B は Z 記法を含有する, VDM と同様の

モデル指向型あるいはモデル規範型 (model oriented) の形式手法である [18], [19] (さらに 2.3 節後半の, Atelier B におけるモデル記述の特徴についても参照)。

苫小牧高専において B を選択した背景として, 筆者らが産業界よりの知見を得た経験がある。筆者大西らは平成 26 年度よりの 3 年間, 経済産業省北海道経済産業局の戦略的基盤技術高度化支援事業『農業機械のさらなる高度化と海外進出に資する次世代電子制御ソフトウェア基盤の開発』[20] に参画しており, 当事業を通じて B に関する, 工業高専としては得難い知見を蓄積することができた。

B は文献 [21] で言及されている「フォーマルメソッド利用のレベル」のレベル 2 でのシステム開発の成功事例の実績が存在しており [22], ソフトウェアシステムの開発現場に適用できるレベルのモデル検証支援ツールを無償で入手できる。そのため, 実践的な環境を無償で構築でき, 学生実験への適用に向いている。さらに B には, 同一モデルにて形式仕様記述・定理証明とモデル検査の双方を実施できるツール [23], [24] が存在する (2.3 節参照)。

B を手段とする実験の実践に向け, 筆者大西と堀は, これまで工業高専生に向けた実験に導入するための題材探しを行い, B によって記述したモデルを提案してきており [25], [26], このモデル記述の際に求められる数理論理学の指導を含めて実験の時間内に収める目途を立てた。

2.2 実験を受講する学生について

実験においては, 約 10 名を 1 班とする学生を対象にする。クラス全員を対象にし, 本実験を除く形式手法の教授の機会はないため, 受講者のうちの約 9 割にとっては, 当実験は形式手法に接することのできる唯一の機会となる。

学生は, 実験受講前までに, 教養系で高校数学レベルの集合と命題の関係を学んでいる。専門系の座学で本実験の実施と同じ学期に同時進行の形で, 集合・写像, 命題論理・述語論理・正規言語・文脈自由言語の基本概念やソフトウェア開発の手順を学んでおり, 本実験の受講が先行する学生が存在する。本実験よりも後の学期の演習・実験において, (形式的手法をとまわらない) UML を活用したモデリングやプロジェクト形式のソフトウェア開発を学ぶ。

2.3 実験環境について

学生用 PC は CPU: Intel Core2Duo (3.00GHz), RAM: 4.00GB, OS: Windows10 Professional を 1 名につき 1 台与える。学生用 PC においては, 2.5 節で述べる実験指導書などを PDF ファイルですべて閲覧できるようにした。

B のツールとしては, B のモデル記述支援および定理証明ツールである仏国 ClearSy 社の Atelier B Ver.4.5.1 [23], および, 独国ハイニンリッヒ・ハイネ大学が開発した B 記述のモデル検査ツールである ProB Ver.1.8.0 [24] を用いる。

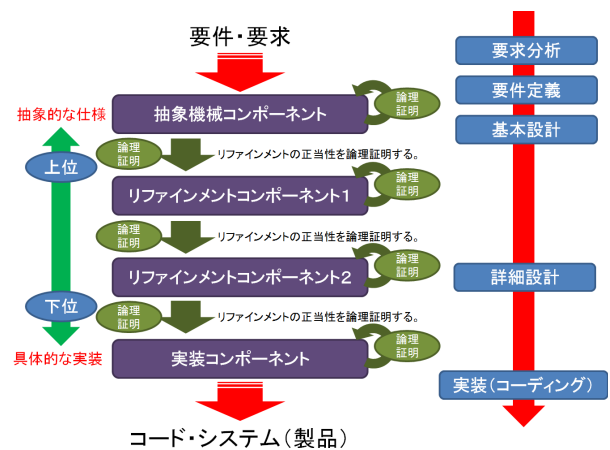


図 1 Atelier B におけるリファインメント

Fig. 1 Refinement in Atelier B.

Atelier B におけるモデル記述においては, 図 1 に示すように, 上位の抽象機械コンポーネントにおいては, 要件・要求に対する分析・定義や基本設計の段階で仕様として詳細に規定することを避けるために集合や非決定的代入などの記法が用意されており, リファインメント (詳細化) [21], [22] と呼ぶ段階的変更を経て, 下位の実装コンポーネントにおいては決定的で実行可能なプログラム相当の記述へと到達させる。B には, ソフトウェアシステムの開発に際して, このリファインメントの過程を経ることにより, モデル記述におけるループ構造や抽象的データなどを実装段階相当へと到達させる機能が用意されている [19], [27] (2.4 節後半 (実験の限定事項) および 3.5 節 (自学習教材) 参照)。

2.4 実験の構成について

実験は 1 週分あたり 3 時限 (実質 140 分) × 2 週で行う。

1 回目 (第 1 週目) の実験 (以下, 実験 1 と呼ぶ) では静的モデルの記述をテーマとして, 文献 [28] にある演繹論理パズルに対する形式モデルを記述させて, ProB の制約充足ソルバ機能を用いてパズルの求解をさせる。

2 回目 (第 2 週目) の実験 (以下, 実験 2 と呼ぶ) では, 実験時間の制約や状態爆発問題の回避のため, たかだか 4 つの状態に遷移する小さな動的モデルの記述をテーマとして, Atelier B におけるリファインメントおよび定理証明, ProB におけるアニメーション [24], [29], LTL 式 (linear temporal logic formula, 線形時相論理式) を用いたモデル検査を行わせる。

本稿で実践する学生実験においては, 「ソフトウェア技術者の素養としての形式手法の体験」という目標を達成すべく, 対象とするモデルの規模は小さいが, 文献 [21] で言及されている「フォーマルメソッド利用のレベル」におけるレベル 0 よりレベル 2 までの手順をひとつとって体験させることを目指す。

表 1 フォーマルメソッド利用のレベルと実験の手順ごとの学習目標との対応

Table 1 Mapping from the learning goals, for each procedure of experiments, to the levels of formal method usage.

◆レベルの名称			
レベルの内容			
レベル内容の分類と学習目標		実験1	実験2
◆レベル0: 形式仕様記述			
数学的な記法を用いて厳密な仕様を記述し、証明や分析までは行わずに、この記述を基にしてプログラムを開発する。			
数学的な記法を用いて厳密な仕様を記述する。		(1-1)	(2-1)(2-2)
数学的な記法を用いた厳密な仕様記述を基にしてプログラムを開発する。		—	(2-6)
◆レベル1: 形式的開発および検証			
プログラムの性質を証明したり、詳細化により仕様からプログラムを作成する。			
プログラムの性質を証明する。		(1-2)(1-3)	(2-5)
詳細化により仕様からプログラムを作成する。		—	(2-10)(2-12)
◆レベル2: 機械支援による証明			
定理証明器や証明支援器を用いてプログラムの性質を証明する。			
定理証明器を用いてプログラムの性質を証明する。		(1-2)	(2-8)(2-9)
証明支援器を用いてプログラムの性質を証明する。		(1-3)	(2-11)(2-13)

実験1と実験2のそれぞれについて、2.7節より2.12節までにおいて示す実験の手順ごとの学習目標を設けた。「フォーマルメソッド利用のレベル」の各レベルと各実験の手順ごとの学習目標との対応について表1に示す。

この表における各レベル内容の細分については本稿で独自に行った。また、産業界が各レベルに要求する水準と比較して、学習目標がその水準を満たしていない事項については、本節で後述する。

1章中盤で述べた工業高専において形式手法を導入する際に考慮すべき問題点として、および、本節で先述したように、前提とする工業高専生のスキル、および、実験時間の制約がある。あわせて、一般に工業高専においては、学年制のカリキュラムとなっており、実験を含む必修科目であれば1科目でも科目単位が取得できなかった場合には、原級のすべての科目の再履修が必要である。時間制約がある実験においても、クラスの一部の学生のみが達成すればよいような高水準の課題を設定できないという事情や風土がある。

よって、本稿で実践する実験の計画に際し、以下の工夫や制限を行った。

実験1においては、形式モデルが正しく記述されていれば、定理証明において、対話証明に頼らずに自動証明のみによって検証を通過することで、制約充足ソルバが唯一解を導出可能になるよう、題材を採択して実験設計をした。

実験2においては、実験の指導者が提示する規模が小さい動的モデルの仕様に対して、状態遷移表を作成させて、形式モデルにおける論理式への定式化に向けてのハードルを下げるようにした。論理式への定式化に際しても、2.9節で述べる becomes such that 非決定的代入を採用し、形式モデルにおけるリファインメントはこの代入式における冗長性の排除の手続きに限定した。

したがって、2.3節で述べた、ソフトウェアシステムの開発に多く求められる、モデル記述におけるループ構造や

抽象的データなどを含まない題材に限定した。

また、「フォーマルメソッド利用のレベル」のレベル1においては「詳細化により仕様からプログラムを作成する」とあるが、実験時間の制約より、令和元年度の実験においては、プログラムの自動生成を行わず、プログラムを生成する直前の段階までに限定してリファインメントを行うこととした(3.7節参照)。

実験時間の制約により、Atelier Bにおける定理証明を経た、仕様の厳密さや安全要件が保証された形式モデルをProBに引き継いでいるため、モデル検査ツールの実験としては、状態遷移を手作業で追跡するアニメーションとLTL式を用いた状態パス探索と安全要件検証の追認に限定した。

2.5 学生への実験指導書などの配布

受講する学生には、以下の実験指導書他の文書を実験前の自学習用に印刷物として配布した。

(1) 実験指導書—形式手法

実験手順のほかに、ソフトウェアシステム開発における形式手法の特徴[30]、形式手法に基づく種々の手法の中でのBの特徴[21], [22], [30]、Bによるモデリングの特徴であるリファインメント[21], [22]について載せた。

(2) 実験指導書別冊

各実験班で共通とする例題について、問題文、学生によるモデルの記述の発散を防ぐための集合名・定数名/変数名・変数の初期設定・操作名などの問題に対する制約、学生に完成させるために未完成のままにした写像・関数の対応図や状態遷移表を載せた。

(3) B-Methodの文法について—Atelier B編

Bの文法の説明のほかに、Bによるモデル記述の際に求められる写像・関数、述語（全般的な説明/不変条件）、代入（決定的/非決定的）、操作に関する説明を載せた。以下のPDFファイルを、学生用PCで閲覧できるようにした。

(4) Atelier Bの操作について（Atelier B 操作手順書）

プロジェクト・コンポーネントの作成・編集、自動証明/対話証明の手順を載せた。

(5) ProBの操作について（ProB 操作手順書）

静的モデルに対する制約充足ソルバ機能を用いた演繹論理パズルの解導出までの手順、小さな動的モデルに対するアニメーションの実行の手順、LTL式の書式の説明、LTL式を用いたモデル検査の手順、LTL式を用いた状態パスの探索の手順を載せた。

(6) B-Method 文法簡易一覧

各文法の概要のほかに、使用される記号のASCII表示、JIS表示、数学表示（Unicodeの符号位置）を記載した。

(7) その他、追加説明書

実験1において、当初、例題のモデルにある記述のみの

提示では、関数・逆関数を複合で参照を行う際にマップレット (1→) を使用できないという B の文法を学生が読み取れなかったため、追加の説明資料を作成した (3.4 節 (2) 参照)。

(8) 課題 (実験 1・実験 2)

各実験班で異なる課題を、完成したモデル記述を除いて、上記 (2) と同じ書式で用意した。

2.6 1 週分 (実験 1・実験 2) の実験の構成

2.4 節の冒頭で述べた実験日程における 1 週分 (実験 1・実験 2) の実験の指導者と受講学生との間で行われる手順についてまとめたものを図 2 に示す。

実験 1 あるいは実験 2 それぞれの 1 週分の実験は、1 題のモデル記述の例題と、1 題のモデル記述の課題を学生が実施することで構成される。最初に実施した実験班に対しては、3 題ほどの課題を実験の指導者が準備していたが、実施時の学生のスキルとのバランスをとり、令和元年度の実践においては、課題を 1 題にすることとした。

令和元年度の実践においては、例題および課題の実施が終了したならば、学生よりアンケート調査を行った (3.3 節参照)。

実験の指導者は、実験 1 あるいは実験 2 それぞれについて、学生に実験日程後の 1 週間以内の実験報告書の提出を課する (2.13 節参照)。

2.7 実験 1：静的モデルの記述

2.4 節の冒頭で述べた実験日程における実験 1 においては、文献 [28] にある演繹論理パズルに対する形式モデルを学生に記述させて、ProB の制約充足ソルバ機能を用いてパズルの求解をさせる。

実験 1 の学習目標を以下のように設定し、指導者より学生へ教授する。

- (1-1) 演繹論理パズルの問題文を自然言語仕様に見立て、パズル問題文にある制約条件を数学的記法に基づく述語として記述できる。
- (1-2) 演繹論理パズルに対する形式モデルにて記述されたパズル問題における制約条件となる述語の無矛盾を証明できる。
- (1-3) 演繹論理パズルを求解する、別解不存在を確認することを通じて、形式モデルの厳密性を証明できる。

実験の指導者と受講学生との間で行われる手順についてまとめたものを図 3 に示す。

例として、文献内の演繹論理パズルにおける問題とその答えについて、装飾を外した要約を図 4 に示す。

図 4 の演繹論理パズルの問題文を基に、図 5 にあるように、Atelier B のシステムモデルの構文構造への対応が付けられた形で、実験の指導者が形式モデルのテンプレート (SETS 節 (集合名と集合要素)・CONSTANTS 節 (定

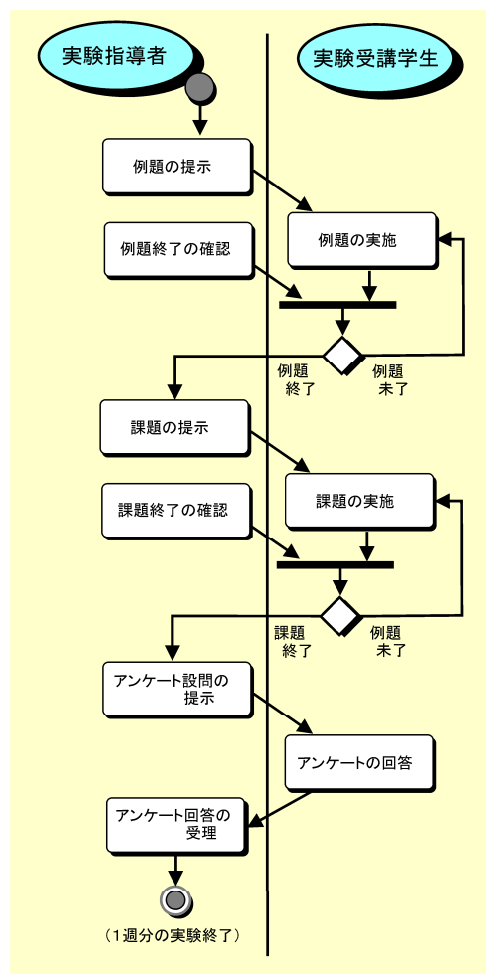


図 2 1 週分 (実験 1・実験 2) の実験の手順

Fig. 2 The procedure of experiment for every week (Exp.1 and Exp.2).

