トップエスイー修了制作

DSLによる設計情報記述に対する誤り検出方法の考察

株式会社NTTデータ
技術開発本部　佐々木高洋　sasakitkh@nttdata.co.jp

開発における問題点

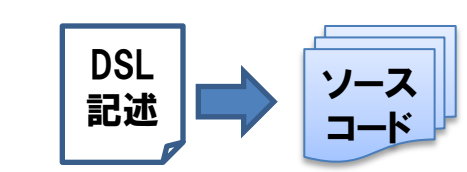
DSLで設計情報を厳密に記述することで，完全なソースコードを自動生成するツールがある

- しかし，設計時点で設計の考慮漏れがある場合は，生成されたコードで，想定外の入力値による実行時エラーが発生する
- 人的レビューでは設計の考慮漏れを全て発見することが難しい

手法・ツールの提案による解決

DSLから生成されるソースコードで実行時エラーが発生するかを，DSL記述の時点で機械的に判定する手法を構築する．
DSL記述を解析して，その設計が暗黙に仮定している入力の事前条件を導出する．さらにその暗黙の事前条件が破られる反例を出力する．

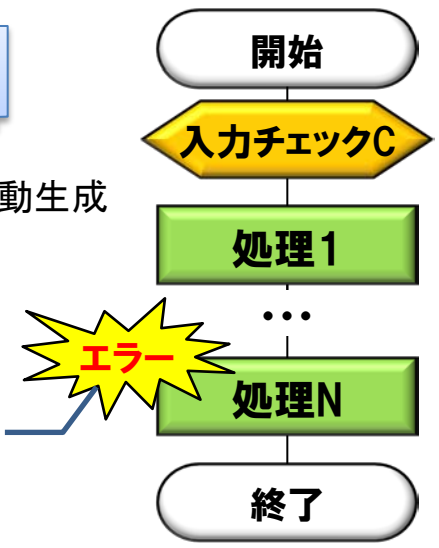
問題点と解決手法の概要



DSL記述からソースコード自動生成

DSL記述の時点で漏れを検出したい

事前条件違反による
実行時エラー
（入力値の想定漏れ）



C≡入力値に対して強制される条件

P≡処理ブロック実行に要求される事前条件

エラーが発生する入力の条件E
E = ¬(C→P)

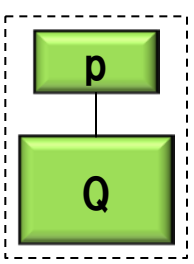
入力値の想定漏れを機械的に検出する手法を考える

手順
1. 入力チェック条件からCを求める
2. 各処理が仮定している暗黙の事前条件を統合して条件Pを求める
3. CとPからエラー入力条件Eを計算する

事前条件の統合方法

1. 処理フローを2分木展開
2. 親子ノード間の事前条件と最弱事前条件の関係を逐次的に定義 ※
3. 深さ優先で再帰計算

※例：ノード群 (p;Q) の事前条件 PRE (p; Q)



単ノードpの事前条件 pre (p)

ノード群Qの事前条件 PRE (Q)

PRE (p; Q) ≡ pre (p) ∧ WPRE (p, PRE (Q))
WPRE (S, I) は最弱事前条件 [S] I を表す

反例の検出例

実例を元にしたサンプル記述に対して手法を適用

DSL
記述

導出結果：入力値が以下のいずれかに該当すれば実行時エラー発生
E1：入力s1が整数キャスト不可
E2 :入力f=1 かつ 入力s1が負数
E3 :入力f=2 かつ 入力s2が6以上

条件に該当する入力値が，入力チェックをすり抜けて処理ブロックで実行時エラーとなることを確認できた

DSL記述の設計漏れを検出することに成功