

Homework 2

SNU 4541.664A

due: ~~4/10~~ 4/17 in class

Kwangkeun Yi

- 이번 숙제의 목적은, D-nogoto(D언어에서 `goto E`가 없는 언어) 프로그램의 정적분석기를 조립식 방식으로 정의하고 그 안전성을 증명해 보는 것이다.
- 여기서 “정적분석기”는 일반화된(generic) 버전이다: 정적분석기(요약해석기)에서 사용하는 요약 의미공간(abstract domains)은 해당 의미공간과 같로 연결되었다고(Galois connection)만 가정한다. 요약 의미공간들을 실제로 정의할 필요는 없다.

D-nogoto언어의 요약문법(abstract syntax)은 다음과 같다.

$$\begin{array}{lcl} C & \rightarrow & x := E \mid *x := E \\ & \mid & C ; C \\ & \mid & \text{if } E \text{ } C \text{ } C \\ & \mid & \text{repeat } C \text{ } E \\ E & \rightarrow & n \quad (n \in \mathbb{Z}) \\ & \mid & E + E \mid E * E \mid - E \\ & \mid & E < E \\ & \mid & x \mid *x \mid \&x \\ & \mid & \text{readInt} \quad (\text{정수입력}) \end{array}$$

분석기를 정의하는 여러분이 할 일을 다음과 같다:

1. 모든 의미구조 $\underline{C}$ 를 정의한다:

$$\underline{C} : 2^{\text{Memory}} \rightarrow 2^{\text{Memory}}.$$

이때 사용하는 모든 의미 연산자들(semantic operators)을 정의하고 그 타입(입출력 의미공간들)이 무엇인지 확인한다.

2. 다음을 가정한다: 요약 의미공간 $\text{Memory}^\#$ 를 포함해서 모든 요약 의미공간들이 갈로아 연결되어 있다. 예를들어,

$$2^{\text{Memory}} \xrightleftharpoons[\alpha]{\gamma} \text{Memory}^\#.$$

3. 요약 의미구조 $\underline{C}^\#$ 를 모든 의미구조와 같은 모양이 되도록 정의한다(homomorphic definition):

$$\underline{C}^\# : \text{Memory}^\# \rightarrow \text{Memory}^\#.$$

오직 다른 점은 의미 연산자들의 요약버전을 사용하는 것이다.

이때 사용하는 모든 요약의미 연산자들(abstract semantic operators)들의 타입(입출력 요약 의미공간들)이 무엇인지 확인한다.

4. 모든 요약의미 연산자들이 안전하게 정의되었다고 가정한다. 즉, 의미 연산자

$$f : 2^A \rightarrow 2^B$$

와 그에 해당하는 요약의미 연산자

$$f^\# : A^\# \rightarrow B^\#$$

사이에 항상 다음의 조건이 만족된다고 가정한다:

$$f \circ \gamma_A \sqsubseteq \gamma_B \circ f^\#.$$

(위에서 A 와 B 는 의미 연산자들에 따라서 다른 집합들이다.)

5. 이러한 가정아래서 다음을 증명한다:

$$\forall C : \underline{C} \circ \gamma \sqsubseteq \gamma \circ \underline{C}^\#.$$