数名)・PROPERTIES 節の一部 (関数型宣言・別解が存在しないことを確認させるためのパズル解の論理否定)) を学生に提示し、学生にパズル問題における制約条件を PROPERTIES 節の述語として追加させることで形式モデルを完成させて、定理証明をさせる。図 5 の最下部のコメントアウト部は、パズルの求解の際に、別解が存在しないことを確認させるために設けたものである。

図 4 の演繹論理パズルに対する形式モデルに対する定理証明の結果を図 6 に示す。

この定理証明において、すべての証明責務は自動証明が行われ、対話証明を求められないように題材を採択している。

続いて、ProB に形式モデルを読み込ませることで、演繹論理パズルの求解を実施する。学生および指導者が求解の結果として解候補数が 1 になるのを確認したならば、学生は図 5 の最下部のコメントアウト部にあるようなパズル解の論理否定を PROPERTIES 節の述語に加えて、求解を実施した結果の解候補数が 0 であることにより、先程の求解の結果であった解候補は誤りである別解ではないことを

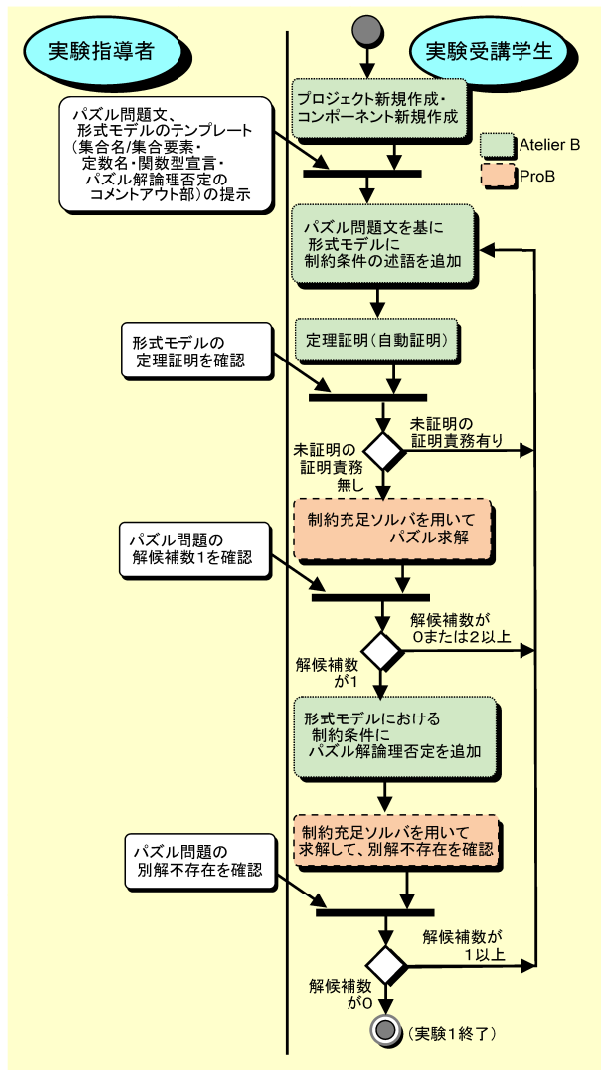


図 3 実験の手順 (実験 1)

Fig. 3 The procedure of experiment (Exp.1).

- ・ 4名の人物イ、ロ、ハ、ニが、a歳、b歳、c歳、d歳と全員が異なる年齢(順不同)である。これらの人物は、それぞれ、とある物を1つ以上(自然数)所有している。
 - ・ b歳の人物とロの2名で、計4つ所有している。
 - ・ c歳の人物とハの2名で、計3つ所有している。
 - ・ a歳の人物とニの2名で、計3つ所有している。
 - ・ c歳の人物とイの2名で、計4つ所有している。
 - ・ イ、ロ、ハ、ニの4名で、計8つ所有している。
 - ◆上記の「人物-年齢-物の所有数の関係」を具体的に述べよ。
- (答え: イ-d-3, ロ-a-2, ハ-b-2, ニ-c-1)

図 4 演繹論理パズルの問題と答えの要約 (実験 1)

Fig. 4 Summary of both question and solution of a deductive logic puzzle (Exp.1).

学生および指導者が確認する。不完全な記述や誤った記述のモデルを読み込ませた場合、導出される解候補数の規模が大きくなり、求解の結果の表示が遅くなる懸念があるた

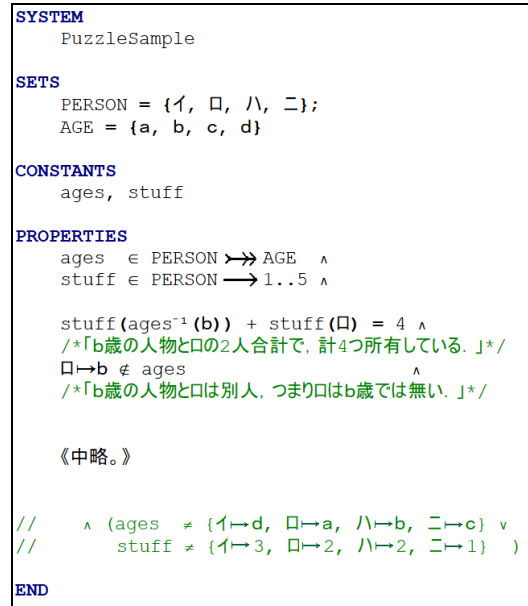


図 5 演繹論理パズルの B の構文構造への対応付け

Fig. 5 Semantic mapping about a deductive logic puzzle onto the syntax structure of B-Method.

コンポーネント	型チェック	証明責務生成	証明責務	証明済	未証明
PuzzleSample	OK	OK	25	25	0

図 6 静的モデルに対する定理証明の結果

Fig. 6 Result of the theoretical proving for a static model.

め、実行時間を計測した結果として、ProB の環境変数の設定により解候補数の最大値を 1,000 に制約することにした [26].

2.8 実験 2: 小さな動的モデルの記述 (1)

(問題の提示より状態遷移表の作成まで)

2.4 節の冒頭で述べた実験日程における実験 2 においては、ただか 4 つの状態に遷移する小さな動的モデルを学生に提示して、仕様の曖昧さを排除した状態遷移表を作成させるという手順をふませたうえで、形式モデルを学生に記述させて、定理証明およびモデル検査のそれぞれのアプローチによるモデル検証を行わせる。

まずは、実験 2 における実験の指導者による問題の提示より学生による状態遷移表の作成までについて述べる。

学習目標を以下のように設定し、指導者より学生へ教授する。

(2-1) たかだか状態数 4 の小さな動的モデルの問題文より「失敗」状態の読解・実験指導者への提案ができる。

(2-2) 小さな動的モデルの問題文より仕様の曖昧さを読解して実験指導者に問い合わせ、自然言語仕様の曖昧さを解消できる。

(2-3) 小さな動的モデルの問題文より仕様の曖昧さを排除した状態遷移表を記述できる。

実験の指導者と受講学生との間で行われる手順について

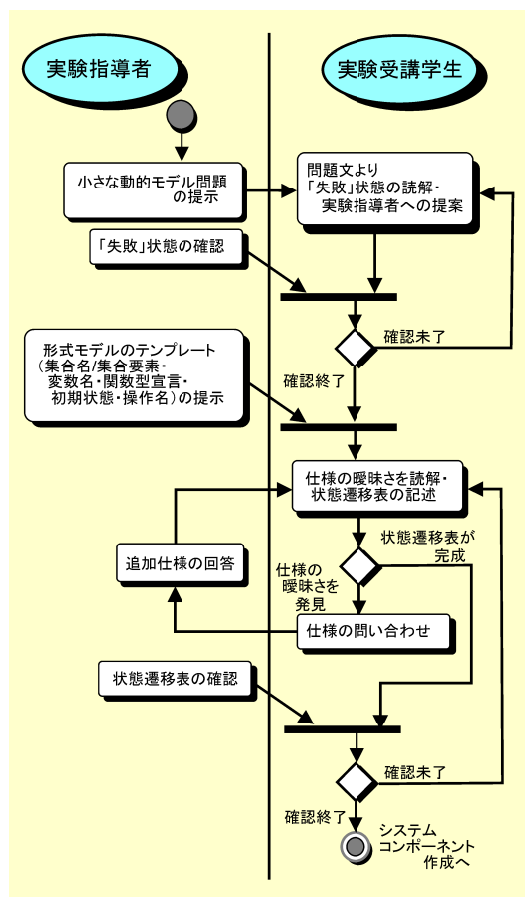


図 7 実験の手順 (実験 2 (状態遷移表作成まで))

Fig. 7 The procedure of experiment (Exp.2 (up to the step of making state transition tables)).

まとめたものを図 7 に示す。

実験において使用する題材として、題材の数を確保しやすいという理由により、筆者大西が作成した本科 3 年生の授業「論理回路」の試験問題をモデル記述に導入した。問題例を図 8 に示す。この問題は本来、小規模の順序論理回路を学生に設計させるものである。

図 8 においては、いわゆる「失敗」に値する状態『スケート靴を履かずに氷上にいる』が定義されている。

実験の指導者は図 8 の動的モデルを学生に提示して、学生には、図 8 における「失敗」の状態はどれであるかを読解させ、指導者に提案させて、指導者はその「失敗」の状態についての確認を行う。

「失敗」の状態の確認の後、実験の指導者が形式モデルのテンプレート (SETS 節 (集合名と集合要素)・VARIABLES 節 (変数名)・INVARIANT 節の一部 (関数型宣言)・INITIALISATION 節 (初期状態)・OPERATIONS 節の一部 (操作名)) を学生に提示する。

学生による形式モデル記述は、Atelier B のシステムモデリングプロジェクトとして実施する。実験の実施に際して、学生によるモデルの記述の発散を防止するために、集合名・変数名を指定し、状態変数の初期値、つまりシステ

問 2 ゆずる君はアイススケートが得意です。友達は、ゆずる君が氷の上で上手に 4 回転ジャンプを決める所を見たいです。
表 1 のように論理変数を割り当てたときに、JK フリップフロップを用いて順序論理回路を設計して、必要な論理式を全て答えよ。
《Mr. Yuzuru is good at skating. His friends want to see his quadruple jumps on the ice. Design a sequential logic circuit using JK flip-flops. Answer all of the essential boolean expressions with the assumption that the boolean variables are assigned as "表 1".》

表 1 順序論理回路の変数の割り当て

論理変数の名称	論理変数が持つ真値の意味
状態: Q_1Q_0	00: スケート靴を履いて氷上にいる。 《Standing on the ice with putting skate shoes on.》 01: スケート靴を履かずに氷上にいる。 《Standing on the ice without putting skate shoes on.》 10: スケート靴を履いてストーブの前にいる。 《Standing in front of the stove with putting skate shoes on.》 11: スケート靴を履かずにストーブの前にいる。 《Standing in front of the stove without putting skate shoes on.》
入力: X_1X_0	00: 氷の上に行く。《Go to the ice link.》 01: スケート靴を履く。《Put on his skate shoes.》 10: ストーブの前に戻って、スケート靴を脱ぐ。 《Go back to the front of the stove, and put off his skate shoes.》 11: 4 回転ジャンプが見事に成功する。 《His quadruple jump succeeded well.》
出力: Z_1Z_0	00: スケート靴を履いて氷の上にいるように期待される。 《Hoped to be on the ice with putting his skate shoes on.》 01: すぐに 4 回転ジャンプが成功することが期待される。 《Hoped his succeeding in quadruple jump coming soon.》 10: 友達が拍手する。《Friends clap their hands.》 11: (ドントケア) 《Don't care》

図 8 小さな動的モデル問題の学生への提示 (実験 2)

Fig. 8 Showing the question of a tiny dynamic modelling for students (Exp.2).

```

SETS
    type_location =
        {front_of_stove, on_ice};
    type_skate_shoes =
        {putting_off, putting_on};
    type_jumping =
        {not_succeed, succeed}

VARIABLES
    location, skate_shoes, jumping

INVARIANT
    location ∈ type_location ∧
    skate_shoes ∈ type_skate_shoes ∧
    jumping ∈ type_jumping

INITIALISATION
    skate_shoes := putting_off ||
    location := front_of_stove ||
    jumping := not_succeed
  
```

図 9 学生に事前に提示する記述 (SETS 節, VARIABLE 節, INVARIANT 節, INITIALISATION 節)

Fig. 9 Specification previously showing for students (SETS clause, VARIABLE clause, INVARIANT clause and INITIALISATION clause).

