演習コースⅡ 形式手法と仕様記述
Bチーム

2015/2/27 発表資料

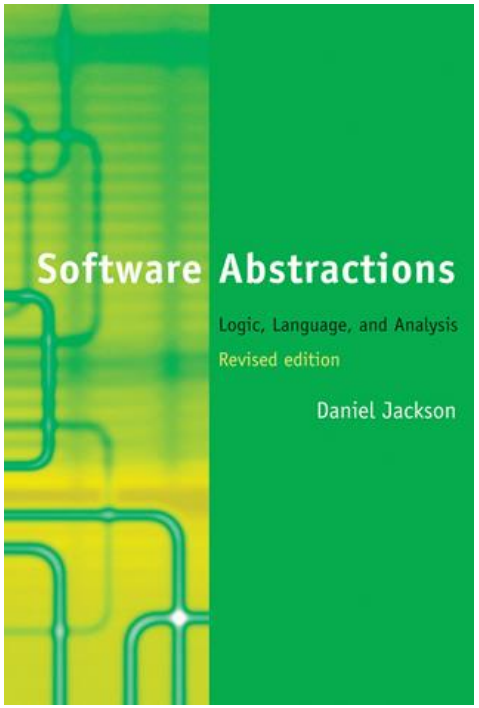
蛸島　昭之

目次

- 課題（活動テーマ）
- Alloyとは？
- Alloyでパズルを解いてみる
- 状態遷移モデルの安全性分析
- N-Switchカバレッジテストケースの生成
- まとめ

課題（活動テーマ）

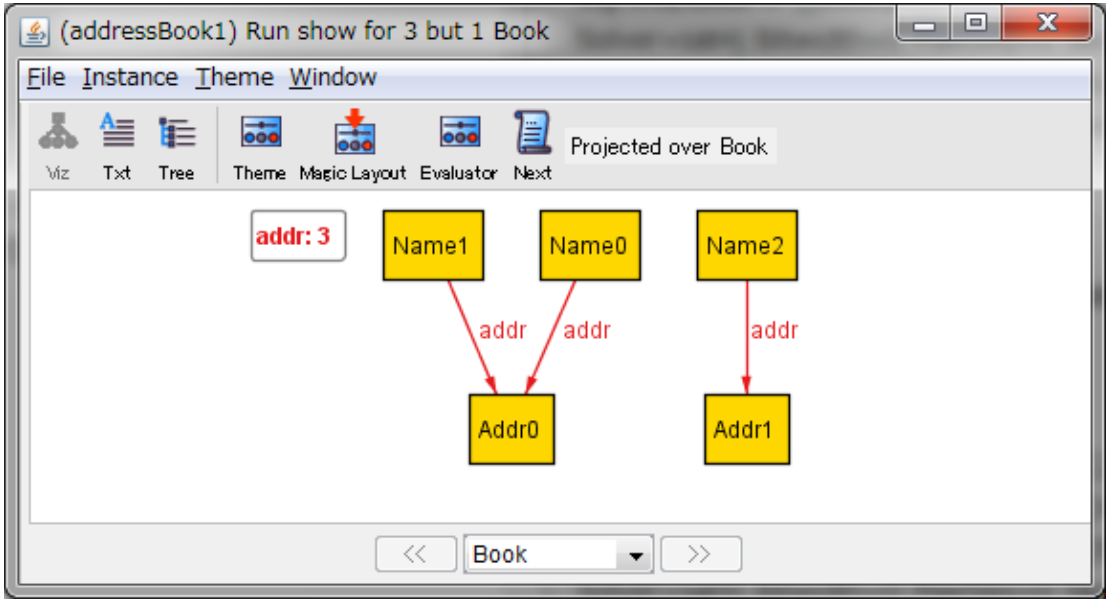
- 形式手法Alloyの車載ソフト開発への適用検討



Alloyとは？

- Alloy：形式仕様言語
- Alloy Analyzer：自動解析ツール
  - 記述された仕様を満たす**充足例**を見つける
  - 記述された仕様に反する**反例**を見つける

```
sig Name, Addr {}
sig Book {
   addr: Name -> lone Addr
   }

pred show (b: Book) {
   #b.addr > 1
   #Name.(b.addr) > 1
   }
run show for 3 but 1 Book

pred add (b, b': Book, n: Name, a: Addr) { b'.addr = b.addr + n -> a }
pred del (b, b': Book, n: Name) { b'.addr = b.addr - n -> Addr }
fun lookup (b: Book, n: Name): set Addr { n.(b.addr) }

pred showAdd (b, b': Book, n: Name, a:  Addr) {
   add [b, b', n, a]
   #Name.(b'.addr) > 1
   }
run showAdd for 3 but 2 Book

assert delUndoesAdd {
   all b, b', b'': Book, n: Name, a: Addr |
      no n.(b.addr) and add [b, b', n, a] and del [b', b'', n] implies b.addr = b''.addr
   }

check delUndoesAdd for 10 but 3 Book
```



