様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１９　日現在

機関番号：　６２６１５
研究種目：　若手研究(A)
研究期間：　2014～2016
課題番号：　２６７００００５

研究課題名（和文）段階的詳細化における複雑さの分散と整合性の保証に関する研究

研究課題名（英文）Research on Complexity Distribution and Consistency Assurance in Stepwise Refinement

研究代表者

石川　冬樹（Ishikawa, Fuyuki）

国立情報学研究所・コンテンツ科学研究系・准教授

研究者番号：５０４５５１９３

交付決定額（研究期間全体）：（直接経費）　　4,500,000円

研究成果の概要（和文）：近年のソフトウェアシステムはますます複雑になっており，その信頼性確保が難しくなってきている．本研究では，抽象度の異なる多段階のモデル（段階的詳細化）を用いる形式手法Event-Bを対象とし，複雑さの軽減や整合性の保証を適切に行うための支援手法・ツールに取り組んだ．特に既存のEvent-Bモデルにおいて，整合性を壊さずに段階構造を変更するリファクタリング手法・ツールを提供することで，理解容易性，検証容易性，再利用性の向上を可能とした．本研究では加えて，Event-Bに限らず一般の要求分析手法にもその成果を展開した．

研究成果の概要（英文）：Recent software systems are increasingly complex and their dependability assurance is challenging. In this work, we investigated methods and tools to support complexity mitigation and consistency assurance by targeting the Event-B method, one of formal methods that uses multi-step models with different abstraction levels (stepwise refinement). The core of the contributions is refactoring method and tool that change the structure of the steps without breaking the consistency to improve understandability, verifiability, and reusability. This work also extended the output not only to the Event-B method but also to general methods for requirements analysis.

研究分野：　ソフトウェア工学

キーワード：　形式手法　システムモデリング　段階的詳細化　サイバーフィジカルシステム

１．研究開始当初の背景

CPS（Cyber-Physical Systems）などの潮流も受け，ソフトウェアが扱う対象は広がっており，ソフトウェアおよびそれと相互作用する環境は，ますます複雑になっている．一方，その開発における信頼性と効率に対する要求は高まるばかりである．効率よく信頼性を高めるためには，上流工程での取り組みが重要とされる．実装詳細を捨象し本質に絞った要求や仕様のモデルを対象とすれば，検証も効率的に行え，後工程での不具合検出による手戻りも防ぐことができる．しかし上記の潮流もあり，仕様モデルの抽象度でも十分に複雑なシステムが増えている．このため，理解や検証を効率的，効果的に行うためには，仕様の複雑さを分散することが重要である．

これらの問題に対し近年，形式仕様記述のための手法の一つである Event-B が盛んに取り組まれている．Event-B は，Dependable Software Forum での取り組みなど，国内産業界でも注目されている．Event-B では環境も含めたシステム全体の複雑な仕様を，抽象的な記述から始め，正当性を検証しつつ徐々に構築する（段階的詳細化）．従来の段階的詳細化は，抽象データ構造をメモリ上のデータ構造に正しく変換するなど，プログラムを得るための比較的単純なものであった．Event-B での段階的詳細化は，仕様内の概念や要件を徐々に導入する自由度が高いものである．このため，理解や検証の容易性，抽象モデルと詳細モデルの整合性など，考慮すべき側面が多くある．

例えばある種の要件については，抽象モデルで定めた以上のことを詳細モデルで追加してはならないという整合性制約がある．すると抽象モデルが妥当そうでも，詳細モデルに至ってから不足に気づき，抽象モデルに戻って追加をせねばならないことがある．さらにその結果，抽象モデルが多くの概念や要件を含み，複雑さが分散されていないものとなってしまうかもしれない．

こういった仕様に関する段階的詳細化の進め方（各段階での導入内容やそれらの順序の決め方）については，科学的，工学的な拠り所が確立されていない．書籍や既存研究でも，うまく進められる段階的詳細化の例や，直感的なガイドラインが示されているが，それらがよい理由は何であるか，他ではだめなのかなどの本質は，ほとんど論じられていない．

仕様内の概念や要件を徐々に導入する段階的詳細化は，ゴール指向など要求分析分野においても重要である．しかし，一段階の詳細化に関する指針（時系列分解など）は示されているが，複数段階の詳細化について，その順序や整合性，複雑さの適切な分散の指針は議論されていない．要求分析では自然言語表現が用いられることが多く属人的になりやすく，また KAOS 手法など形式論理が伴う場合でも，複数段階の詳細化に関する指針や厳密な議論には踏み込んでいない．