ムの初期状態も実験の指導者があらかじめ指定した。

実験の指導者が学生に提示する、SETS 節・VARIABLE 節・INVARIANT 節 (形式モデルへの安全要求としての不変条件を除く)・INITIALISATION 節を図 9 に示す。

図 9 の例では、形式モデルの状態空間を構成する 2 つの変数 location と skate_shoes, および, LTL 式への適用 (表 3 参照) のために便宜的に設けた変数 jumping を用意した。

図 8 の動的モデルによる論理回路における 4 通りの入力に対応させて、形式モデルの OPERATIONS 節における 4 つの操作を定義した。

```

OPERATIONS
go_to_ice_link =
BEGIN
END;

put_on_skate_shoes =
BEGIN
END;

go_to_front_of_stove_and_put_off_skate_shoes =
BEGIN
END;

try_quadruple_jump =
BEGIN
  jumping
  ∈(jumping ∈ type_jumping
    ((location$0 = on_ice
      skate_shoes$0 = putting_on) ⇒
      jumping = succeed
    )
  )
END

```

図 10 学生に事前に提示する記述 (OPERATIONS 節)

Fig. 10 Specification previously showing for students (OPERATIONS clause).

学生による記述の発散を防止するために、それぞれの操作名を実験の指導者があらかじめ指定した。

実験の指導者が学生に提示する、OPERATIONS 節の内容を図 10 に示す。

図 10 における操作の中身は基本的に空であるが、操作 try_quadruple_jump については、実質的に状態空間を構成する変数への新たな代入はなく、変数 jumping への代入が本質であるため、あらかじめ関係箇所をのみの記述を行っている。

図 10 の OPERATIONS 節にある 4 つの操作に対応させて、実験の指導者は、4 つの未完成の状態遷移表を学生に印刷物として配布し、学生に空欄を埋めさせることで、安全要求を満たす状態遷移モデルを設計させる。

操作 go_to_ice_link に対応させた完成版の状態遷移表を表 2 に示す。学生には表の網掛けのセルが空欄となっており、空欄を埋めさせて 4 つの状態遷移表を完成させる。

学生が表 2 などの状態遷移表の空欄を埋める際には、2.10 節で述べるリファインメントにおける便宜を図るために、状態遷移の前後で変数値に変化がない場合には、具体的な値ではなく、状態遷移前の変数値を意味する「(変数名) \$0」の記述を埋めさせる。

表 2 において学生が埋めるべき項目のうち、太字箇所は、学生にとっては事前に提示された情報のみでは正解が得られない「曖昧な仕様」にあたる箇所である。

システムへの安全要求を満たすために学生は、動的モデルの仕様の曖昧さを読解して、実験の指導者に問い合わせて明文化させなければならない。

学生による仕様の問合せに対し、表 2 の例では、『ゆずる君がスケート靴を脱いでいるならば、氷上に行けと言われても行かない』という追加仕様の回答となる挙動を、実験の指導者は事前に用意しなければならない。

学生において動的モデルの仕様の曖昧さが解消したなら

表 2 学生に空欄を埋めさせる状態遷移表の 1 つ

Table 2 One of state transition tables for students to fill the blanks.

go_to_ice_link

状態遷移前の変数値		状態遷移後の変数値	
location\$0	skate_shoes\$0	location	skate_shoes
front_of_stove	putting_off	location\$0	skate_shoes\$0
front_of_stove	putting_on	on_ice	skate_shoes\$0
on_ice	putting_off	(don't care)	(don't care)
on_ice	putting_on	location\$0	skate_shoes\$0

ば、状態遷移表が完成するはずなので、実験の指導者がその状態遷移表を確認する。

2.9 実験の手順 (実験 2: 小さな動的モデルの記述 (2)) (システムコンポーネントの記述)

学生が状態遷移表を完成させたならば、形式モデルの記述に着手するために、学生にシステムコンポーネントを記述させて、不変条件の提案・追加を行わせ、システムコンポーネントの定理証明を行わせる。

コンポーネントの記述に限定した学習目標を以下のように設定し、指導者より学生へ教授する (コンポーネントの定理証明については 2.11 節で述べる)。

(2-4) 状態遷移表を基に、(冗長性のある) becomes such that 非決定的代入記法による述語として、形式仕様を記述できる。

(2-5) 小さな動的モデルにおける「失敗」状態に陥らないための不変条件の提案ができる。

図 7 に引き続き、学生によるシステムコンポーネントの記述や定理証明について、実験の指導者と受講学生との間で行われる手順についてまとめたものを図 11 に示す。

学生にシステムモデリングプロジェクトを新規作成させ、このプロジェクトの下のシステムコンポーネントを新規作成させる。

学生には、2.8 節で確認した「失敗」に値する状態に陥らせないための安全要求として、不変条件『ゆずる君は氷上にいるならば、スケート靴を履いている。』および『ゆずる君はスケート靴を脱いでいるならば、ストーブの前にいる。』を提案させて、INVARIANT 節に図 12 にあるような述語を追加させる。

図 10 の OPERATIONS 節にある 4 つの操作について、本来ならば、2.10 節の図 15 にあるような if 文などによる単純な記述をすべきところを、あえて状態遷移表の記述を基にして、学生には図 13 の BEGIN~END 間にあるような becomes such that 非決定的代入^{*1}[31] の記法を使った、

^{*1} 与えられた述語を満足する値を変数に非決定的に割り当てることができる代入の手段である [26]。代入の対象とする変数を x とする場合、 x にかかる述語において、代入前を「 x0$ 」、代入後「 x 」と表記することとなっているため、 x を状態変数とするならば、「 x0$ 」が状態遷移前、「 x 」が状態遷移後に対応する。

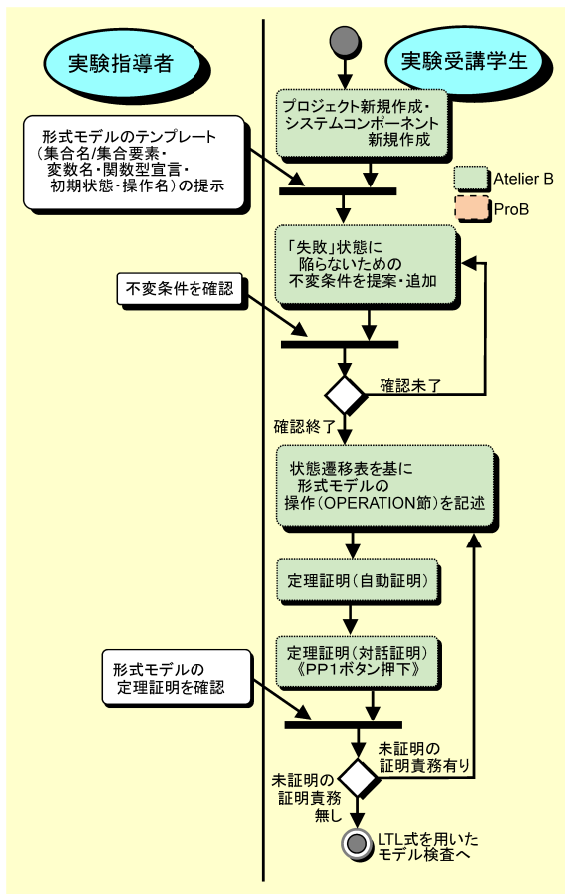


図 11 実験の手順 (実験 2 (システムコンポーネント))

Fig. 11 The procedure of experiment (Exp.2 (system component)).

```

INARIANT
(location = on_ice      => skate_shoes = putting_on)  ^
(skate_shoes = putting_off => location = front_of_stove)

```

図 12 学生に提案させる「不変条件」

Fig. 12 Invariants, should be brought up by students.

```

OPERATIONS
go_to_ice_link =
BEGIN
  location, skate_shoes
  ∈ (location ∈ type_location           ^
     skate_shoes ∈ type_skate_shoes     ^
     (location$0 = front_of_stove =>
       (skate_shoes$0 = putting_off =>
         location = location$0 ^
         skate_shoes = skate_shoes$0 ) ^
       (skate_shoes$0 = putting_on =>
         location = on_ice ^
         skate_shoes = skate_shoes$0 ) ) ^
     (location$0 = on_ice =>
       location = location$0 ^
       skate_shoes = skate_shoes$0 ) )
END

```

図 13 システムコンポーネントでの 1 つの「操作」の記述

Fig. 13 Specification of one of operations in a system component.

冗長ではあるが状態遷移表に則した記述を完成させる。

表 2 の状態遷移表の記述を基にして完成させた操作 go_to_ice_link を完成させた結果は、図 13 のようになる。

表 2 より図 13 を導出するなどを行うシステムコンポーネント J3test_iceskate.sys の記述の例では、実験 2 における初回の例題として扱うため、2.5 節 (2) で述べた指導書別冊を用いて、実験の指導者より学生に対して、次のコンポーネント記述の方針を提示している。

- システムの状態遷移 (変数値の変化) によってもつねに成立しなければならない論理式、いい換えるとシステムの安全にかかる論理式を、不変条件として INVARIANT 節に追加する。
- becomes such that 代入を用いて、漏れの無いすべての場合分けについての状態遷移を愚直に記述する。
- 状態遷移の前と状態遷移の後との間で、変数値が変化しないものについては、勝手に具体的な値を割り当てるのではなく、「事前の変数値を引き継ぐこと」を明示する (変数 var について例えると、「var\$0」が状態遷移前、「var」が状態遷移後。つまり、事前の変数値を引き継ぐことは「var = var\$0」と表現する)。

続いて行うシステムコンポーネントの定理証明の詳細については、2.11 節で述べる。

システムコンポーネントの定理証明を確認したならば、システムコンポーネントについて、2.12 節で述べる LTL 式によるモデル検証を行う。

2.10 実験の手順 (実験 2: 小さな動的モデルの記述 (3)) (リファインメントコンポーネントの記述)

2.9 節で述べたシステムコンポーネントの定理証明を確認して、2.12 節で述べる LTL 式によるモデル検証を行ったならば、学生に数段にわたるリファインメントコンポーネントを記述させて、リファインメントコンポーネントの定理証明を行わせる。

コンポーネントの記述に限定した学習目標を以下のように設定し、指導者より学生へ教授する (コンポーネントの定理証明については 2.11 節で述べる)。

(2-6) (冗長性のある) becomes such that 非決定的代入記法による述語を基にして、冗長性を排除した if 文記述に整理できる。

(2-7) becomes such that 非決定的代入記法による述語における冗長性を排除して実装直前の if 文記述までに整理すること限定して、形式仕様を詳細化できる。

学生によるリファインメントコンポーネントの記述や定理証明について、実験の指導者と受講学生との間で行われる手順についてまとめたものを図 14 に示す。

学生に上位コンポーネントのリファインメント (2.3 節参照) を行うためのリファインメントコンポーネントを新規作成させる。この際、OPERATIONS 節のすべての操作を上位コンポーネントより継承する。

図 13 のようにシステムコンポーネントに記述された操作に対して becomes such that 非決定的代入での記述にお

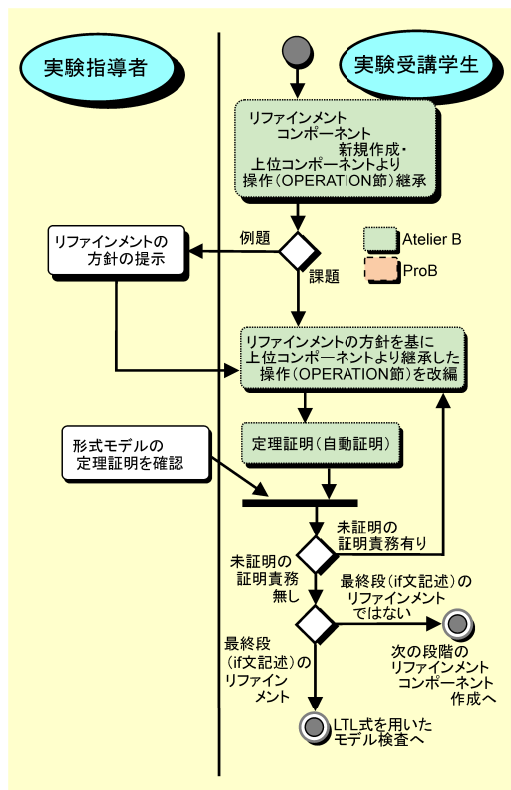


図 14 実験の手順 (実験 2 (リファインメントコンポーネント))

Fig. 14 The procedure of experiment (Exp.2 (refinement component)).

```

OPERATIONS
go_to_ice_link =
BEGIN
  IF
    skate_shoes = putting_on
  THEN
    location := on_ice
  END
END

```

図 15 リファインメントされた「操作」の記述

Fig. 15 Specification of a refined operation.