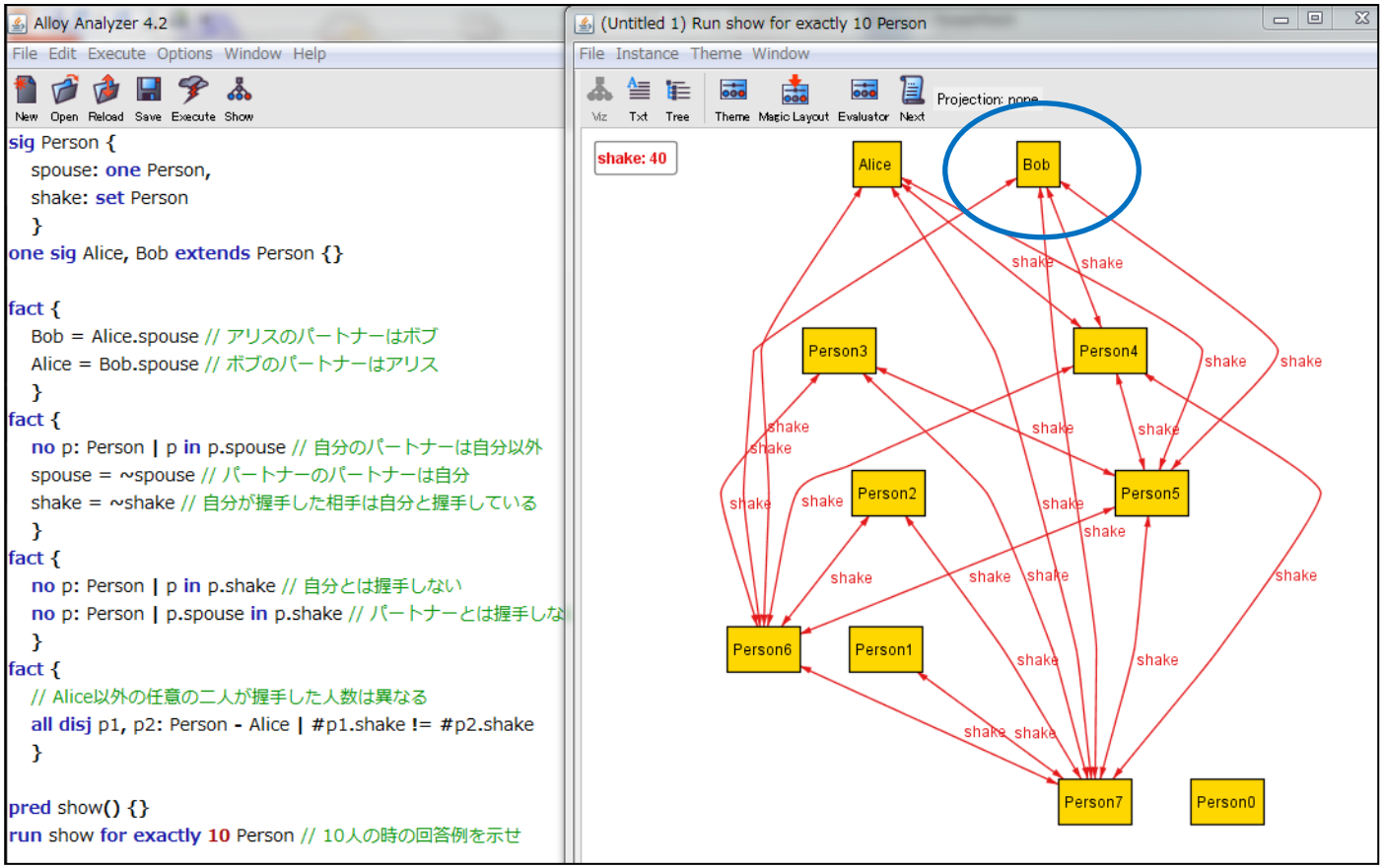
Alloyでパズルを解いてみる (1/2)

Paul Halmos の握手問題

アリスとボブはディナーに四組のカップルを招待しました。
彼らが到着したとき、お互いに握手をしました。
誰も自分自身や自分の連れとは握手しませんでした。
アリスが全員に「あなたは何人の人と握手したの？」と尋ねると一人ひとりの答えは違っていました。
さて、**ボブが握手したのは何人**でしょうか？

