분석기 검증

강지훈, 이영석, 조성근
서울대학교 프로그래밍 연구실

ROSAEC Workshop
2012.7.27.

동기

- 분석기가 올바르다는 것을 어떻게 믿나?
  - 엉터리 디자인, 엉터리 구현

"프로그램을 분석하는 프로그램인데, 설마~ 잘 짰겠지?"

증명 보조기를 이용한 프로그램 검증

- 증명 보조기
  - Coq, Isabelle, ACL2, Agda 등등
- 검증사례
  - CompCert(compiler), seL4(OS)

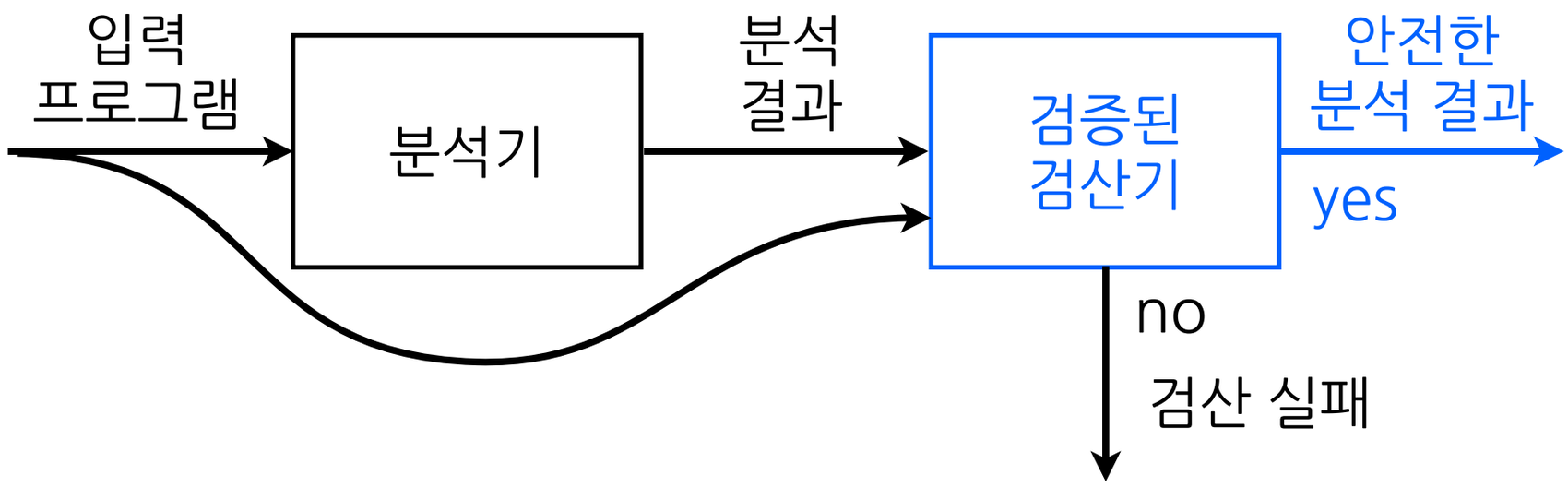
목표

- 증명 보조기, Coq을 이용하여 프로그램 분석기, Sparse Airac을 검증
- 분석결과가 실제 있을 수 있는 실행을 모두 포섭함을 증명

검증의 두 가지

1. 분석기를 직접 검증 (verification)

2. 분석결과를 검산하는 검산기 검증(validation)