ける条件分岐の冗長な箇所についての統合を繰り返すという洗練化を行う。具体的には、上位コンポーネントより継承された OPERATIONS 節にある操作の記述の改編である。

定理証明によるコンポーネント間の無矛盾の検証を行いながら数段にわたるリファインメントを実施して、最終的に図 15 にあるような、実装に近い if 文記述まで導出させる。

実験 2 において、初回の例題となる形式モデル記述については、実験の指導者より学生に対して、2.5 節 (2) で述べた指導書別冊を用いてリファインメントの方針を提示して、それ以降の課題となる形式モデル記述については、リファインメントの方針を提示せずに、学生による任意の段数でのリファインメントについても許容することにする。

図 13 および図 15 の例では、実験 2 における初回の例

題として扱うため、実験の指導者より学生に対してリファインメントの方針を提示して、学生は 3 段階のリファインメントを経ている。

システムコンポーネント J3test.iceskate.sys より 1 段階目のリファインメントコンポーネント J3test.iceskate.r.ref を導出する方針として、次を学生に示している。

- 状態遷移の記述における冗長な箇所を徐々に排除する。
- あらゆる場合分けにおいて、ある変数の事前事後で変数値が引き継がれるならば、その変数値の引継ぎの行為を場合分けの枠の外に出す。
- あらゆる場合分けにおいて、ある変数に結果的に同じ変数値が割り当たるならば、その変数への値の割当ての行為を場合分けの枠の外に出す。

J3test.iceskate.r.ref より 2 段階目のリファインメントコンポーネント J3test.iceskate.2r.ref を導出する方針として、次を学生に示している。

- 引き続き、状態遷移の記述における冗長な箇所を徐々に排除する。
- あらゆる場合分けにおいて、ある変数の事前事後で変数値が引き継がれるならば、その変数値の引継ぎの行為を場合分けの枠の外に出す。
- あらゆる場合分けにおいて、ある変数に結果的に同じ変数値が割り当たるならば、その変数への値の割当ての行為を場合分けの枠の外に出す。
- 場合分けが必要な変数の割当てを最小限までに縮小する。

J3test.iceskate.2r.ref より 3 段階目のリファインメントコンポーネント J3test.iceskate.3r.ref を導出する方針として、次を学生に示している。

- becomes such that 代入文を、単純な代入文、あるいは if 文による代入文に変更する。
- すべて決定的代入とし、複数の代入については逐次代入にする。

続いて行うリファインメントコンポーネントの定理証明の詳細については、2.11 節で述べる。

リファインメントコンポーネントの定理証明を確認したならば、最終段 (実装に近い if 文記述) のリファインメントコンポーネントについては、2.12 節で述べる LTL 式によるモデル検証を行う。最終段を除いたリファインメントコンポーネントについては、次の段階のリファインメントを実施する。

2.11 実験の手順 (実験 2 : 小さな動的モデルの記述 (4)) (コンポーネントの定理証明)

システムコンポーネントおよびリファインメントコンポーネントの記述の後、2.5 節 (4) で述べた Atelier B 操作手順書を用いて、学生にコンポーネントの定理証明 (自動証明/対話証明) を行わせる。

コンポーネント	型チェック	証明責務生成	証明責務	証明済	未証明
J3test_iceskate	OK	OK	9	9	0
J3test_iceskate_2r	OK	OK	11	11	0
J3test_iceskate_3r	OK	OK	6	6	0
J3test_iceskate_r	OK	OK	15	15	0

図 16 小さな動的モデルに対する定理証明の結果

Fig. 16 Result of the theoretical proving for a tiny dynamic model.

コンポーネントの定理証明にかかる実験の学習目標を以下のように設定し、指導者より学生へ教授する（コンポーネントの記述については 2.9 節および 2.10 節で述べる）。

(2-8) (システムコンポーネント) 小さな動的モデルに対する形式モデルにおいて、「失敗」状態に陥らないための不変条件が満足することを証明できる。

(2-9) (リファインメントコンポーネント) becomes such that 非決定的代入記法による述語における冗長性を排除して実装直前の if 文記述までに整理することに限定して、詳細化の正当性を定理証明できる。

システムコンポーネント J3test.iceskate.sys および各段のリファインメントコンポーネント (J3test.iceskate_r.ref, ..._2r.ref, ..._3r.ref,) に対する定理証明の結果を図 16 に示す。すべてのコンポーネントについて, well definedness properties^{*2} [32] にかかる証明責務は皆無であった。

システムコンポーネント J3test.iceskate.sys において, 9 個の証明責務の中で 3 個の対話証明が必要となるが, すべての対話証明が PP1 (最初のレベルの仮説で述語証明) 1 回のみの手続き (当該ボタンの左クリック) で証明済みになるように, すべての例題・課題を設定しており, 仮に未証明の証明責務が残る場合は, コンポーネントの記述を見直す必要がある。

3 つのリファインメントコンポーネントについては, すべて自動証明のみで証明済みになるように, すべての例題・課題を設定しており, 仮に未証明の証明責務が残る場合は, コンポーネントの記述を見直す必要がある。

2.12 実験の手順 (実験 2: 小さな動的モデルの記述 (5)) (LTL 式を使ったモデル検査)

システムコンポーネント, あるいは最終段 (実装に近い if 文記述) のリファインメントコンポーネントの定理証明を確認したならば, それぞれのコンポーネントについて, LTL 式を使ったモデル検査を行うこととする。

学習目標を以下のように設定し, 指導者より学生へ教授する。

(2-10) 小さな動的モデルにおける, 実験指導者が提示した状態パス探索のゴール要件を基に, LTL 式を導出で

^{*2} 対象とする数式において, その数式に相応の有意義な意味がつけに割り当てられ, 数式が無意味になることがない保証がされていることである [27]。例をあげると, 全射ではない写像においては値域の要素に写像の対応漏れが存在しうするため, 逆写像を参照する際に, 対応付けされている値域の要素からのみに限定するという保証がされていることである。

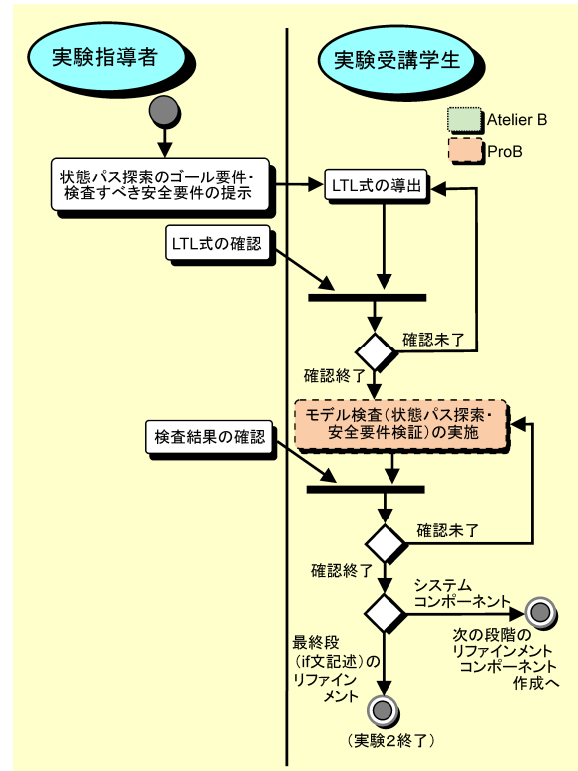


図 17 実験の手順 (実験 2 (LTL 式を使ったモデル検査))

Fig. 17 The procedure of experiment (Exp.2 (model checking using LTL formula)).

表 3 学生に導出させる LTL 式

Table 3 LTL formulae, should be derived by students.

ゆずる君が4回転ジャンプを決めるまでの経歴を探索するための LTL 式
$\neg \Diamond (\{ \text{jumping} = \text{succeed} \})$
「ゆずる君がスケート靴を履かずに氷上にいることはない」ことを証明するための LTL 式
$\Box (\neg (\{ \text{skate_shoes} = \text{putting_off} \wedge \text{location} = \text{on_ice} \}))$
「ゆずる君がスケート靴を履いていないならば氷上にはいない」ことを証明するための LTL 式
$\Box (\{ \text{skate_shoes} = \text{putting_off} \} \Rightarrow \neg \Diamond (\{ \text{location} = \text{on_ice} \}))$

きる。

(2-11) 小さな動的モデルにおける形式モデルにおいて, LTL 式を用いた状態パス探索ができる。

(2-12) 小さな動的モデルにおける, 実験指導者が提示した安全要件を検証する LTL 式を導出できる。

(2-13) 小さな動的モデルにおける形式モデルにおいて, LTL 式を用いた安全要件検証ができる。

学生による LTL 式を使ったモデル検査について, 実験の指導者と受講学生との間で行われる手順についてまとめたものを図 17 に示す。

実験の指導者は, 形式モデルにおいて状態パスを探索したいゴールの要件や検査したい安全要件について, 学生に日本語で提示して, 2.5 節 (5) で述べた ProB 操作手順書を用いて, 表 3 にあるように学生に LTL 式を導出させる。指導者はその LTL 式の確認を行う。

LTL 式の確認を行ったならば, ProB を用いて状態パス

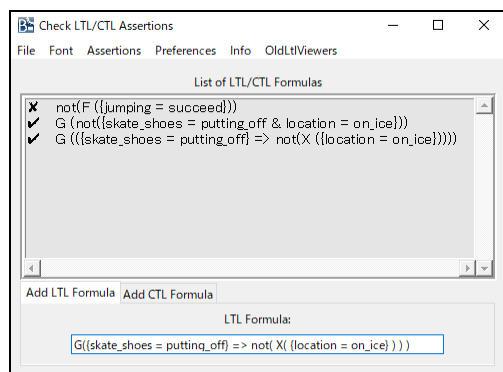


図 18 ProB での LTL 式を用いたモデル検査の結果

Fig. 18 Result of the model checking using LTL formulae by ProB.

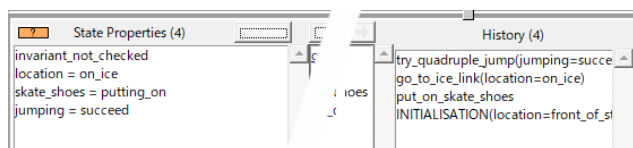


図 19 ProB での LTL 式を用いた状態パスの探索結果

Fig. 19 Result of state path tracking using LTL formula by ProB.

探索, あるいは安全要件検証といったモデル検査を行う。

ProB において LTL 式を用いたモデル検査を行った結果を図 18 に示す。状態パスを探索する表 3 や図 18 の第 1 式を用いた結果の画面の一部を図 19 に示す。

図 19 の History ビューにおいて, 形式モデルの初期状態よりゴールまでのパスが表示され, State Properties ビューにおいて現状態としてのゴールが表示されている。

2.13 実験報告書の提出について

実験 1 あるいは実験 2 それぞれについて, 実験の指導者は学生に実験報告書の提出を課する。

工学生が一般に報告書に記載すべき項目に加えて, 実験の指導者は, 学生よりの実験指導書の受理に際し, 以下の成果物の記載を課している。

(1) コンポーネントのソースリスト

Atelier B のエディタにおいて各コンポーネントのソースを A4 判に PDF 印刷したものを, 形式モデル記述の成果物として確認する。各コンポーネントの新規作成の際に, 自動作成されるヘッダにおいて学生の氏名をあらかじめ記述させておく。

各コンポーネントのソースは数キロバイトのテキストデータであるため, 学生による不正防止を目的として, 考察などでの引用の際に限り用いさせる。

(2) 定理証明の結果 (Atelier B)

図 6 や図 16 に相当する, Atelier B のメイン画面のクラシカルビューの画像コピーデータより, 各コンポーネントにおける相当数の証明責務の存在と未証明の証明責務

が 0 であることを確認する。

(3) (実験 1) 制約充足ソルバの実行結果 (ProB)

ProB のメイン画面の画像コピーデータより, 2.7 節において論理パズルの求解を実施する際に, 解候補数が 1 になり, パズルの正解が表示されることを確認する。続いて, 別解の存在を確認する際に, 解候補数が 0 になることを確認する。

(4) (実験 1) 写像の対応図

学生による作図により, 2.7 節において論理パズルの求解を実施する際に判明した, CONSTANTS 節において定義された定数における, 写像 (関数) としての定義域・値域の各要素の対応付けを表した対応図を確認する。

(5) (実験 2) 状態遷移表

学生による作表により, 2.8 節の表 2 に相当する状態遷移表の完成を確認する。

(6) (実験 2) アニメーションの実行結果 (ProB)

ProB のメイン画面の画像コピーデータより, History ビューにおける状態遷移パスと State Properties ビューにおける最終状態より, 学生が任意に実施したアニメーションの結果を確認する。

(7) (実験 2) LTL 式の検査結果 (ProB)

図 18 に相当する ProB のダイアログの画像コピーデータより, 2.12 節において LTL 式を用いたモデル検査を行った結果を確認する。

(8) (実験 2) 状態パス探索の実行結果 (ProB)

図 19 に相当する ProB のメイン画面の画像コピーデータより, 2.12 節において状態パス探索を行う際に, History ビューにおける状態パスと State Properties ビューにおけるゴール状態を確認する。

2.14 学生実験実践の有効性の評価

本稿における形式手法の教育実践に際し, その教育効果を議論すべく, 以下の RQ を定義する。

- (RQ1) 仕様書から形式仕様記述を適切に抽出することができていたか?
- (RQ2) 記述した形式仕様において, 定理証明を行うことができていたか?
- (RQ3) 記述した形式仕様において, モデル検査を行うことができていたか?
- (RQ4) 記述した形式仕様において, 仕様に論理的な矛盾や曖昧性がある場合には, それらを明らかにできていたか?

