Homework 2
SNU 4541.664A

Kwangkeun Yi

- 이번 숙제의 목적은, 의미구조를 조립식 스타일로 정의하면서 안전한 프로그램분석을 디자인하고 프로그램으로 구현해 보는 것이다.
- 분석대상은 (가상의) 로켓 KX-22의 한 sw모듈이다. 이 sw모듈은 대기권밖에 있는 무인 로켓의 현재 우주위치정보와 속도를 센서로 부터 입력받아서 지구 대기권진입 과정을 밟아 대기권안으로 진입하는 순간 지구표면에 해당하는 위치를 계산하는 모듈이다. 이 계산과정에서 모든 정수값들은 달 공전반경(768,000km)으로 나누었을 때 그 나머지가 항상 지구반경(12,742km) 내에 들어오는 값들이 계산되야 한다. (믿거나말거나)
- 디자인 기한: 10/27(목) 15:30 프린트제출
- 구현 기한: 10/31(월) 24:00 이메일제출 `dklee@ropas.snu.ac.kr`

Exercise 1 (100pts)

무인로켓 KX-22의 sw모듈은 다음 언어로 짜여진 프로그램이라고 하자.

분석하고자 하는 성질: 프로그램이 실행중에 변수들이 가지는 정수값들을 8(7.68 때문)로 나누었을 때 나머지값들이 어떻게 되는지를 알고싶다. 항상 0과 1(1.2742 때문)사이의 값이면 맞는 프로그램이다.

$$
\begin{array}{rcl}
C & \to & x \texttt{ := } E \\
& | & C \texttt{ ; } C \\
& | & \texttt{if } E\ C\ C \\
& | & \texttt{repeat } C\ E \\
E & \to & n \quad (n \in \mathbb{Z}) \\
& | & E \texttt{ + } E \\
& | & \texttt{ - } E \\
& | & x \\
& | & \texttt{readInt[}n, n\texttt{]}
\end{array}
$$

값이 저장되지않은 변수는 임의의 정수값을 가진다. 입력식은 주어진 구간의 값을 입력으로 받는다.

분석기의 디자인은 아래를 완성하는 것이다:

- 각 명령문 C가 실행된 후의 메모리를 모두 모으는 모듬의미구조(collecting semantics) $\underline{C}$를 정의
$$\underline{C} \in 2^{Store} \to 2^{Store}.$$

- 요약 의미공간 $Store^{\#}$을 모듬 의미공간 2^{Store}과 갈로아연결 되도록 정의
$$2^{Store} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} Store^{\#}$$

- 모듬의미구조의 요약본(abstract semantics) $\underline{C}^{\#}$를 정의
$$\underline{C}^{\#} \in Store^{\#} \to Store^{\#}.$$

- 요약본이 올바른지(모듬의미를 포섭하는지)는 임의 프로그램 C에 대해서
$$\underline{C} \circ \gamma \sqsubseteq \gamma \circ \underline{C}^{\#}$$
를 확인하면 된다.

분석기는 관심있는 메모리들 $S \in 2^{Store}$에 대해서 $\underline{C}^{\#}(\alpha S)$ 를 계산하면 된다.

단, 분석목표는 프로그램의 실행후 최종 상태뿐 아니라 프로그램의 실행중 상황을 모두 파악하는 것이므로, $\underline{C}^{\#}(\alpha S)$ 계산을 구현할때 내부의 모든 명령문을 분석한 결과를 따로 기록하면된다. □