분석기 검증

조성근, 이영석, 강지훈
{skcho, yslee, jhkang}@ropas.snu.ac.kr

ROSAEC center
Research On Software Analysis for Error-free Computing
http://rosaec.snu.ac.kr

Programming Research Laboratory
http://ropas.snu.ac.kr

SEOUL NATIONAL UNIVERSITY

동기와 목표

- 분석기의 결과를 어떻게 믿을 수 있을까?
  - Sparse Airac: 44 KLOC in Ocaml
  - 복잡한 최적화 (Localization, Sparse analysis, ...)
- Sparse Airac의 결과를 Coq으로 검증하자.
  - 분석기 전체를 검증하면 분석기 성능이 저하
  - 분석 결과가 대체로 올바르다면 OK!

Coq으로 검증하기

- Xavier Leroy 외: C 컴파일러
- Pichardie 외: 간단한 프로그램 분석기
- 우리: 실용적인 프로그램 분석기의 결과 검증기

프로그램 분석

- 요약 실행 (abstract interpretation) 후 결과 분석

```
0: x := 0
1: while (x < 100) {
2:   x := 2 * x + 1
3: }
4: return x
```

	x
0	[0, 0]
1	[0, 199]
2	[0, 99]
3	[1, 199]
4	[100, 199]

- 분석기를 만들며 가능한 실수들
  - Galois connection을 잘못 만듬
  - 변수들의 Def-Use 관계를 잘못 계산, 잘못된 최적화 수행
  - Abstract transfer function을 잘못 정의
  - join/meet/order와 같은 domain 관련 연산을 잘못 정의
  - ...

증명 방법

- 준비
  - 프로그램 P와 분석 결과 $\hat{s}$를 입력으로 받음
  - 프로그램 P의 상태의 집합 S와 실행 의미 $R \subseteq S \times S$와 초기 상태 $i \in S$ 정의
  - 가능한 분석 결과의 집합 $\hat{S}$를 정의. $\hat{s} \in \hat{S}$가 성립하도록.
  - 안전하게 포섭된다는 관계 $\gamma \subseteq S \times \hat{S}$를 정의.
  - Abstract transfer function $\hat{F} : \hat{S} \to \hat{S}$ 정의
- 검증기를 만들며 증명해야 할 것
  - $\hat{F}$ is monotone ($\hat{a} \sqsubseteq \hat{b}$이면 $\hat{F}(\hat{a}) \sqsubseteq \hat{F}(\hat{b})$)
  - γ is monotone ($\hat{a} \sqsubseteq \hat{b},\ s\ \gamma\ \hat{a}$ 이면 $s\ \gamma\ \hat{b}$)
  - 오른쪽 diagram

$$\begin{array}{ccc} s_1 & \xrightarrow{\quad R \quad} & s_2 \\ \big|\ \gamma & & \vdots\ \exists\gamma \\ \hat{s_1} & \xrightarrow{\quad \hat{F} \quad} & \hat{s_2} \end{array}$$

- 검증기가 확인할 것 $i\ \gamma\ \hat{s}$ $\hat{F}(\hat{s}) \sqsubseteq \hat{s}$
- 안정성 증명

$$\begin{array}{ccc} s_0 & s_1 \xrightarrow{\quad R \quad} & s_2 \\ \big|\ \gamma & \big|\ \gamma & \vdots\ \exists\gamma \\ \hat{s} & \hat{s_1} \xrightarrow{\quad \hat{F} \quad} & \hat{s_2} \\ & \hat{F}(\hat{s}) \sqsubseteq \hat{s} & \end{array} \Rightarrow \quad s_0\ R^n\ s \text{ 이면 } s\ \gamma\ \hat{s} \text{ 이다.}$$

진척 상황

- concrete/abstract semantics 정의 (아직 Full C는 다루지는 못함)
- 전체 증명의 얼개는 맞춤. 세부적인 내용을 채워 넣어야 함
- 도메인 구현
  - equivalence class, partially-ordered set, lattice
  - interval, sum, product, set, map