3. 実験の実施結果・学生アンケートの実施結果の考察および実験実践で得た知見・意見

3.1 学生実験の実施結果

本稿において実施した学生実験の実施結果について, 2.7 節より 2.12 節までにおいて述べた実験の手順ごとの学

表 4 実験 1 の学習目標の到達度

Table 4 Achievement degrees for the learning goals of Exp.1.

学 習 目 標
目標の達成度
■実験1: 静的モデルの記述
(1-1) 演繹論理パズルの問題文を自然言語仕様に見立て、パズル問題文にある制約条件を数学的記法に基づく述語として記述できる。 ※学生の実験報告書において、形式モデルの記述を確認しており、パズルの求解の成功の確認をしており、全員が達成している。
(1-2) 演繹論理パズルに対する形式モデルにて記述されたパズル問題における制約条件となる述語の無矛盾を証明できる。 ※学生の実験報告書において、未証明の証明責務が無いことを確認しており、全員が達成している。
(1-3) 演繹論理パズルを求解する、別解不存在を確認することを通じて、形式モデルの厳密性を証明できる。 ※学生の実験報告書において、パズルの求解、未証明の証明責務が無いことを確認しており、全員が達成している。

表 5 実験 2 (1) (問題の提示より状態遷移表の作成まで) の学習目標の到達度

Table 5 Achievement degrees for the learning goals (Exp.2 (1): from the step of showing the question to the step of making state transition tables).

学 習 目 標
目標の達成度
■実験2: 小さな動的モデルの記述(1) (問題の提示より状態遷移表の作成まで)
(2-1) 高々状態数4の小さな動的モデルの問題文より「失敗」状態の読解・実験指導者への提案ができる。 ※実験時における各実験班単位にて、「失敗」状態の読解・指導者への提案の実施を確認しており、全ての実験班が達成している。
(2-2) 小さな動的モデルの問題文より仕様の曖昧さを読解して実験指導者に問い合わせ、自然言語仕様の曖昧さを解消できる。 ※実験時における各実験班単位にて、仕様の曖昧さの読解・指導者への問い合わせの実施を確認しており、全ての実験班が達成している。
(2-3) 小さな動的モデルの問題文より仕様の曖昧さを排除した状態遷移表を記述できる。 ※学生の実験報告書において、状態遷移表の完成を確認しており、全員が達成している。

習目標の到達度を示すことで報告する。

まず、実験 1 の学習目標の到達度を表 4 に示す。

実験 1 においては、学生の実験報告書において、例題および課題における演繹論理パズルの求解および別解不存在の確認をしており、全員が目標を達成する成果の確認している。

実験 2 の問題の提示より状態遷移表の作成までの学習目標の到達度を表 5 に示す。

例題および課題は実験班ごとに同じものを使用するため、学生より実験の指導者への、動的モデルにおける「失敗」状態の提案や仕様の曖昧さの問合せは、各実験班単位での到達の見極めとなり、すべての実験班での達成を確認している。

状態遷移表については、学生の実験報告書において、全員が目標を達成する成果の確認している。

実験 2 のシステムコンポーネントの記述についての学習目標の到達度を表 6 に示す。

例題および課題は実験班ごとに同じものを使用するため、学生より実験の指導者への、動的モデルにおける不変条件の提案は、各実験班単位での到達の見極めとなり、すべての実験班での達成を確認している。

状態遷移表より becomes such that 非決定的代入記法による述語への記述については、学生の実験報告書において、

表 6 実験 2 (2) (システムコンポーネントの記述) の学習目標の到達度

Table 6 Achievement degrees for the learning goals (Exp.2 (2): specifying system components).

学 習 目 標
目標の達成度
■実験2: 小さな動的モデルの記述(2) (システムコンポーネントの記述)
(2-4) 状態遷移表を基に、(冗長性のある) becomes such that 非決定的代入記法による述語として、形式仕様を記述できる。 ※学生の実験報告書において、コンポーネントの記述を確認しており、また、学習目標(2-8)(2-11)(2-13)を達成しており、全員が達成している。
(2-5) 小さな動的モデルにおける「失敗」状態に陥らないための不変条件の提案ができる。 ※実験時における各実験班単位にて、不変条件の提案の実施を確認しており、全ての実験班が達成している。

表 7 実験 2 (3) (リファインメントコンポーネントの記述) の学習目標の到達度

Table 7 Achievement degrees for the learning goals (Exp.2 (3): specifying refinement components).

学 習 目 標
目標の達成度
■実験2: 小さな動的モデルの記述(3) (リファインメントコンポーネントの記述)
(2-6) (冗長性のある) becomes such that 非決定的代入記法による述語を基にして、冗長性を排除したif文記述に整理できる。 ※学生の実験報告書において、コンポーネントの記述を確認しており、また、学習目標(2-9)(2-11)(2-13)を達成しており、全員が達成している。
(2-7) becomes such that 非決定的代入記法による述語における冗長性を排除して実装直前のif文記述までに整理することに限定して、形式仕様を詳細化できる。 ※学生の実験報告書において、コンポーネントの記述を確認しており、また、学習目標(2-9)(2-11)(2-13)を達成しており、全員が達成している。

表 8 実験 2 (4) (コンポーネントの定理証明) の学習目標の到達度

Table 8 Achievement degrees for the learning goals (Exp.2 (4): theoretical proving of components).

学 習 目 標
目標の達成度
■実験2: 小さな動的モデルの記述(4) (コンポーネントの定理証明)
(2-8) (システムコンポーネント) 小さな動的モデルに対する形式モデルにおいて、「失敗」状態に陥らないための不変条件が満足することを証明できる。 ※学生の実験報告書において、システムコンポーネントにおける、不変条件を含めた記述、定理証明の遂行を確認しており、全員が達成している。
(2-9) (リファインメントコンポーネント) becomes such that 非決定的代入記法による述語における冗長性を排除して実装直前のif文記述までに整理することに限定して、詳細化の正当性を定理証明できる。 ※学生の実験報告書において、リファインメントコンポーネントの記述、定理証明の遂行を確認しており、全員が達成している。

全員が目標を達成する成果の確認している。

実験 2 のリファインメントコンポーネントの記述についての学習目標の到達度を表 7 に示す。

becomes such that 非決定的代入記法による述語における冗長性の排除に限定しているうえにおいて、リファインメントの遂行については、学生の実験報告書において、全員が目標を達成する成果の確認している。

実験 2 のコンポーネントの定理証明についての学習目標の到達度を表 8 に示す。

システムコンポーネント・リファインメントコンポーネント双方において、定理証明の遂行については、学生の実験報告書において、全員が目標を達成する成果の確認している。

実験 2 の LTL 式を使ったモデル検査についての学習目標の到達度を表 9 に示す。

表 9 実験2 (5) (LTL 式を使ったモデル検査) の学習目標の到達度

Table 9 Achievement degrees for the learning goals (Exp.2 (5): model checking using LTL formulae).

学習目標 目標の達成度
実験2: 小さな動的モデルの記述(5) (LTL式を使ったモデル検査)
(2-10) 小さな動的モデルにおける, 実験指導者が提示した状態パス探索の ゴール要件を基に, LTL 式を導出できる。 ※実験時における各実験班単位にて, LTL 式の導出を確認しており, 全ての実験班が達成している。
(2-11) 小さな動的モデルにおける形式モデルにおいて, LTL 式を用いた 状態パス探索ができる。 ※学生の実験報告書において, 状態パス探索の遂行を確認しており, 全員が達成している。
(2-12) 小さな動的モデルにおける, 実験指導者が提示した安全要件を 検証するLTL 式を導出できる。 ※実験時における各実験班単位にて, LTL 式の導出を確認しており, 全ての実験班が達成している。
(2-13) 小さな動的モデルにおける形式モデルにおいて, LTL 式を用いた 安全要件検証ができる。 ※学生の実験報告書において, 安全要件検証の遂行を確認しており, 全員が達成している。

例題および課題は実験班ごとに同じものを使用するため, LTL 式の導出は, 各実験班単位での到達の見極めとなり, すべての実験班での達成を確認している。

例題および課題における状態パス探索および安全要件検証の遂行は, 学生の実験報告書において, 全員が目標を達成する成果の確認している。

3.2 実験報告書での学生の感想

本稿で実践した実験の結果を報告する学生の実験報告書(実験1・実験2)における学生による感想のすべてを集約したものを web ページ^{*3}よりダウンロードできるようにした。

総じて, 形式手法に悪いイメージを持つ学生の感想はなく, 未経験の分野の体験に関心を持つ感想が多いと考える。

実験2におけるリファインメントに時間を要したという感想があった(3.4 節(4) 参照)。

3.3 学生アンケートの実施と考察

実験1 および実験2 の各実験終了時点で, 実験実施の達成度を自己評価させるべく, 学生に対するアンケートを実施している。

これまでに工業高専における形式手法の教授の実績などがなく, カリキュラム標準 J17-SE [14] の形式手法の学習目標・発展学習目標よりは当実験の目標である「ソフトウェア技術者の素養としての形式手法の体験」に見合う形式手法の教育指標をうまく見つけられず, 本稿における実験の実践を経るまでは暗中模索の状況であった。

そこで, 当実験においては, 表 11, 表 12 にある「(1-A) 形式仕様記述対象における, 明文化された構成要素を定義できる」などの, 実験1 においては 13 項目, 実験2 においては 15 項目の達成目標を独自に設けた。

「フォーマルメソッド利用のレベル」の各レベルと, 設

表 10 フォーマルメソッド利用のレベルと実験アンケートの達成目標との対応

Table 10 Mapping from the achievement aims, for the questionnaire for students, to the levels of formal method usage.

◆レベルの名称			
レベルの内容			
レベル内容の分類と達成目標		実験1	実験2
◆レベル0: 形式仕様記述			
数学的な記法を用いて厳密な仕様を記述し, 証明や分析までは行わずに, この記述を基にしてプログラムを開発する。			
数学的な記法を用いて厳密な仕様を記述する。		(1-A) (1-B) (1-C) (1-D) (1-E) (1-J) (1-K) (1-L)	(2-A) (2-B) (2-K)
数学的な記法を用いた厳密な仕様記述を基にしてプログラムを開発する。		—	(2-C) (2-N)
◆レベル1: 形式的開発および検証			
プログラムの性質を証明したり, 詳細化により仕様からプログラムを作成する。			
プログラムの性質を証明する。		(1-E) (1-F) (1-G) (1-H)	(2-D) (2-H) (2-I) (2-M)
詳細化により仕様からプログラムを作成する。		—	(2-C)
◆レベル2: 機械支援による証明			
定理証明器や証明支援器を用いてプログラムの性質を証明する。			
定理証明器を用いてプログラムの性質を証明する。		(1-E) (1-M)	(2-C) (2-D) (2-E) (2-O)
証明支援器を用いてプログラムの性質を証明する。		(1-F) (1-G) (1-H) (1-I) (1-M)	(2-H) (2-I) (2-J) (2-O)

定した学生アンケートにおける達成目標との対応について表 10 に示す。

この表における各レベル内容の細分については本稿で独自で行った。

アンケートの設問については, 当初設定の目標達成の見極めという目的としては曖昧な表現の設問や, 形式手法の初学者である学生が読解できるように実験の達成目標に対応する平易な文章表現とした代わりに 2.7 節より 2.12 節までにおいて示した実験の手順ごとの学習目標や上記の達成目標の趣旨より外れてしまう設問が含まれる。

実験を受講したクラス全員の学生 37 名分のアンケートの集計結果を表 11 および表 12 に示す。

すべての設問において 5 段階評価の 3 点超である。全体の 9 割弱の設問において 4 点超である。総じて一定の評価を得ていると考える。

後述の 2 つの設問を除き, 評価点の分布が 2 つに割れる現象を見受けられない。これらの項目においては達成度の低い学生群の出現を阻止できていると考える。

実験1 の設問「パズルの要素の関係性を写像(関数)で表現できたと思いますか?」, および設問「パズル問題の文章に書かれていない事実も明らかにできたと思いますか?」(つまり, 図 4 における「b 歳の人物と口は別人」の類の事実の発見の有無)に評価値 5 と 3 の 2 つの分布の山と計 7 名の評価値 2 を見受ける。両者とも平均点が 4.03, および 3.73 と低い評価値ではないが, 前者については実践の過程において一時は評価値 3 がピークになる分布であったが, 2.5 節(7)にある追加説明書などの対応によって評価値 5 にもピークができた結果と考える。後者については時間不足, 指導不足の可能性もある。例題における説明の

^{*3} <http://www007.upp.so-net.ne.jp/yukemuri/b-method.html>

表 11 学生アンケート（実験 1）の集計結果（N = 37）

Table 11 Result of the questionnaire survey for students (Exp.1, N = 37).