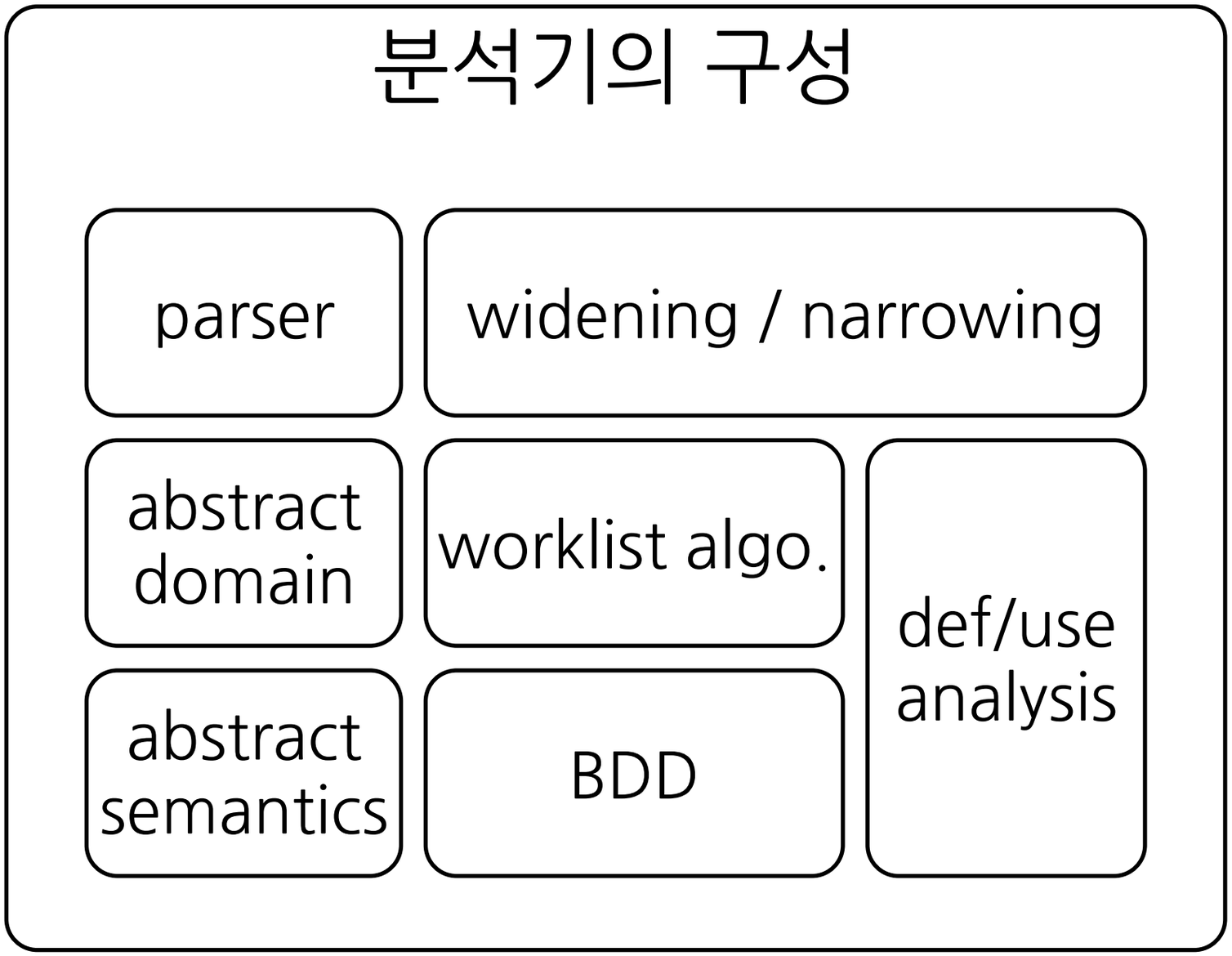


검산기 검증의 특징

- 증명이 간단함
- 분석기의 구현 최적화에 독립적
- 분석결과가 나올 때마다 매 번 검산기를 실행해야 함