以上のように，複雑なシステムの仕様に関する段階的詳細化の進め方について，科学的・工学的な知見を明らかにし，その知見に基づく支援手法を構築することが重要な課題となっている．

２．研究の目的

本研究では，仕様に関する段階的詳細化の進め方（各段階での導入内容やそれらの順序の決め方）について，下記項目の達成を目指す．本研究では，厳密な定式化と議論が可能な Event-B を対象とした取り組みを中心とするが，それに限らない展開も追求する．

【研究項目１】　Event-B における段階的詳細化に関する定式化

【研究項目２】　Event-B における段階的詳細化のための工学手法・ツールとその評価

【研究項目３】　一般的な段階的詳細化への展開

研究項目１では，段階的詳細化に関する複数の計画に対し，複雑さの分散や整合性など，どのような観点から各計画がどう評価されるかを明らかにする（不可能なもの，可能だが不適切，適切さの順位付けなど）．このために，段階的詳細化における構成要素や，それらの依存関係などを明示的に定式化することで，段階的詳細化の進め方に関する議論の道具として確立する．

研究項目２では，段階的詳細化に関する具体的な作業支援を行うための工学手法・ツールを構築し，その評価を行う．特に，段階的詳細化に関する設の様々な候補を確認してその良し悪しを議論し，実際に設計を行う，あるいは設計を変更するための手法・ツールを構築する．この手法・ツールについては，実践的な観点からその有効性・有用性の評価を行う．

研究項目３では，Event-B という特定の手法（言語表現や段階的詳細化の制約）に限らず，より一般的に活用可能な知見や手法を追求する．具体的には，プロブレムフレームなど，よく知られた要求分析手法において段階的詳細化を適切に行い活用するための手法を構築する．

以上の取り組みを行う本研究は，以下の点で独創的であるといえる．

- 段階的詳細化の複数段階に対し，各段階での導入内容やそれらの順序の決め方について，明示的に議論し，科学的知見および工学手法を確立する点
- 概念や要件，およびそれらの間の依存関係などを拠り所として，厳密な整合性と，理解容易性や再利用性などの実用性との双方に取り組む点
- 形式手法に基づき厳密に議論される知

見や手法を，一般の要求分析手法に展開する点

本研究により以下の貢献が期待される．まず，直接的な貢献として，Event-B における段階的詳細化の計画を定める具体的な手法とツールが提供され，産業界にて Event-B を組織的に活用していくことが可能になる．また現在では属人的，芸術的になりがちな，要求や仕様の段階的詳細化においても，指針に基づき一定の効果，品質が担保できるようになる．より長期的には，複雑さの分散に関するメトリクスの定義，システム理解支援（抽象モデル生成）への活用など，より多様な工学アプローチに対する取り組みに発展していくことが期待される．

以上のように，複雑になる一方であるソフトウェアに対し，複雑さの分散，そのための抽象と具体との対応づけという本質に取り組むことにより，安定化・効率化を広く促進していく．

３．研究の方法

(1) 研究項目１

本研究において核となるアプローチは，各段階において導入し扱おうとする要件に対して，依存関係により概念が付随して導入されるという関係を明示的に定式化することである．研究項目１においては，様々な例題を検討することによりこの定式化に取り組んだ．

図１は，第一段階目にて要件 P を，第二段階目にて要件 Q を導入するという段階的詳細化の例を示している．要件には例えば，「駐車場に入っている車の数が定数を超えることがない」,「車の数が定数に達しているならば遮断機は下がっている」といった命題が含まれる．図ではさらに，「要件 P を導入するために概念 a と概念 b が必要」,「概念 b を導入するために概念 c が必要」といった依存関係も示されている（上の例では「駐車場」「遮断機」など）．各段階のモデルは以前の段階のモデルで導入，定義した概念を引き継ぐため，新たに加わった概念のみを導入，定義した上で，要件に対する検証を行う．図では第二段階にて，必要となる 5 個の概念のうち，第一段階にて導入されていない概念 d，概念 e のみが導入される様子を示している（塗りつぶされた斜めの矢印）．

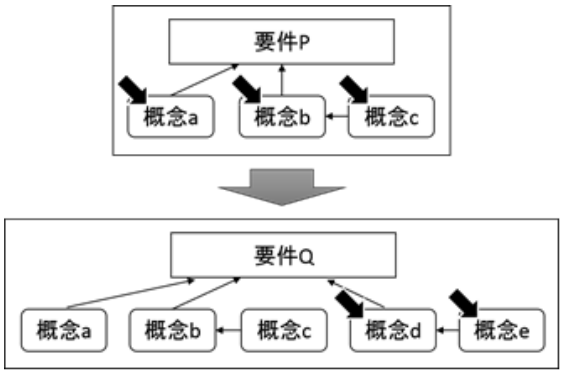

図 1 段階的詳細化の定式化アプローチ

ここで，要件 P と要件 Q の導入順序を逆にすることを考えてみる．すると，最初の段階では要件 Q に関し 5 個の概念が一気に導入され，次の段階では概念が追加されず要件 P の検証のみが行われる．すると，第一段階に複雑さが集中し，第二段階が無意味になる（第一段階で要件 P もともに検証してしまえばよい）．つまり，複雑さの分散に失敗しているということが説明できる．

