편리하고 확장 가능한 분석기 생성 도구 만들기

2011-01-07

이승중
ROPAS

필요성

- 새로운 정적 분석기를 만들려고 할 때?
  - **디자인** -> 구현
    - 도메인과 함수들을 정의
    - 함수들의 안전성을 증명

필요성

- 새로운 정적 분석기를 만들려고 할 때
  - 디자인 -> **구현**
  - 구현은 ~~귀찮다~~ 복잡하다
    - 디자인을 옮기는 과정에서 발생하는 버그
    - 이전 분석기에서 사용했던 내용들도 다시 써줘야

목표

- **편리하고** 확장 가능한 도구 만들기
  - 분석할 프로그램의 의미에 집중할 수 있게
  - 기술 언어로 디자인을 쉽게 적을 수 있게
    - 기술 언어 만으로 직접 분석기가 만들어지도록

목표

- **편리하고** 확장 가능한 도구 만들기
  - 많이 쓰이는 부분들을 미리 제공
    - 정수 범위, Boolean 집합 등..
    - 기본적인 CPO(Complete Partial Order)
    - Fixpoint iteration 알고리즘

목표

- **편리하고** 확장 가능한 도구 만들기
  - 기본적인 CPO와 결합해서 다양한 CPO 생성
    - A + B
    - A * B
    - A + { ⊥, ⊤ }
    - A -> B

목표

- 편리하고 **확장 가능한** 도구 만들기
  - 기본 기능을 다른 기능으로 교체하기 쉽게
    - frontend 교체로 다양한 언어 지원
    - 효율적인 고정점 반복 알고리즘으로 교체

요약

- 정적 분석기 구현은 중복되는 일이 많다
  - 분석하고자 하는 **특성**에 집중
  - 분석기의 **안전성 증명**에 집중
  - 간단한 분석기를 만들어서 시험해 볼 수 있게

하는 분석기 생성 도구를 만드는 것이 목표

기존의 불편했던 점, 필요한 기능 제안 환영!

참고자료

- Automatic Generation and Management of Interprocedural Program Analysis

  Kwangkeun Yi and Luddy Harrison

  The 20th ACM Symposium on Principles of Programming Languages, pp. 246-259, Jan. 1993

- Program Analysis System 'Zoo'
  - http://ropas.snu.ac.kr/zoo/
  - The Specification Language Rabbit

- The Program Analyzer Generator
  - http://www.absint.com/pag/