Alloyでパズル問題をモデル化すると
解析機が自動で解答（充足例）を見つけてくれる

Alloyでパズルを解いてみる (2/2)



充足例を見ることでBobは4人と握手したことがわかる！

【参考ページ】正しい仕様の見つけ方
http://homepage3.nifty.com/avidya/alloy/docs/alloyintro.pdf

状態遷移モデルの安全性分析(1/2)

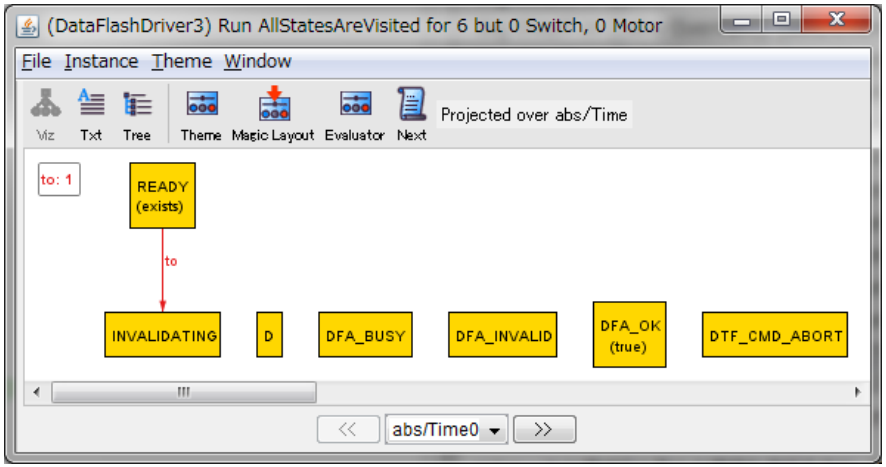
- 組込みシステム開発では状態を持つシステムを対象とすることが多いため、状態遷移の設計が重要
- 状態遷移図と状態遷移表を併用することで、必要な遷移の抜け・漏れがないことを確認しながら状態遷移設計を行うことができる
- 安全性分析を行うには遷移の抜け・漏れを検査するだけでは不十分
  - 安全性の例:車の走行中はドアロック解除が発生しないこと

Alloy Analyzerを用いて状態遷移モデルの
安全性分析が行えるかを検討

状態遷移モデルの安全性分析(2/2)

- 題材
  - フラッシュメモリのデバイスドライバ
- 成果
  - 状態遷移をAlloyのモデルとして表すことができた
- 課題
  - 複雑な安全プロパティをアサーションとして表現するのがむずかしい

```
abstract sig DFA extends Variable { }
one sig
   DFA_OK, DFA_BUSY, DFA_INVALID
extends DFA { }

abstract sig DTF_CMD extends Variable {}
one sig
   DTF_CMD_READ, DTF_CMD_WRITE,
   DTF_CMD_INVALIDATE, DTF_CMD_INVALIDATE2WRITE,
   DTF_CMD_RETRY, DTF_CMD_ABORT
extends DTF_CMD { }

abstract sig ACTIVE extends State { }
one sig READY, ERROR extends State { }
one sig  READING, WRITING, INVALIDATING extends ACTIVE { }
```



N-Switchカバレッジテストケースの生成（1/2）

- N-Switchテスト
  - ある状態遷移の影響がN回先の状態遷移に影響を及ぼすかのテスト[1]
  - N-Switchカバレッジを網羅するテストケースを得るには関係行列や直行表を用いた計算を行う必要があり難易度が高い

安全性分析に用いたAlloyの状態遷移モデルから
N-Switchカバレッジテストケースを自動生成したい

[1] 秋山浩一, N-Switchカバレッジテストの問題点と解決策, SS2013

N-Switchカバレッジテストケースの生成(2/2)

- 成果
  - 簡易モデルによる検討を実施したところ実現できそうな感触が得られた
- 課題
  - 安全性分析に用いたのとは異なる記述スタイルで状態遷移をモデル化することが必要
- 解決策
  1. 安全性分析とN-Switchカバレッジ生成の両方に利用できる統一的なモデル記述スタイルを構築する
  2. 状態遷移図のモデリングツールから2つのAlloyモデルを自動生成できる環境を構築する

まとめ

- Alloyがコーディング前の設計段階で欠陥の検出に役立つことが実感できた
- 有用なAlloyのユースケース（安全性検討とN-Switchカバレッジテストケース生成）は見つかったが具体的な成果まではつなげられなかったため、引き続き検討を続けたい