本研究は，仕様のモデル化とその段階的詳細化について厳密な Event-B，その個々の例題を拠り所とすることにより，このような分析，議論を具体的に，定式化を通して行う．

実際には上記の例は,「要件 P の方が要件 Q よりも抽象的である」と，人間（特に熟練者）は直感で自明と判断できるものである可能性もある．定式化により，そういった直感に対し一つの説明を与えることができる（科学的知見としての成果の例）．一方，ある段階で導入が必要となる概念は，複雑な依存関係や，これまでの要件の導入履歴に応じて決まるため，直感では見抜きにくい場合もある．しかし上記のように，論理的な分析を通し，複雑さを見抜き避けることを支援することができる（工学手法としての成果の例）．

(2) 研究項目２

上記の定式化に基づいて，研究項目２においては，段階的詳細化の支援を行う手法・ツールに取り組んだ．具体的には，可能な段階的詳細化の設計を洗い出すプランニング，および既存の Event-B モデルの段階構造を変更するリファインメントの二つに関する手法に取り組んだ．いずれについても，様々な例題に対し，段階的詳細化に関する明示的あるいは暗黙的な指針を把握すると共に，異なる段階的詳細化を検討することにより，手法の具体化と洗練を反復的に行った．

リファインメントに関する手法については特に有用性が高かったため，Event-B の標準ツールプラットフォームである Rodin におけるプラグインとしての実装にも取り組んだ．

得られた手法およびツールについては４にて述べる．

(3) 研究項目３

代表的な要求分析手法の一つであるプロブレムフレームを対象とし，その段階的詳細化を支援する手法に取り組んだ．プロブレムフレームを選択した理由は，ゴール指向要求分析手法など他の手法と比較して，より問題構造に踏み込んだモデル化を行う点，それゆえに複雑さの軽減が必要となる点である．

プロブレムフレームには段階的詳細化の考え方がないため，そもそも Event-B のような段階的詳細化を考えることの意義や方法

から検討し，その上で段階的詳細化の支援手法を検討した．
　得られた手法については４にて述べる．

４．研究成果

(1) リファクタリング手法・ツール

　Event-B の既存モデルに対して，その段階的詳細化の構造を変更するリファクタリング手法を得た．この手法は，段階の分割と統合を基本的な操作として組み合わせることにより，任意の構造変更を可能としている．抽象度の異なる多段階のモデルに対し，その段階構造を変更するようなリファクタリングは独自である．
　基本的な操作のうち，段階の統合は比較的容易である一方，段階の分割は自明ではない．提案手法においてはまず，分割において抽出したい側面（概念や要件）の集合として与える．これに対し，依存関係を考慮して必要な側面を加えた上で新たな段階を構築する．しかしこの際に証明済みの整合性が崩れてしまうことがあるため，整合性を復元する方法も含めている．この方法は，古典的な基礎理論を従来とは異なるやり方でうまく活用することで導いている．
　このリファクタリング手法については支援ツールを構築した．図 2 にツールの一画面を示す．この画面は，分割の際に抽出する側面を選択するためのものである．例えば，赤で示されている側面は，依存関係を考慮すると現状の抽出対象に加えるべきものを表している．

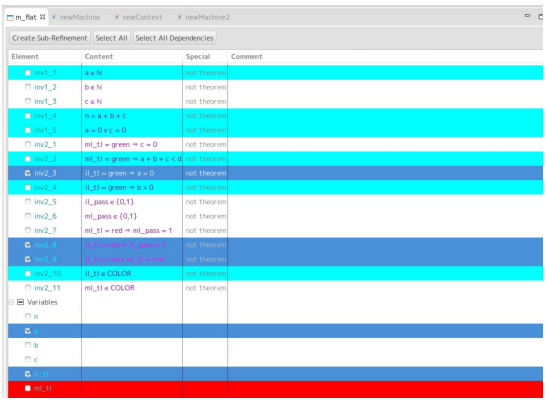

図 2 リファクタリング支援ツール

　リファクタリング手法については，複雑さの軽減に関する評価，再利用性の向上に関する評価を行った．前者については，既存の複雑なモデルを分割することで，自動証明率が向上し，人にとっても把握しやすいモデルに変更することができた．後者については，事前に想定していなかったモデルの一部再利用について，段階的詳細化の構造を変えることで柔軟に対応できることを示した．
　本手法についてはこの結果が高く評価され，形式手法の旗艦国際会議である FM 2016（The 21st International Symposium on Formal Methods）に採択された．

