SS2009「形式手法適用」WG

「形式手法」の「適用」について

2009年6月18日

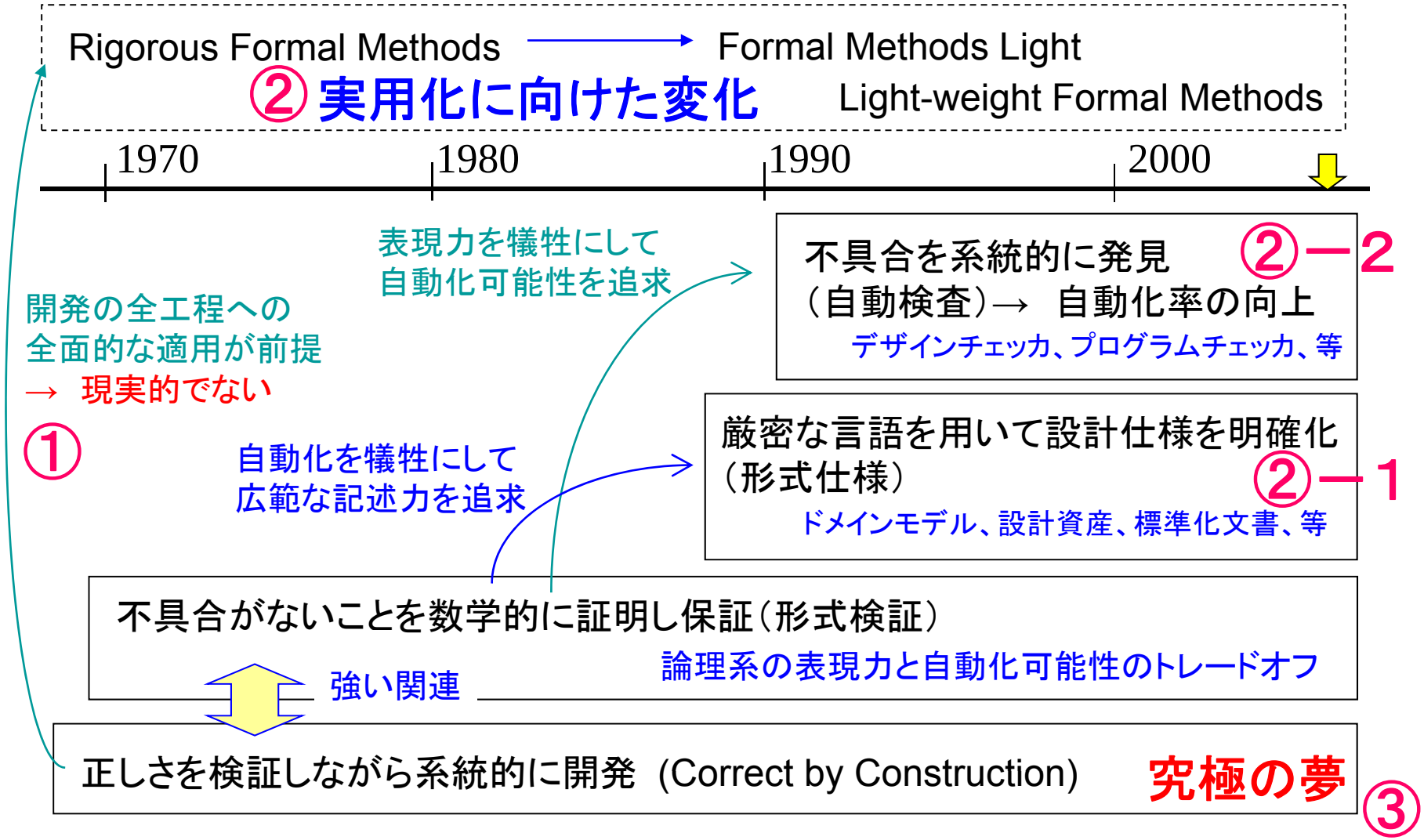
中島震
国立情報学研究所

形式手法適用

- 論点１
  - 「形式手法」とは何で、「適用」するとは何か
- 論点２
  - 「何らかの」形式手法を、「産業界」で適用する
- 論点３
  - 「何らかの」形式手法を、具体的な「システム開発」に適用する