アンケート設問									
達成目標	思うー	⑤	④	③	②	①	→思わない	平均点	
■Atelier Bについて									
パズル問題の構成要素を論理式によるモデルで表現できたと思いますか？ (1-A)形式仕様記述対象における、明文化された構成要素を定義できる。	思うー	16	14	5	2	0	→思わない	平均: 4.19	
パズル内の要素の関係性を画像(関数)で表現できたと思いますか？ (1-B)形式仕様記述対象における、明文化された関係性を定義できる。	思うー	15	9	12	1	0	→思わない	平均: 4.03	
パズル問題のそれぞれの文章と、モデル内のそれぞれの論理式との対応付けを明確にできたと思いますか？ (1-C)形式仕様記述対象における、明文化された制約や性質を記述できる。	思うー	15	14	8	0	0	→思わない	平均: 4.19	
パズル問題の文章に書かれていない事実も明らかにできたと思いますか？ (1-D)形式仕様記述対象において直接的に明文化されていない事柄の存在を理解できる。	思うー	13	7	11	6	0	→思わない	平均: 3.73	
実験の例題・課題を行う過程で、Atelier Bの使用手順を理解したと思いますか？ (1-E)形式仕様の記述支援および論理証明ツールの基本的な使用手順を理解できる。	思うー	18	18	1	0	0	→思わない	平均: 4.46	
■ProBについて									
モデルを書き進めて、解の候補数が絞られることを確認できたと思いますか？ (1-F)仕様記述の追加することで、制約充足ソルバ機能において解空間が限定されていくことを理解できる。	思うー	34	2	1	0	0	→思わない	平均: 4.89	
モデルを書き上げると、パズルの正解が導けることを確認できたと思いますか？ (1-G)仕様における制約の記述が適切ならば、制約充足ソルバ機能によって求解できることを理解できる。	思うー	36	1	0	0	0	→思わない	平均: 4.97	
「パズルの正解の論理否定」を条件に加えて、パズルの別解が無いことも確認できたと思いますか？ (1-H)仕様における制約の記述が適切ならば、制約充足ソルバ機能によって求解できることを理解できる。	思うー	35	1	0	0	1	→思わない	平均: 4.86	
実験の例題・課題を行う過程で、ProBの使用手順を理解したと思いますか？ (1-I)検査ツールの制約充足ソルバ機能の基本的な使用手順を理解できる。	思うー	20	15	2	0	0	→思わない	平均: 4.49	
■B-Method全般について									
B-Methodを使った、論理式の表現法に慣れたと思いますか？ (1-J)自然言語による仕様を、論理式を用いて表現できる。	思うー	2	17	11	6	1	→思わない	平均: 3.35	
パズル問題に対する論理式を用いた厳密で明解な表現が、正解を自動的に導くことに役立つと理解したと思いますか？ (1-K)形式仕様記述の厳密性・明解性の意義を理解できる。	思うー	24	8	5	0	0	→思わない	平均: 4.51	
形式手法を利用することの価値を感じることができたと思いますか？ (1-L)形式仕様記述の意義を理解できる。	思うー	24	11	2	0	0	→思わない	平均: 4.59	
実験の例題・課題を行う過程で、形式手法B-Methodに親しみを持てたと思いますか？ (1-M)形式仕様記述、論理証明および制約充足ソルバ機能による求解の手順の意義について支持できる。	思うー	15	15	6	1	0	→思わない	平均: 4.19	

強調と追加説明書による説明の補充による指導の強化を通じて実践の向上を試みたいと考える。

実験 1 の設問群において、Atelier B 関連より ProB 関連の評価が総じて高い。学生の視座よりは、Atelier B での定理証明によるモデルの無矛盾の確認よりも ProB の制約充足ソルバの機能によるパズルの求解がより明解であり、強い興味を惹いた結果であろうと考える。ProB 関連の 1 つの設問における特異的な 1 名の評価 1 については後述する。

実験 1 および実験 2 における 3 つの設問「実験の例題・課題を行う過程で、Atelier B の使用手順を理解したと思いますか?」、「実験の例題・課題を行う過程で、ProB の使用手順を理解したと思いますか?」、「実験の例題・課題を行う過程で、形式手法 B-Method に親しみを持てたと思いますか?」について、実験 1 における最後の設問での 1 名を除く全学生について 3 以上の評価であり、平均点が 4 点超であり、実験 1 より実験 2 と実験回数を経るごとに、3 つの平均点が向上している。当実験の実践を通じて、ツール

表 12 学生アンケート（実験 2）の集計結果（N = 37）

Table 12 Result of the questionnaire survey for students (Exp.2, N = 37).

アンケート設問									
達成目標	思うー	⑤	④	③	②	①	→思わない	平均点	
■Atelier Bについて									
問題より、漏れの無い場合分けを論理式で表現できたと思いますか？ (2-A)形式仕様記述対象に対して、明文的に条件分岐を網羅する取り組みができる。	思うー	13	21	2	1	0	→思わない	平均: 4.24	
問題における安全に関する要件を、不変条件という論理式で書けたと思いますか？ (2-B)明文化された機能安全要求を、論理式を用いて表現できる。	思うー	14	16	6	1	0	→思わない	平均: 4.16	
論理式の表現からリファインして、論理証明を進めながら、IF文表現による欠陥の無い記述までに導けたと思いますか？ (2-C)垂直リファインメントによって、実装コードに近づく欠陥の無い記述まで詳細化する過程を理解できる。	思うー	19	11	7	0	0	→思わない	平均: 4.32	
不変条件が常に成立することを論理証明して、安全を確かめたと思いますか？ (2-D)機能安全要求が満たされていることを、定理証明ツールを活用して確認できる。	思うー	17	12	7	1	0	→思わない	平均: 4.22	
実験の例題・課題を行う過程で、Atelier Bの使用手順を理解したと思いますか？ (2-E)形式仕様の記述支援および論理証明ツールの基本的な使用手順を理解できる。	思うー	21	15	1	0	0	→思わない	平均: 4.54	
■ProBについて									
モデルをアニメーション機能で動かせることを確認できたと思いますか？ (2-F)モデルのアニメーション実行の方法を理解できる。	思うー	27	9	1	0	0	→思わない	平均: 4.70	
アニメーション機能を実行してみて、システムが安全であることを見ることができたと思いますか？ (2-G)モデルのアニメーションを活用して、辿れる一部のパスで安全要求を満たしていることを視認できる。	思うー	17	16	3	1	0	→思わない	平均: 4.32	
LTL式を用いて、確認したい状態への経歴を探索できたと思いますか？ (2-H)LTL式を定義でき、モデル検査においてLTL式を与えて特定の状態パスを探索できる。	思うー	16	16	4	1	0	→思わない	平均: 4.27	
LTL式を用いて、システムの安全を検証できたと思いますか？ (2-I)モデルがあらゆるパスで安全要求を満たしていることを、LTL式を用いて検証できる。	思うー	17	14	5	1	0	→思わない	平均: 4.27	
実験の例題・課題を行う過程で、ProBの使用手順を理解したと思いますか？ (2-J)形式検証ツールの基本的な使用手順を理解できる。	思うー	20	16	1	0	0	→思わない	平均: 4.51	
■B-Method全般について									
B-Methodを使った、論理式の表現法に慣れたと思いますか？ (2-K)自然言語による仕様を、論理式を用いて表現できる。	思うー	12	18	5	1	1	→思わない	平均: 4.05	
不変条件の証明や、LTL式を用いた検証によって、デビアンタビリティ向上を目指すことを理解したと思いますか？ (2-L)形式手法がシステムのデビアンタビリティ向上に寄与するという意義を理解できる。	思うー	12	13	10	2	0	→思わない	平均: 3.95	
LTL式を用いることにより、システムの全状態を網羅した上で、無欠陥を検証できることを理解したと思いますか？ (2-M)システムの全状態を網羅する形式検証の意義を理解できる。	思うー	17	14	6	0	0	→思わない	平均: 4.30	
とにかく動くコードを作るのとは異なる、無欠陥のコードを生成するために、形式手法は役立つことを理解したと思いますか？ (2-N)形式仕様が無欠陥のコード生成に寄与するアプローチであることを理解できる。	思うー	23	10	4	0	0	→思わない	平均: 4.51	
実験の例題・課題を行う過程で、形式手法B-Methodに親しみを持てたと思いますか？ (2-O)形式仕様記述、論理証明および形式検証の手順の意義について指示できる。	思うー	21	9	7	0	0	→思わない	平均: 4.38	

の使用手順の理解度や B への親近感について一定の評価を得ており、形式手法の敷居を下げる一定の効果を認める。

実験 1 および実験 2 における設問「B-Method を使った、論理式の表現法に慣れたと思いますか?」について、形式仕様記述に関する高度な達成目標に対応する設問項目と考えるが、実験 1 における平均点は 3.35、実験 2 においては 4.05 と実験回数を経るごとに向上している。当設問において低評価を出した学生の中には実験 1・実験 2 を通して評価値 2 の学生 1 名、評価値 1 の学生 1 名が含まれており、この 2 名の学生を除いた全員は実験 2 において評価値 3 以上となっている。実験 1・実験 2 を通じて評価値 2 の学生は、前述もしているが、実験 1 の ProB 関連の設問「パズルの正解の論理否定」を条件に加えて、パズルの別解がな

いことも確認できたと思いますか？」において、他の学生全員が4以上の評価値の中で特異的に評価1を答えている者であり、実験1・実験2を通じて評価値1の学生は、実験1・実験2を通じた残りの設問項目においてすべて評価値5を答えるという極端な回答をする者である。上記2名による低評価の回答については、回答の指向の特異性に起因する影響が大きいと考える。

3.4 実験実践で得た知見

実験を受講した学生37名の実験の実践を通じて、実験の状況および実践より得た知見は以下のとおりある。

(1) 実験全体について

使用した学生用PCにおけるAtelier B, ProBの使用について、動作速度なども含め、トラブルは生じていない。10名程度の各実験班において1名ずつほど、Atelier BおよびProBを自身のPCに導入したい、あるいは独自に無償版を導入したという学生が出現した。

(2) 実験1—写像・関数の扱いについて

比較的能力の低い学生に対しては（未完成の）写像・関数の対応図を与えておくことは必要と考える（2.5節(2)参照）。写像・関数の定義域・値域の対応付けが曖昧に理解されている場合が多く、実験が進むにつれ、課題の題意より関数・逆関数の参照の記述を導出の方法についての学生間での議論が始まるが、その際に写像の対応図が議論の道具として多く用いられる。

当初、例題のモデルにある記述のみでは、関数・逆関数を複合で参照を行う際にマップレット（ $1 \rightarrow$ ）を使用できないというBの文法を学生が理解できなかったため、追加で説明資料を作成した（2.5節(7)参照）。

(3) 実験2—状態遷移系の扱いについて

例題のモデルにある操作の形式記述における *becomes such that* 非決定的代入より状態遷移表を学生に書き起こさせ、続いて学生に課題を取り組ませる際に、状態遷移表を書かせてから形式モデルの記述を行わせることは必要と考える（2.8節, 2.9節参照）。当実験の受講学生の能力では、状態遷移表を介さずに適切な条件分岐をした *becomes such that* 非決定的代入による記述をすることは不可能に近いと考える。

学生より状態遷移表を書かせる時点において、課題の題意より、モデルの安全を保証するために求められる状態遷移系に課する新たな制約の必要性について、学生が実験指導者に問い合わせることができている。

比較的能力のある学生は、リファインメントの段数が1段でも定理証明、モデル検査を通過させられている（3.5節のLecomte氏のコメントを裏付けている）。

(4) 実験2—リファインメントの扱いについて(1)

能力に自信のない学生、特に *becomes such that* 非決定的代入において文法の理解より条件分岐の理解までの広

い意味にわたるネスティングの理解が不十分なレベルにある学生は、例題での指針（2.10節参照）に従って3段のリファインメントを実施しており、最大5段のリファインメントを実施する者が出現した。

2.10節において実験の手順を述べ、3.1節の表7において学習目標の達成の確認を報告し、3.2節における学生の感想に表れているが、一部の学生に、*becomes such that* 非決定的代入における冗長性の排除に苦心した者がいた。今後の説明資料の追加などの手段でハードルを下げ、実験の時間を短縮する対応を検討しているが、定理証明ツールが、各学生の理解速度に足並みを揃えて、状態遷移系を意識した条件分岐フローを記述する能力の獲得を支援する事象と判断しており、実験の設計者あるいは指導者としては、学生による学習目標の達成を歓迎すべきものと考ええる。

(5) 実験2—リファインメントの扱いについて(2)

一部の学生においては、Atelier Bの証明器によって未証明の証明責務がなくなる事象を、プログラミング言語のコンパイルにおける「バグがないこと」と同じ感覚で、「記述に論理的な誤りがないこと」と誤解しており、文法的な問題はなく未証明の証明責務はないが論理的な誤りのある記述を放置していた。結果、そのリファインメント後については正しい論理で記述した際に、リファインメントの前後の記述における矛盾が生じて証明できない証明責務が発生した時点において、リファインメント元の対応箇所における記述に論理的な誤りを見出すという事例があった。

(6) 実験2—リファインメントの扱いについて(3)

システムコンポーネントにおいて、図12のようなモデルへの安全要求のための新たな不変条件を付加することを学生が失念しており、結果、システムコンポーネントにおける証明責務の数が0のままでリファインメントを進めているのを見受けた際に、不変条件の不備を指摘する事例があった。

3.5 ツール提供元よりの意見、およびBの教材について

当実験についての産業界よりの意見を得るため、Atelier B提供元の仏国ClearSy社のLecomte氏（謝辞参照）に、当実験の実践に関する報告をし、次のコメントを頂戴した。

- The first example is mainly a modelling example with constants (so nothing to demonstrate). It is good to jump start formal modelling. Michael Leuschel used to model sudoku game or the queens problem [29].
- For the second one, maybe you could reduce the number of refinement levels and insist on (easy - with boolean predicates only - to ensure full automation) functional proof with Atelier B and non-functional proof (LTL) with ProB.

