トップエスイー修了制作

VDM++とSPINの連携による検証プロセスの効率化

(株)東芝 ソフトウェア技術センター　　鷲見　毅　　takeshi.sumi@toshiba.co.jp

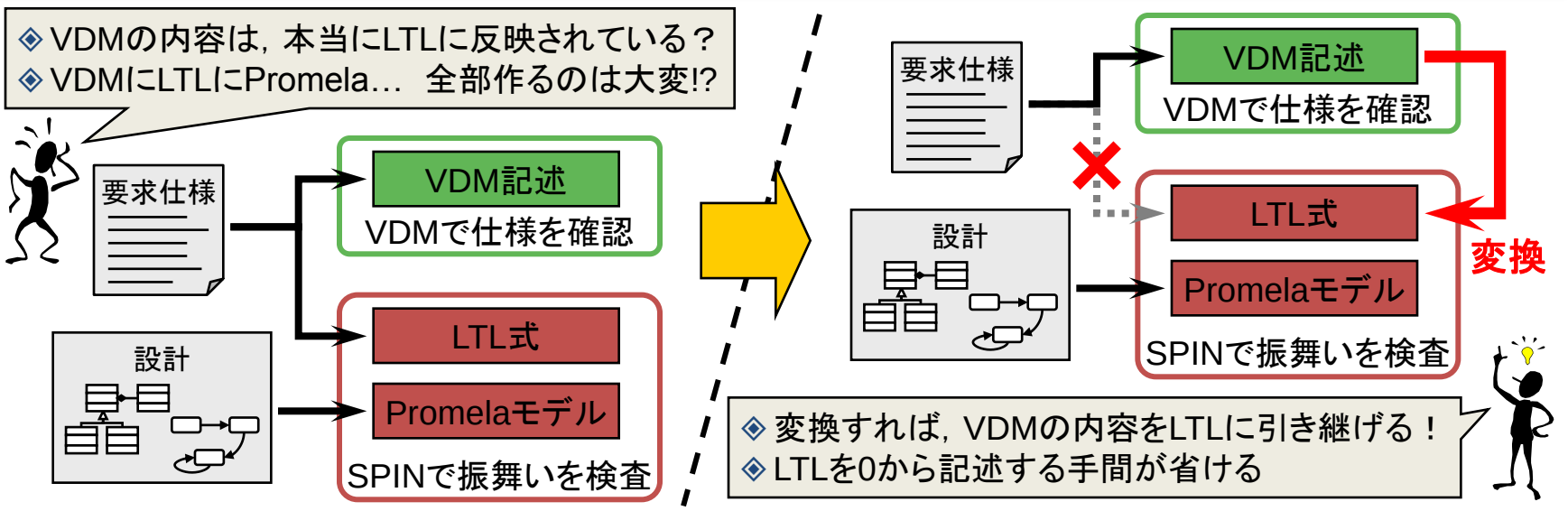
開発における問題点

正しさが確認された仕様が，設計でも満足されているかを確認する為には，形式仕様記述とモデル検査を連携させて使う事が必要になる．
しかし，形式仕様記述とモデル検査を連携させて使う為の手法やツールは，十分に整備されておらず，検証担当者の力量に依存している．

VDM++とSPINの連携手法の提案

VDMによって形式的に記述され，正しさが確認されたシステムの仕様を，SPINの検査に用いる事ができる形式に変換する手法を提案した．
これによって，要求仕様を満足した設計になっているかを，モデル検査によって網羅的に検査する事が可能になった．

提案手法の狙い

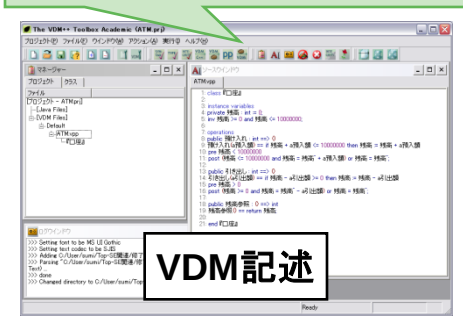


VDM記述からLTL式への変換手法

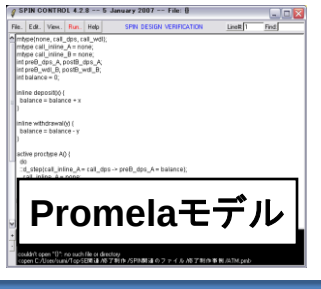
VDM記述の“不変条件”，“事前条件”，“事後条件”の3つを，LTL式に変換
※モデル検査で検査されるべき性質の一部を，VDM記述からの変換によって作成

- 不変条件（invariant）
- 事前条件（pre-condition）
- 事後条件（post-condition）

不変条件、事前条件、事後条件の検査をする為のLTL式構造
- 不変条件 ： [] 不変条件
- 事前条件 ： [] !（操作を実行しようとしている状態 && ! 事前条件）
- 事後条件 ： [] !（操作の実行が終了した瞬間 && ! 事後条件）



▣ 提案手法で，検査の為のLTL式構造を定義
⇒ この式にあてはめれば，VDMで記述された仕様を検査できる
▣ 検査のタイミングは，Promelaの中にモデル化
⇒ タイミングのモデルリング方法も提案



事例に適用し，VDM記述を反映した検査ができる事を確認できた