トップエスイー修了制作

VDM++→Event-B変換器

東京大学　川俣 洋次郎　kawamata@nii.ac.jp

開発における問題点

形式仕様記述言語VDM++を用いて仕様を記述すると、仕様上の不整合をテスティングにより検出することができる。しかし、不整合の検出精度はテストケースの網羅性や検証者の「気づき」に依存してしまい、検証の抜け漏れを回避することが困難であった。

手法・ツールの適用による解決

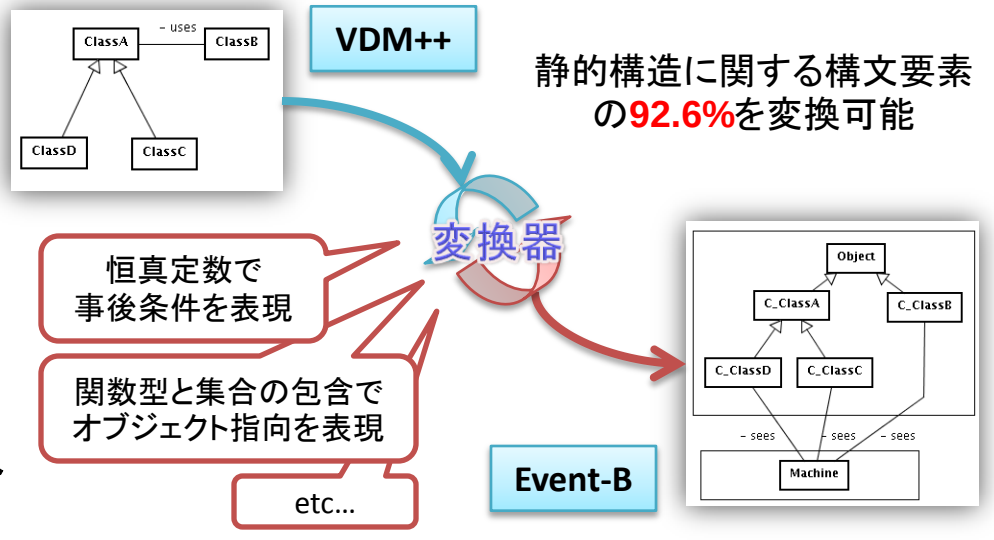
数学的証明による厳密な検証が可能な形式仕様記述言語Event-Bを検証エンジンとして用いることにより、検証の抜け漏れを回避する。本修了制作では、VDM++→Event-B変換器を構築することで「仕様の記述はVDM++で、検証はEvent-Bで」という検証プロセスを実現する。

手法の概要

	言語	検証	表現力
VDM++	簡単	軽量	豊富
Event-B	難解	厳密	限定的

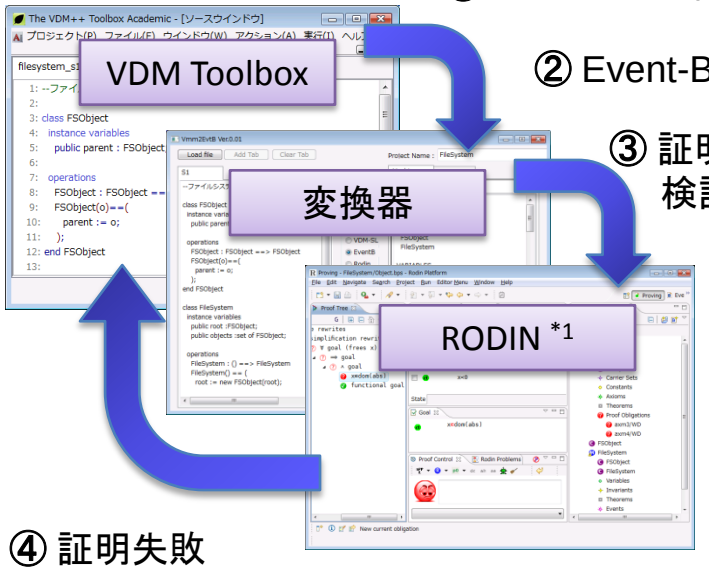
相互補完の関係 → 変換による良いとこ取りが可能

表現力のギャップ → 表現ノウハウの導入による解決



静的構造に関する構文要素の**92.6%**を変換可能

検証の流れ



① VDM++で仕様を記述

② Event-Bへ変換

③ 証明による検証

④ 証明失敗
→ 対応する部分を修正

*1 Event-Bの開発環境

評価

3つの題材について検証実験を実施（100〜140LOC）

	蔵書管理システム	ファイルシステム	ワークフロー
自動証明成功	95	85	145
自動証明失敗	4	11	0

（単位：証明責務数）

原因?

仕様の抜けを検出
（同じ書籍を複数冊扱うかが明示されていない）
→ 検証は有効

証明器の力不足
（補題を与えると証明成功
→仕様の不整合ではない）
判別法が今後の課題