HW 3

SNU 4541.664A

Design Due: 11/05, 15:30(in class)

Implementation Due: 11/09, 24:00(email to TA)

Kwangkeun Yi

- 이번 숙제의 목적은, 의미구조를 조립식 스타일로 정의하면서 안전한 프로그램분석을 디자인하는 이론을 수업에서 익혔으므로, 이를 적용해서 분석기를 디자인하고 프로그램으로 구현해 보는 것이다.
- 분석대상은 무인우주기 KX-37C의 한 sw모듈이다.

이 sw모듈은 대기권밖에 있는 무인우주기의 현재 우주위치정보와 속도를 센서로 부터 입력받아서 지금부터 무인우주기가 지구 대기권진입 과정을 밟아 대기권안으로 진입하는 순간 지구상의 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)

Exercise 1 (50pts)

무인우주기 KX-37C의 sw모듈은 다음 언어로 짜여진 프로그램이라고 하자.

분석하고자 하는 성질: 프로그램이 실행중에 변수들이 가지는 정수값들을 768로 나누었을 때 나머지값들이 어떻게 되는지를 알고싶다. 항상 0과 12사이의 값이면 맞는 프로그램이다.

분석기는 의미있는 프로그램("잘 도는" 프로그램)만 입력으로 받는다고 가정한다.

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

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)
$$\underline{C} \circ \gamma \sqsubseteq \gamma \circ \underline{C}^{\#}$$
를 확인한다.

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 사이드로 기록하도록 하면서 계산하게 하면 된다. 그렇게 해서 실행중 상황을 모두 안전하게 미리 파악할 수 있다. □

Exercise 2 (70pts)

숙제문제1에서 디자인한 분석기 `analyzer`를 실제로 구현해 본다.

$$\texttt{analyzer} : \texttt{program} \rightarrow \texttt{result}$$

를 구현하라. TA가 `program`과 `result`의 OCaml 타입과 기타 뼈대코드를 제공할 것이다.