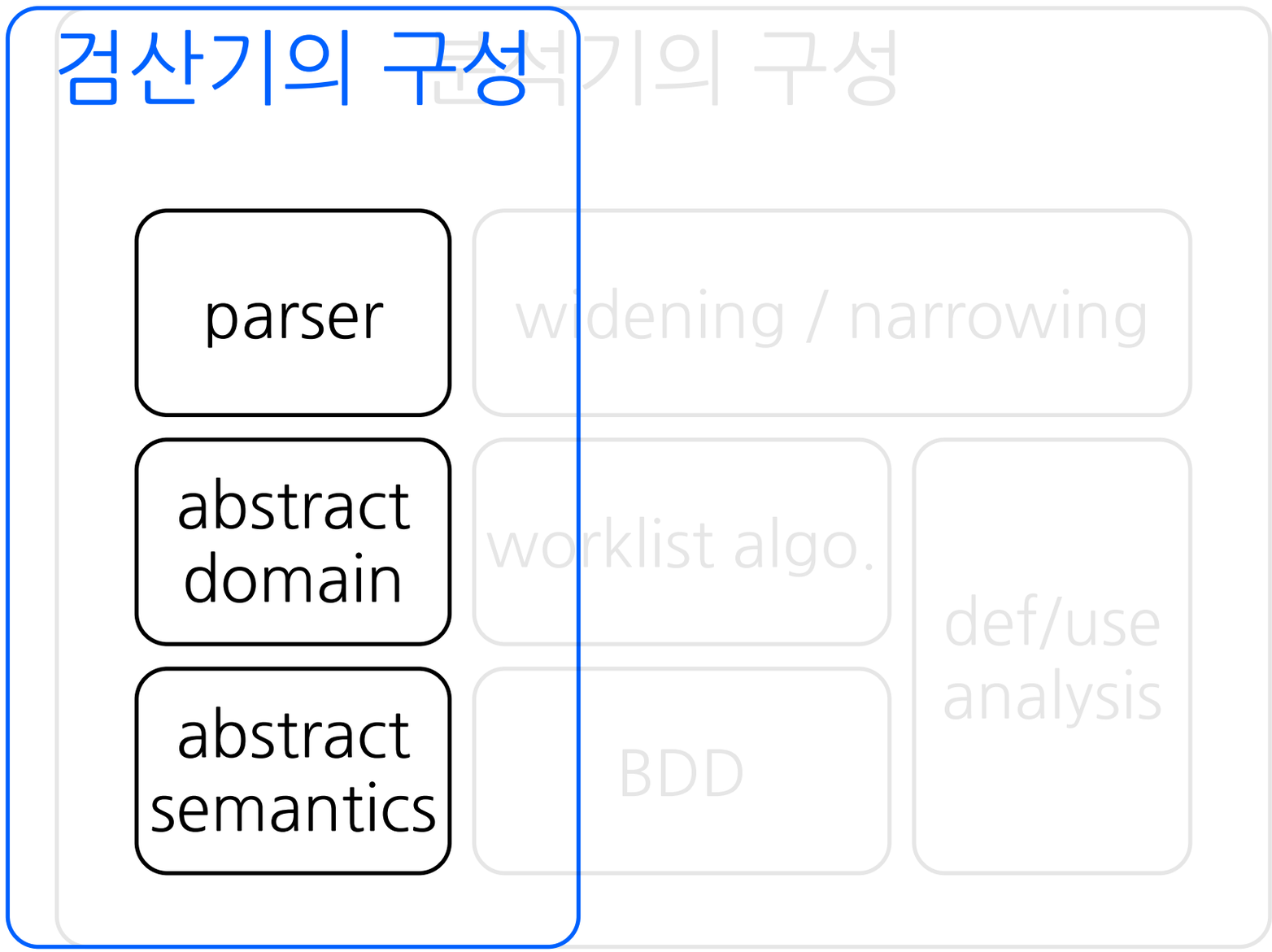
검산기 검증의 특징

증명이 간단함



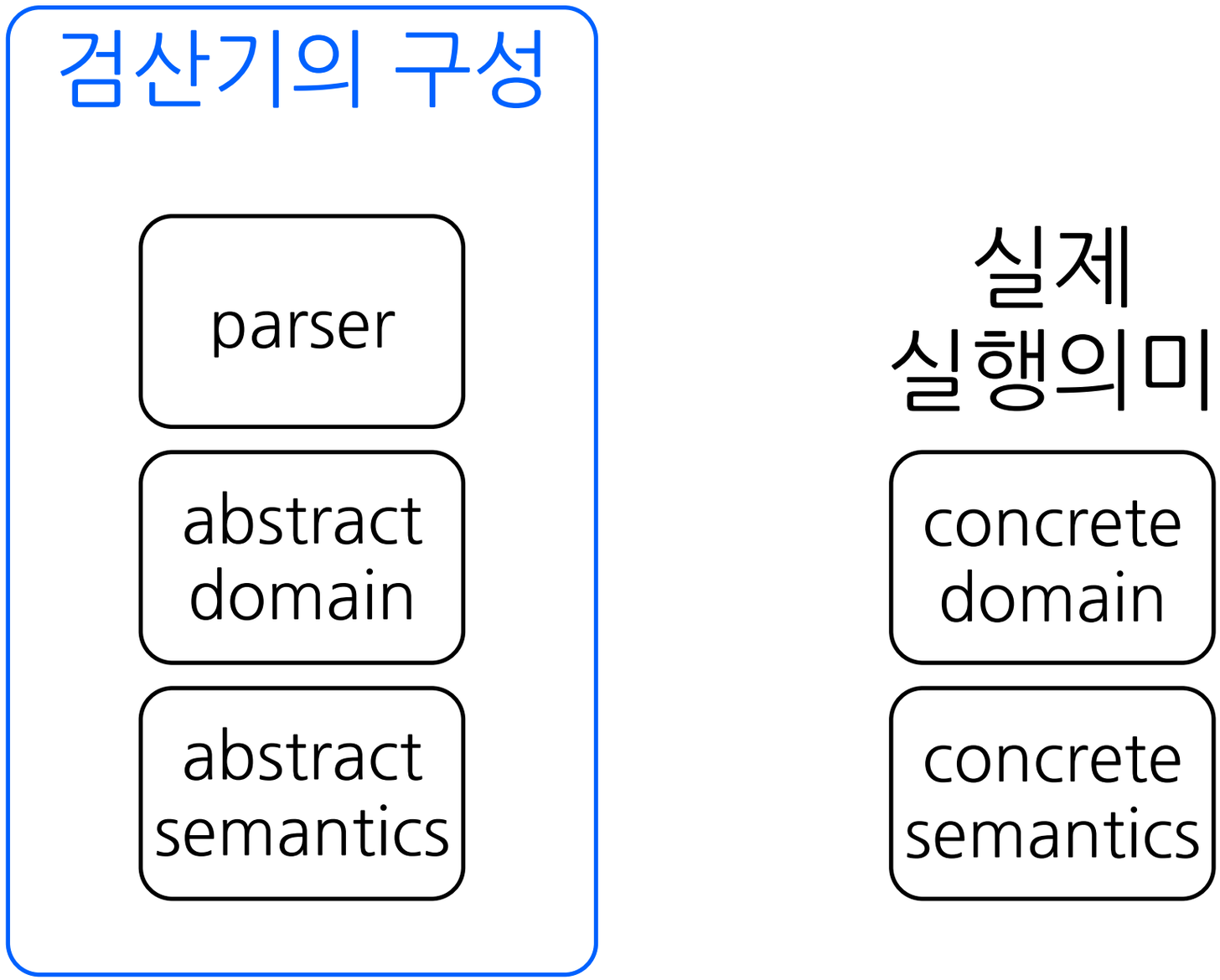
검산기 검증의 특징

증명이 간단함



검산기 검증의 특징

증명이 간단함



요약

- 목표: Coq을 이용하여 분석기의 검산기를 검증
- 검산기 검증(validator)
  - 증명이 간단
  - 분석기의 구현 최적화에 독립적
- 현재 도메인과 실행의미를 구현 중

감사합니다.