- 論点の次元
  - 形式手法とは
  - 適用する人は
  - 適用する対象は

形式手法の40年


Rigorous Formal Methods
Formal Methods Light
②実用化に向けた変化
Light-weight Formal Methods
1970
1980
1990
2000
表現力を犠牲にして
自動化可能性を追求
不具合を系統的に発見
（自動検査）→ 自動化率の向上
デザインチェッカ、プログラムチェッカ、等
②－2
開発の全工程への
全面的な適用が前提
→ 現実的でない
①
自動化を犠牲にして
広範な記述力を追求
厳密な言語を用いて設計仕様を明確化
（形式仕様）
ドメインモデル、設計資産、標準化文書、等
②－1
不具合がないことを数学的に証明し保証（形式検証）
論理系の表現力と自動化可能性のトレードオフ
強い関連
正しさを検証しながら系統的に開発（Correct by Construction）
究極の夢
③

代表的な形式手法

		適するデザインの観点			リファインメント	自動検査	基礎理論	
		機能	静的	動的（通信機構）				
形式仕様言語	Event-B	○		△（共有メモリ）	FWD		(+ Guarded Commands)	研究 EU FP7
	B メソッド	○	△		FWD		型付き集合論 1階述語論理	実用 フランス
	Z 記法	○	○		FWD / BWD			実用 英国
	Alloy	○	○		Functional	○	1階関係論理	研究 アメリカ
	VDM	○			FWD	△（実行可能仕様）	LPF	実用 英国、デンマーク
モデル検査	SPIN	―	―	○（同期、非同期）		○	オートマトン LTL	実用 アメリカ
	SMV	―	―	○（同期）		○	CTL	実用 アメリカ（ハードウェア）
	UPPAAL	―	―	○（同期）		○	時間オートマトン サブセットCTL	研究 スェーデン

LFM=Light-weight Formal Methods
FML=Formal Methods Light

LPF=Logic of Partial Function

モデル検査の作業分類

大まかな位置づけ

	1	2	3A	3B	3C
	検証性質駆動作業	コンポーネント駆動作業	アルゴリズム記述駆動作業		
			デザイン記法	リバース	プログラム検査
適用工程	分析・設計		詳細設計		テスト
所与の情報	検証性質	システム構成	処理手順記述	プログラム＋設計情報	プログラム
目的	所与の性質を満たす（満たさない）システム条件を得ること	構成要素、要素間の情報連携を検査、確認（アーキテクチャ記述）	処理手順の正しさを確認、不具合発見	プログラムをリバースし、正しさを確認、不具合発見	プログラムを自動解析（対象プログラム、検査性質に制限）
抽象化作業	人手	人手	人手・ツール	支援ツール	自動化ツール
実施例	（NIIで実施）	EJB, BluRay	BPEL解析、等	MODEX、等	Bandera、SLAM、VARVEL、等
展開の困難さ	★★★★	★★★	★★	★★	★