また、Lecomte 氏より Atelier B Ver.4.5.1 を活用した B の動画教材サイトであるブラジル・リオグランデノルテ連邦大学の MOOC [33] の紹介を受けており、当サイトは文献 [19] に則した内容で、ソフトウェア開発において要求されるモデル記述におけるループ構造や抽象的データの扱いなども載っており、学生の今後の B の自学習にも活用できるものと考ええる。

3.6 RQ への考察

2.14 節で定義したそれぞれの RQ について考察する。

(1) RQ1 への考察

『(RQ1) 仕様書から形式仕様記述を適切に抽出することができていたか?』について考察する。

実験 1 について、2.7 節で定義した学習目標 (1-1) を、3.1 節の表 4 に示すように、実験報告書において学生全員の達成を確認している。

実験 2 について、2.8 節および 2.9 節で定義した学習目標と、3.1 節の表 5 および表 6 に示す達成度評価によって、学習目標 (2-3), (2-4), つまり状態遷移表と becomes such that 非決定的代入記法による述語の記述について、実験報告書において学生全員の達成を確認しており、学習目標 (2-1), (2-2), (2-5) を、つまり「失敗」状態の読解、仕様の曖昧さの解消、および不変条件の提案について、実験時における各実験班単位で確認している。

実験アンケートに関して、3.3 節の表 10 の分類されたレベル内容「数学的な記法を用いて厳密な仕様を記述する」に対応する達成目標に対応する設問への評価は、2 つの設問を除き 4 点以上であり、一定の評価があったと考える。実験 1 における設問「パズル問題の文章に書かれていない事実も明らかにできたと思いますか?」(3.73 点) については、表 11 直前の記述にあるように苦慮している。実験 1 における設問「B-Method を使った、論理式の表現法に慣れたと思いますか?」(3.35 点) は、表 12 直後の記述にあるように、実験 2 における同設問にて評価が向上している。

したがって、筆者らは、実験 1 については、一部の課題が残るが、学生全員が実践できたものと考え、実験 2 については、一部、各実験班単位という限定の下において実践できたものと考え。

(2) RQ2 への考察

『(RQ2) 記述した形式仕様において、定理証明を行うことができていたか?』について考察する。

実験 1 について、2.7 節で定義した学習目標 (1-2) を、3.1 節の表 4 に示すように、実験報告書において学生全員が達成を確認している。

実験 2 について、2.11 節で定義した学習目標 (2-8), (2-9) を、3.1 節の表 8 に示すように、実験報告書において学生全員が達成を確認している。

実験アンケートに関して、3.3 節の表 10 の分類されたレベル内容「プログラムの性質を証明する」および「定理証明器を用いてプログラムの性質を証明する」に対応する達成目標に対応する設問への評価は、すべての設問で 4 点以上であり、一定の評価があったと考える。

したがって、筆者らは、学生全員が実践できたものと考え。

(3) RQ3 への考察

『(RQ3) 記述した形式仕様において、モデル検査を行うことができていたか?』について考察する。

実験 1 について、2.7 節で定義した学習目標 (1-3) を、3.1 節の表 4 に示すように、実験報告書において学生全員が達成している。

実験 2 について、2.12 節で定義した学習目標 (2-11), (2-13), つまり状態パス探索、安全要件検証の手順について、3.1 節の表 9 に示すように、実験報告書において学生全員の達成を確認しており、学習目標 (2-10), (2-12), つまり LTL 式の導出について、実験時における各実験班単位にて確認している。

実験アンケートに関して、3.3 節の表 10 の分類されたレベル内容「プログラムの性質を証明する」および「証明支援器を用いてプログラムの性質を証明する」に対応する達成目標に対応する設問への評価は、すべての設問で 4 点以上であり、一定の評価があったと考える。

したがって、筆者らは、実験 1 については、学生全員が実践できたものと考え、実験 2 については、一部、各実験班単位という限定の下において実践できたものと考え。

(4) RQ4 への考察

『(RQ4) 記述した形式仕様において、仕様に論理的な矛盾や曖昧性がある場合には、それらを明らかにできていたか?』について考察する。

実験 1 について、3.3 節中盤で述べた追加説明書によるサポートもあり、2.7 節で定義した学習目標 (1-1) を、3.1 節の表 4 に示すように、実験報告書において学生全員が達成している。

実験 2 について、定理証明については、2.8 節における手続きにおいて、形式記述する以前に状態遷移表を作成するまでに仕様の曖昧性を排除する。

同節で定義した学習目標 (2-3), 状態遷移表の完成について、実験報告書において学生全員の達成を確認しており、学習目標 (2-2), 曖昧さの読解について、実験時における各実験班単位にて確認している。

また、3.4 節 (4) および (5) の事例が形式仕様された記述における矛盾の発見例である。

モデル検査については、実験時間の制約により、Atelier B における定理証明を経た、仕様の厳密さや安全要件が保証された形式モデルを ProB に引き継いで追認に限定

しているため、形式仕様に矛盾や曖昧性を含んだ検証を行っていない。

実験アンケートに関して、3.3 節の表 11 にある達成目標「(1-D) 形式仕様記述対象において直接的に明文化されていない事柄の存在を理解できる」に対応する実験 1 における設問「パズル問題の文章に書かれていない事実も明らかにできたと思いますか？」(3.73 点) については、表 11 直前の記述にあるように苦慮している。実験 2 については、該当する達成目標が存在しない。

したがって、筆者らは、実験 1 については、一部の課題が残るが、学生全員が実践できたものと考え、実験 2 については、定理証明については、一部、各実験班単位という限定の下において実践できたものと考え、

モデル検査については、実施していない。

(5) 教育効果としての実践の有効性について

上述の RQ への考察をふまえ、教育効果としての本稿での実験実践の有効性について考察する。

2.4 節後半に示すように、工業高専での実験実践における制約が存在し、受講者全員の目標達成を要件とする水準を見据えて実験計画を行っており、2.13 節に示すように、学生よりの実験指導書に記載すべき項目のすべてについて、実験の指導者は、報告書の受理に際して項目の記載を確認しており、報告書の受理をもってクラス全員の実験の終了としている。

また、2.13 節 (1) などの学生による不正の防止を目的とした取り組みを行い、学生による成果物や報告書の質の維持に努めている。

一方、2.8 節の動的モデルよりの「失敗」状態の読解および仕様の曖昧さの解消・2.9 節の不変条件の提案・2.12 節の LTL 式の導出については、実験班内での学生同士の討論の機会を是として、各実験班単位で達成を確認しており、学生全員の能力獲得を保証するまでには至っていない。

また、記述した形式仕様における矛盾や曖昧性を明らかにすることについては、モデル検査の観点よりは実践できていない。

3.7 実験実践の効果向上のためになすべきこと

当実験の実践に際して、今後の効果向上のための目下の事項として以下のことを行うべきと考える。同時に、4 章で述べる先進事例などを参考に、形式手法のより客観的な教育効果の指標の整理を進めるべきと考える。

- 「フォーマルメソッド利用のレベル」のレベル 1 におけるプログラム自動生成までの手順を完結させる。
本件については、2.3 節の図 1 の実装コンポーネントへのリファインメント、C 言語への自動生成の事項を実験項目に加える目途を立てており、令和 2 年度より実施する見込みである。

- 実験 2 において、図 8 の類の問題に代わる、より実製品の開発に近い題材探しを行う。
- リファインメント前後におけるリンク不変条件や、操作における事前条件/事後条件の考え方を追加する。
- モデル検査ツールを活用した、形式仕様に矛盾や曖昧性を含んだ検証を行う。

4. 関連分野の先例となる実践との比較について

4.1 仕様記述言語ツールを活用した実践例

1 章前半において言及したが、形式手法を活用しつつ数学的論理思考をソフトウェア科学関連の大学学部レベルやそれ以下のレベルの教育に導入する実践例は多数存在する。

文献 [5] においては、米国の複数の大学が連携して、教育目的に独自に開発したプログラミング言語上の仕様記述言語を融合する開発環境 RESOLVE を活用した教育プログラムを紹介し、20 年程度にわたり実践していると報告している。

文献 [34] においては、形式手法の様々な教育を 30 年近く取り組んでいる米国の大学が、既存ツールにおける教育適用への複雑さを排除する目的でプログラミング言語上の仕様記述言語である Spext を独自に開発し、学部生に対する授業において、既存の JML との 2 種類のツールそれぞれについての自動テスト生成による教育実践を報告している。

本稿での実践と比較して、両者とも長年の経緯に基づいて独自のツールを開発して教育実践していると評価できる。一方、形式仕様記述ツールの適用に限定しているところは、形式仕様記述・定理証明とモデル検査の双方を含有している本稿の実践が優れていると考える。

教育の対象を工学生より枠を広げた国内での導入教育の実践例である文献 [13] においては、VDM を活用している。要求工学・システム開発の立場より、基礎からの導入が試みられており、要所で適宜、数学的記法の導入が図られている。取り上げられる演習例も実用的な実製品やシステムである。教育水準の指標について、本稿で採用した「フォーマルメソッド利用のレベル」[21] とは異なる、Larsen による 4 段階の形式手法適用のレベル [35] を導入し、Larsen によるレベルの上位より 2 番目の「レベル 3: 厳密な仕様を検証する」のうちの「レベル 3 (1): テストによる検証」への適用を想定すると明確化している。また、あらゆる形式手法ツールを紹介し、形式仕様記述ツールについては詳述している。

本稿での実践と比較して、要求工学や数学的記法よりシステム開発現場の実用面までを綿密にかつ広範囲に網羅する教育内容であり、受講者アンケートを実施して、適宜、教材の改訂を実施しているところが評価できる。一方、当事例の主な対象者を学生ではなく、20 代後半より 30 代前

半のリーダクラスの技術者に据えられているところは、大学学部生相当の年齢の学生にも対応できる本稿の実践が優れていると考える。形式仕様記述ツールの適用のみであるところは、形式仕様記述・定理証明とモデル検査の双方を含有している本稿の実践が優れていると考える。形式仕様の妥当性確認 (validation)・正当性検証 (verification) とテストを扱っているが、定理証明の手前の手順までに限定しているところは、定理証明までを含有している本稿の実践が優れていると考える。

4.2 モデル検査に基づく実践例

文献 [36] においては、インドにおける大学の学部生・院生レベルとされるモデル検査の立場としての形式手法の教育の実践および普及推進の方向性について報告している。

形式手法の教育に際しての克服すべき 3 つの課題 (学びたいという動機付け、実世界との関連性、関連する数学の必要性) を指摘し、普及推進のための 3 つの当事者の観点 (学部生が学ぶ観点、教員が教授する観点、産業界が企業内研修で教える観点) を述べている。

学部生においては、形式手法そのものの知識はないが、現状の教育課程で形式手法の基礎となるものを学んでいるため、実世界に則した問題の解決などを通じて学習への動機付けを行うべきと述べている。教師においては、大学での最新のモデル検査ツール (NuSMV, SPIN) に関する実用的な事例やパズルを扱った教員研修の成果を述べている。産業界においては、ワークショップを通じてモデル検査ツールの有効性を訴えて関連数学の必要性にかかる神秘性からの脱却を説いて、形式手法の有効性を述べている。

最後には、形式手法の教育に対する要求を満足する唯一の方法は産学連携であると提唱し、実践の様子を報告している。

本稿での実践と比較して、形式手法の教育実践や普及推進への理念的な高い視座に立っていると評価できる。本稿においては産学連携が筆者らによる教育実践への動機付けになっているが、当事例では産学連携を教育実践への具体的な解決策までに結び付けている。一方、当事例はモデル検査ツールの適用に限定しているところは、形式仕様記述・定理証明とモデル検査の双方を含有している本稿の実践が優れていると考える。また、受講者には相応の予備知識が事実上備わっていることが当文献における主張の前提となっているところは、形式手法の導入を容易にするという観点では、求められる数理論理学の指導を含めて時間内に収める目途を立てている本稿の実践が優れていると考える。