(2) プランニング手法

　Event-B のモデル構築前の計画段階において，段階的詳細化の構造検討を支援するための手法を得た．経験的に得られている段階的詳細化の指針や，随時与えられる開発者の指示に従い，段階的詳細化の構造に関する候補をインタラクティブに出力することができる．このプランニング手法により，教科書のモデルについて，教科書に示されている以外の妥当な段階的詳細化を何種類か示すなど，可能な設計空間の探索を支援することができた．

(3) プロブレムフレームの拡張

　代表的な要求分析手法であるプロブレムフレームにおいて，Event-B にあるように整合性を考慮した段階的詳細化を扱い，またその支援を行う手法を得た．この手法においては，段階的詳細化のパターン（同時に，抽象化により，整合性保証の本質をとらえつつ簡易化するパターン）を提案し，これにより，広く一般の開発者でも，段階的詳細化を活用できるようにした．

(4) 今後の展望

　以上のように本研究においては，複雑なシステムの仕様に対し，複雑さを軽減しつつ整合性保証を扱う段階的詳細化を支援する手法・ツールに取り組んだ．本研究では，近年開発されシステムモデリングを対象とする Event-B 手法を軸として取り組んだ．
　直接的には，Event-B モデルのリファクタリング手法・ツールを中心として，段階的詳細化を効果的・効率的に用いるための支援を実現した．加えて，段階的詳細化に関する様々な知見を得たことで，より長期的な展開も拓くことができた．特に，リファクタリング手法・ツールにより，様々な段階構造を探索する基盤を得ることができたため，段階的詳細化に関する実証的研究や，自動的な構造変更による理解支援・入力支援などの研究の方向性が得られた．
　本研究終了後も，リファクタリング支援ツールの実装強化を続けるとともに，科学研究費基盤研究（B）を中心として発展的な研究を続けている．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 0 件）

〔学会発表〕（計 7 件）

① Tsutomu Kobayashi, Fuyuki Ishikawa, Shinichi Honiden. Stepwise Refinement of

Software Development Problem Analysis. The 35th International Conference on Conceptual Modeling (ER 2016). pp.488-495. Gifu, Japan, November 2016

② Tsutomu Kobayashi, Fuyuki Ishikawa, Shinichi Honiden. Refactoring Refinement Structures of Event-B Machines. The 21st International Symposium on Formal Methods (FM 2016). pp.444-459. Limassol, Cyprus, November 2016

③ Tsutomu Kobayashi, Aivar Kripsaar, Fuyuki Ishikawa, Shinichi Honiden. SliceAndMerge: A Rodin Plug-in for Refactoring Refinement Structure of Event-B Machines. The 6th Rodin User and Developer Workshop. pp.13-14. Linz, Austria, May 2016

④ Tsutomu Kobayashi. Stepwise Refinement of Problem Analysis. The 5th Asian Workshop on Advanced Software Engineering. Nara, Japan, March 2016

⑤ Fuyuki Ishikawa. Toward Flexible Restructuring of Refinement. The 5th Asian Workshop on Advanced Software Engineering. Nara, Japan, March 2016

⑥ Fuyuki Ishikawa. Tsutomu Kobayashi, Refinement Engineering? Shonan Meeting on Science and Practice of Trustworthy Cyber-Physical Systems (TCPS). Miura-gun, Japan, October 2014

⑦ Fuyuki Ishikawa. Refinement Engineering for Reducing Complexity in Reliability Assurance. The 4th Asian Workshop on Advanced Software Engineering. Beijing, China, October 2014

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕
開発したツールの Web サイト
http://research.nii.ac.jp/slicenmerge/

６．研究組織

(1)研究代表者
石川　冬樹（ISHIKAWA, Fuyuki）
国立情報学研究所・コンテンツ科学研究系・准教授
研究者番号：50455193

(2)研究分担者

(3)連携研究者

(4)研究協力者
小林　努（KOBAYASHI, Tsutomu）
東京大学大学院・コンピュータ科学専攻・博士課程学生

本位田　真一（HONIDEN, Shinichi）
国立情報学研究所・アーキテクチャ科学研究系・教授

アレクサンダー　ロマノフスキー
（Alexander Romanovsky）
ニューカッスル大学・計算機科学科・教授