状態ベース仕様

- オペレーション

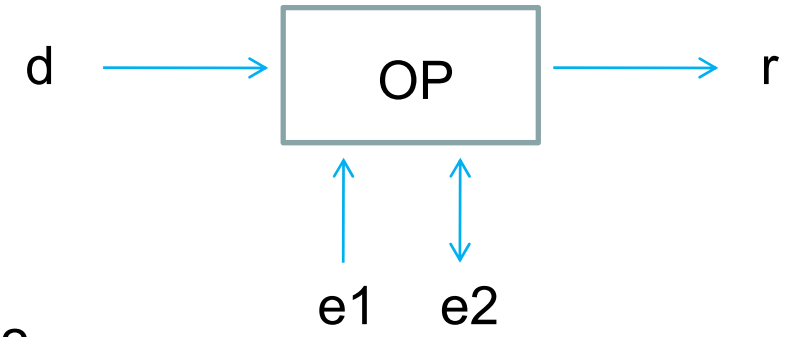
  OP (d : D) r : R

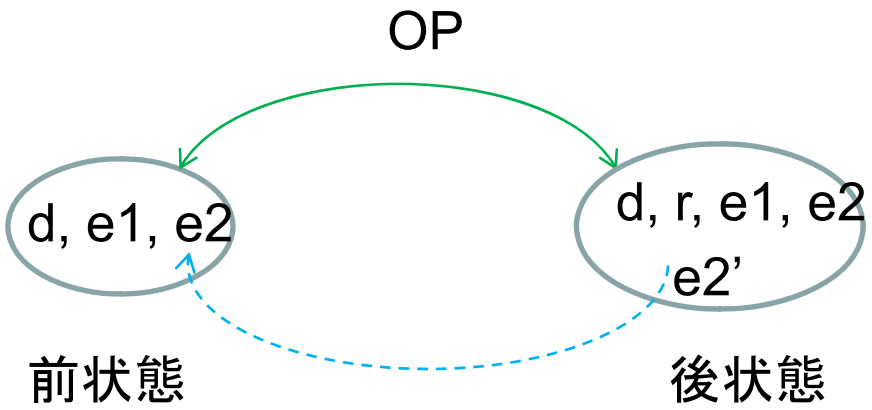
  ext rd e1 : T1,

  wr e2 : T2

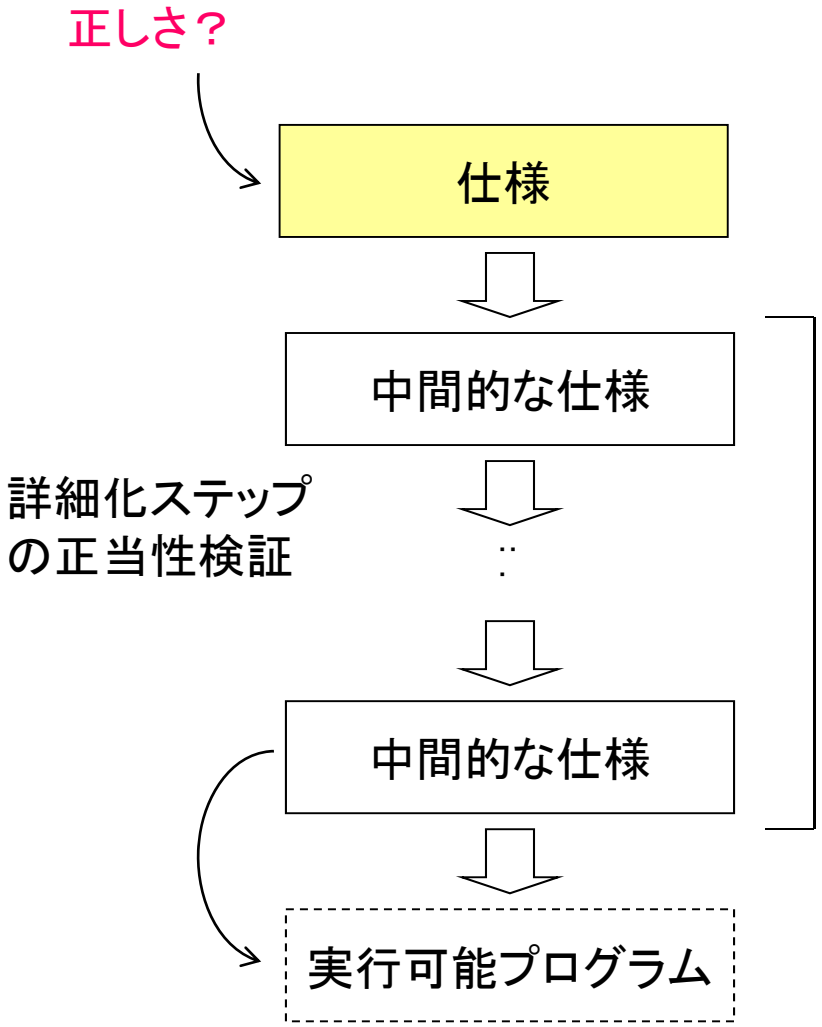
  pre … d … e1 … e2 …

  post … d … e1 … e2’ … r … e2 …





段階的な詳細化



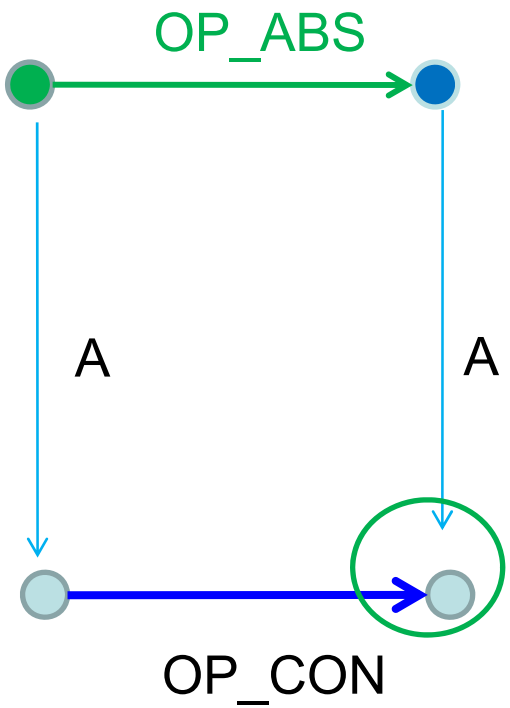
what の記述：システムがどのように
振舞うことが求められているかの記述