文献 [37] においては、独国の大学の学部生に対する要求工学の概論を教授する教育課程において、数学的論理思考に根差した「形式的記法」として決定表やシーケンス図などの UML の手法に基づいた教育プログラムを紹介し、

SAT ソルバのようなツールの導入の可能性について言及しており、3 年以上にわたり実践していると報告している。

本稿での実践と比較して、学生アンケートなどではなく、試験による客観的指標による教育効果のデータを蓄積していると評価できる。一方、当事例はモデル検査の考え方の導入に限定しており、ツールを使った実践をしておらず、形式仕様記述・定理証明とモデル検査の双方のツールの活用を含有している本稿の実践が優れていると考える。

教育の対象を工学生より枠を広げた国内での導入教育の実践例である文献 [10] においては、対象者に情報科学・情報工学を専攻する学生も含まれている。演習環境として独自に開発した KINOPPIX の下、モデル検査ツール (NuSMV, SPIN) を活用している。4 日間の短い教程において、本稿で採用したものよりも状態空間が広い動的パズル問題を採用しており、LTL 式の活用について詳述されており、状態遷移系としての欠陥のあるモデルの事例も取り上げられている。続編として CTL (computation tree logic, 計算木論理) も活用した、より実践的な教育課程につないでいる [38]。

本稿での実践と比較して、学生を対象に含めているのと同時に産業界が求める実用面が意識された内容であると評価でき、本稿における実験設計の時点において、LTL 式の活用などについて参照した経緯がある。一方、当事例はモデル検査のツールの適用に限定しているところは、形式仕様記述・定理証明とモデル検査の双方を含有している本稿の実践が優れていると考える。

5. まとめ

本稿では、形式手法における人材の養成確保の問題への解決策の 1 つとして「ソフトウェア技術者の素養としての形式手法を体験させる」ことを目標に、工業高専本科生に対して形式手法 B-Method の学生実験を実践した。

工業高専本科生向けの実践例が皆無のため、構想段階より実践にかけて暗中模索の状態が続いたが、実践の結果、当実験は受講学生よりツールの使用手順の理解度や B への親近感について一定の評価を得ており、学生よりツールを導入したいという希望が出ているなどの一定の関心を得ており、学生の形式手法に対する敷居を下げることに成功しており、当初の目標を達成するものであり、人材の養成確保の問題解決に向けて寄与するものと考え、今後の課題として、実験の題材・手順の改善を通じてのブラッシュアップを行い、学生にとっての形式手法の敷居を下げる効果の向上策を検討する。

謝辞

- 経済産業省北海道経済産業局の戦略的基盤技術高度化支援事業を通じて、筆者らは形式手法 B-Method の知見を得る機会を得たことをここに報告して謝意を表し、当事業において共同研究を行った株式会社ヴィッ

ツ, 株式会社アトリエ, アーク・システム・ソリューションズ株式会社の関係各位に謝意を表する。

- 当実験で使用しているツール Atelier B の提供元の窓口として日頃アドバイスを頂戴している, 仏国 ClearSy 社 R&D プロジェクトディレクタ兼 B モデル・シニアエキスパートの Thierry Lecomte 氏に謝意を表する。

参考文献

- [1] 青木利晃: 車載システム開発における形式手法実践の現状と課題, システム制御情報学会「システム/制御/情報」, Vol.62, No.4, pp.134–140 (2018).
- [2] ウィンターワークショップ 2018・イン・宮島論文募集: T4-形式手法—導入支援と技術教育 (2018), 入手先 (<http://www.sigse.jp/2018/cfp.html>) (参照 2019-07-20).
- [3] 室 修治: 変革を求められる IT 人材—高信頼設計・検証を担う人材育成, *SEC Journal*, Vol.8, No.1, pp.26–29 (2012).
- [4] 栗田太郎: 形式手法の実践に対してよく尋ねられる質問とその回答—モバイル FeliCa の開発における形式仕様記述を通して, *SEC Journal*, Vol.7, No.1, pp.34–39 (2011).
- [5] Heym, W. et al.: Integrating Components, Contracts and Reasoning in CS Curricula with RESOLVE: Experiences at Multiple Institutions, *2017 IEEE 30th Conference on Software Engineering Education and Training (CSEET)*, pp.202–211 (2017).
- [6] Integrating Mathematical Reasoning into Computer Science Curricula, available from (<http://www.math-in-cs.org/>) (accessed 2019-07-20).
- [7] 本位田真一, 糸野文洋, 田原康之, 鷲崎弘宜: トップエスイー: サイエンスによる知的ものづくり教育, 情報処理, Vol.48, No.11, pp.1264–1272 (2007).
- [8] Ishikawa, F., Yoshioka, N. and Tanabe, Y.: Keys and Roles of Formal Methods Education for Industry: 10 Year Experience with Top SE Program, *The 1st workshop on Formal Methods in Software Engineering Education & Training (FMSEET2015)*, pp.35–42 (2015).
- [9] 木下佳樹: 産総研システム検証研究センター紹介, 日本ソフトウェア科学会「コンピュータソフトウェア」, Vol.21, No.4, pp.307–310 (2004).
- [10] 産業技術総合研究所システム検証研究センター: 4 日で学ぶモデル検査 (初級編) (CVS 教程 (1)), NTS (2006).
- [11] 北陸先端科学技術大学院大学 21 世紀 COE プログラム検証進化可能電子社会, 入手先 (<http://www.jaist.ac.jp/jaist-coe/index-jp.html>) (参照 2019-10-20).
- [12] 荒木啓二郎: ソフトウェア開発現場への形式手法導入—形式手法適用の実経験から得られた知見, *SEC Journal*, Vol.6, No.2, pp.104–107 (2010).
- [13] 実務家のための形式手法—厳密な仕様記述を志すための形式手法入門—厳密な仕様記述入門 (情報処理推進機構ソフトウェア・エンジニアリング・センター), 入手先 (<https://www.ipa.go.jp/files/000026829.pdf>) (参照 2019-10-15).
- [14] カリキュラム標準ソフトウェアエンジニアリング領域 J17-SE (情報処理学会情報処理教育委員会), 入手先 (<https://www.ipsj.or.jp/annai/committee/education/j07/ed-j17-SE.html>) (参照 2019-07-20).
- [15] 苫小牧高専情報科学・工学系 2019 年度 Web シラバス, 入手先 (<https://syllabus.kosen-k.go.jp/Pages/PublicSubjects?schoolid=02&departmentid=12&year=2019&lang=ja>) (参照 2019.07.20).
- [16] 苫小牧高専共通専門科目 2019 年度 Web シラバス, 入手先 (<https://syllabus.kosen-k.go.jp/Pages/PublicSubjects?schoolid=02&departmentid=23&year=2019&lang=ja>) (参照 2019-07-20).
- [17] 大分高専専攻科電気電子情報工学専攻 2019 年度 Web シラバス—形式手法 (西村俊二), 入手先 (https://syllabus.kosen-k.go.jp/Pages/PublicSyllabus?schoolid=48&departmentid=24&subject_code=31AES210&year=2013&lang=ja) (参照 2019-07-20).
- [18] 来間啓伸: トップエスイー実践講座 1 B メソッドによる形式仕様記述 ソフトウェアシステムのモデル化とその検証, 近代科学社 (2007).
- [19] Schneider, S.: *The B-Method: An Introduction*, Palgrave Macmillan (2001).
- [20] 平成 26 年度戦略的基盤技術高度化支援事業の採択結果について, 入手先 (<http://www.hkd.meti.go.jp/hokis/20140728/index.htm>) (参照 2019-07-20).
- [21] 荒木啓二郎: フォーマルメソッドの過去・現在・未来—適用の実践に向けて, 情報処理, Vol.49, No.5, pp.493–498 (2008).
- [22] 来間啓伸, 石川冬樹: 形式手法に基づくソフトウェア開発手法の紹介—B メソッドを中心に, 日本ソフトウェア科学会「コンピュータソフトウェア」, Vol.29, No.4, pp.50–58 (2012).
- [23] Atelier B とは, 入手先 (<http://www.atelierb.eu/ja/>) (参照 2019-07-20).
- [24] The ProB Animator and Model Checker, available from (https://www3.hhu.de/stups/prob/index.php/The_ProB_Animator_and_Model_Checker) (accessed 2019-07-20).
- [25] 大西孝臣: 工業高専生への導入を目的とした B-Method のモデル記述 (1), ウィンターワークショップ 2018・イン・宮島, pp.38–39 (2018).
- [26] 大西孝臣, 堀 武司: 工業高専生への導入を目的とした B-Method のモデル記述 (2), ウィンターワークショップ 2019・イン・福島飯坂, pp.1–2 (2019).
- [27] Abrial, J.-R.: *The B-Book Assigning Programs to Meanings*, Cambridge University Press (1996).
- [28] 小野田博一: 論理パズル BEST100, PHP 研究所 (2015).
- [29] Leuschel, M. et al.: Easy Graphical Animation and Formula Visualisation for Teaching B, *Conference: The B Method, from Research to Teaching, the University of Nantes, France* (2008).
- [30] 中島 震: ソフトウェア工学の道具としての形式手法 (改訂版), 国立情報学研究所「NII Technical Reports」, NII-2007-007J (2007).
- [31] ClearSy: *B Language Reference Manual ver1.8.7* (2010).
- [32] ClearSy: *Atelier B Interactive Prover Reference Manual ver4.0* (2009).
- [33] Massive Open Online Course, The B-Method, available from (<https://mooc.imd.ufrn.br/course>) (accessed 2019-07-20).
- [34] Fisher, G. et al.: Making Formal Methods More Relevant to Software Engineering Students via Automated Test Generation, *Proc. 2016 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '16)*, pp.224–229 (2016).
- [35] Formal Methods Introduction (Peter Gorm Larsen), available from (<https://www.ipa.go.jp/files/000005449.pdf>) (accessed 2019-10-20).
- [36] Jeppu, N. et al.: Teaching Formal Methods at Undergraduate/ Graduate Level: The three perspectives, *2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp.310–315 (2017).
- [37] Westphal, B.: An Undergraduate Requirements Engi-

neering Curriculum with Formal Methods, 2018 IEEE 8th International Workshop on Requirements Engineering Education and Training (REET), pp.1–10 (2018).

- [38] 産業技術総合研究所システム検証研究センター：モデル検査（上級編）—実践のための三つの技法（CVS 教程（2）），ナノオプト・メディア（2010）。



大西 孝臣 （正会員）

2002 年室蘭工業大学大学院工学研究科博士後期課程修了。2004 年苫小牧工業高等専門学校情報工学科助教授。2007 年同情報工学科准教授。2016 年同創造工学科准教授，現在に至る。博士（工学）（室蘭工業大学）。形式手法

の教授法・普及推進を中心とした研究に従事。



吉村 斎 （正会員）

1983 年北海道大学大学院工学研究科修士課程修了。朋立技研（株），（学）桑国学園開発センター，1995 年室蘭工業大学大学院工学研究科博士後期課程修了。同年苫小牧工業高等専門学校情報工学科助手，1998 年同情報工学科助教授，1999 年同情報工学科教授，2016 年同創造工学科教授。2019 年同創造工学科特任教授および名誉教授，現在に至る。博士（工学）（室蘭工業大学）。ロボティクス，組込みシステムおよびエッジコンピューティングに興味がある。精密工学会および日本ロボット学会の正会員。

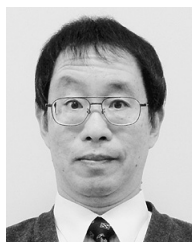
の教授法・普及推進を中心とした研究に従事。



阿部 司 （正会員）

1984 年豊橋技術科学大学大学院工学研究科修士課程修了。同年電電公社入社。2004 年苫小牧工業高等専門学校情報工学科教授。2005 年室蘭工業大学大学院工学研究科博士後期課程修了。2016 年苫小牧工業高等専門学校創造工学科教授，現在に至る。博士（工学）（室蘭工業大学）。組込みシステム，情報通信，計算機工学等の教育研究に従事。精密工学会会員。

の教授法・普及推進を中心とした研究に従事。



稲川 清

1989 年北海道大学大学院工学研究科修士課程修了。同年苫小牧工業高等専門学校電気工学科助手。1992 年苫小牧工業高等専門学校情報工学科講師。1995 年同助教授。2001 年同教授。2016 年苫小牧工業高等専門学校創造工学科教授，現在に至る。弾性表面波デバイスの解析・設計法，FPGA を用いたハードウェア開発および教育，組み込みシステムの開発および教育等に関する研究に従事。博士（工学）（北海道大学）。電子情報通信学会，IEEE，日本工学教育協会各会員。

の教授法・普及推進を中心とした研究に従事。



山本 涼太 （学生会員）

2017 年名古屋大学大学院情報科学研究科博士前期課程修了。現在，同大学院情報学研究科博士後期課程在学中。リバースエンジニアリング，自然言語処理および組込みシステム開発の研究に従事。



堀 武司

1997 年北海道大学大学院工学研究科修士課程修了。同年北海道立工業試験場（2010 年北海道立総合研究機構工業試験場に改組）に勤務。画像計測，組込みシステム，形式手法等の研究および企業支援に従事。