大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

トップエスイー ソフトウェア開発実践演習

モデル検査を活用し、Androidアプリ設計時の考慮漏れ(設計ミス)を削減する方法について

キヤノン株式会社　　井浦 雅貴

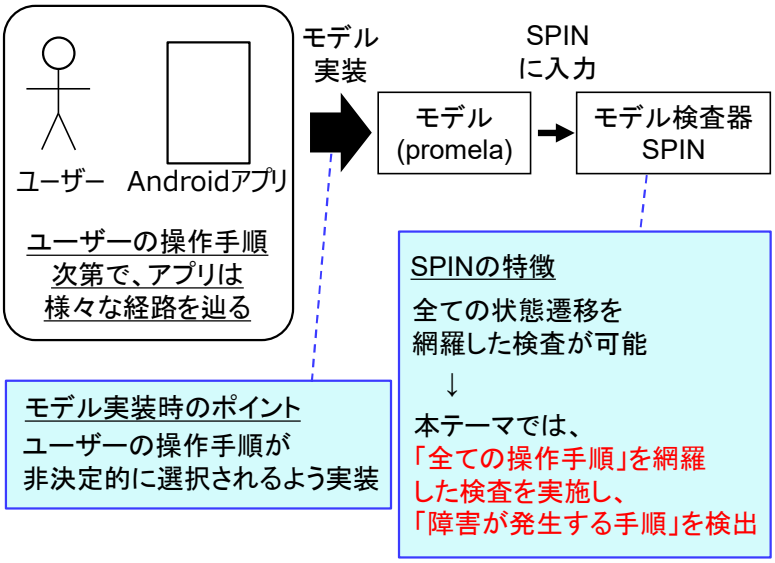
開発における問題点

Androidアプリは、ユーザーの操作手順に応じて、画面の状態がどのように遷移するかが変わる。
自社で開発しているプリンター関連アプリは、
特定の操作手順でのみ発生する障害が埋め込まれることがあるが、ユニットテストや結合テストでは、全ての操作手順を網羅するのが困難なため、障害を見逃してしまう場合があった。

手法・ツールの適用による解決

ユーザーの操作手順に応じて、Androidアプリの画面の状態が遷移する振舞いをモデル化し、モデル検査器SPINで検査を行う。モデル化する際、ユーザーの操作手順が非決定的に選択されるようにすることで、ユーザーの操作手順に関して網羅的な検査を行うことができるようにした。

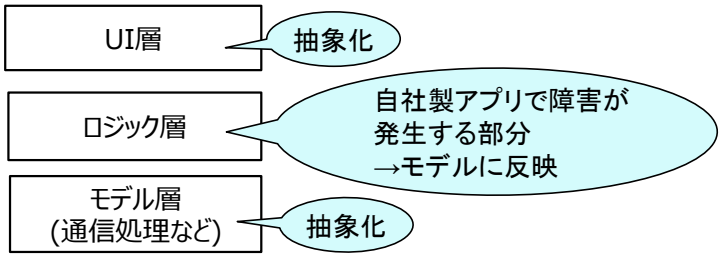
Androidアプリとユーザーが形成するシステムをモデル化



モデル化方法 ~ソースコードを元にモデルを実装~

- ソースコード上の実装ミスを検出できるよう、ソースコードを元にモデルを実装した
- ソースコードの内容を全てモデルに反映すると、状態数が増えて発散する恐れあり
  → 注目しているレイヤー以外は抽象化し、モデル(promela)を実装した

ソースコードのレイヤー



検証内容

上述したモデル化方法で、自社製プリンター関連アプリの中の1つの画面をモデル化し、過去に発生した「ダイアログの多重表示」の障害を検出できるかを検証した。

検証に用いたassert文
assert(ダイアログの表示数をカウントする変数 < 2);

検証結果
- 過去に発生した障害2件を、モデル検査で検出できた。
- モデル検査で報告された「障害の発生手順」は、正しい内容だった。
- 今回検証した範囲では、偽反例は検出されなかった。

まとめ・今後の課題

- 自社製プリンター関連アプリにおいて、ユーザーの操作に応じて画面の状態が遷移する振舞いをモデル化し、SPINによって、ユーザーの操作手順に関して網羅的な検査を行った。
- 過去に発生した「ダイアログの多重表示」の障害を検出できた
  →自職場でモデル検査を活用することで、特定の操作手順でのみ発生する障害を検出できる可能性がある
- 「ダイアログの多重表示」以外の障害を検出できるかは未検討なため、今後検討が必要である。