抽象的に書かれた仕様を段階的に
実行可能コードに近付けるための
whatとhowが入り交じった記述

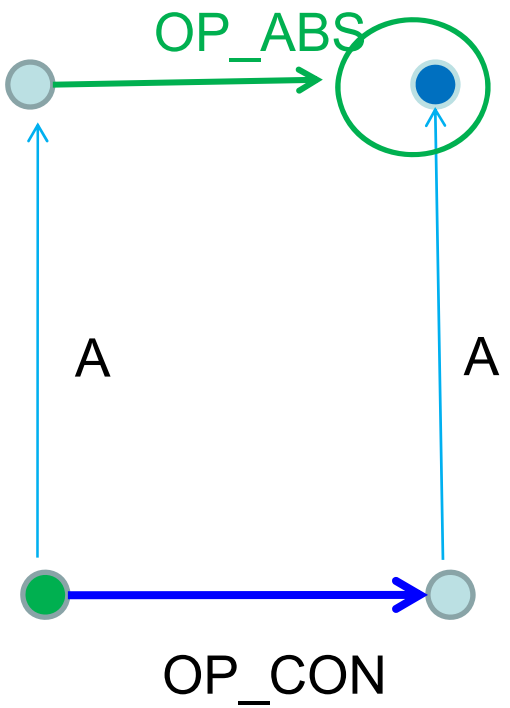
how の記述：システムの振舞いを
どのようにして達成するかの記述

リファインメント

Forward (Downward)



Backward (Upward)



難しさの理由

- 新しい開発技術の導入
  - １５年ほど前：オブジェクト指向開発技術の導入
- 形式手法に固有の考え方、パラダイム
  - 抽象化、模倣関係、等
- モデリング
  - 適切な抽象レベルでの対象把握
- 次のステップへ
  - 教育（形式手法の真髄、パラダイム）
  - 事例の蓄積
  - 知識集積：ガイドライン、ノウハウ（記述、解析）