

Homework 6

SNU 4541.664A

due: 6/18 24:00

Kwangkeun Yi

- 이번 숙제의 목적은, HW5에서 각자 구현한 D “watercheck” 분석기(watermark checker)의 아쉬운 점(안전성, 정확도, 모듈화 구현등)을 각자 재정비 하도록 한다.
- 새로운 D “interval” 분석기를 디자인하고 위에서 정비된 분석기를 바탕으로 구현한다.
- 위의 두 분석기의 간추린곱(reduced product) 분석기를 구현한다. 간추린 곱 분석기의 정확도가 두 분석기를 독립적으로 돌린 결과들의 단순 곱보다 좋다는 것을 확인한다.

할 일은 다음과 같다:

1. 조금 확장한 D 언어를 대상으로 디자인과 구현을 확장한다. D언어의 계산식 E 가 다음과 같이 확장되었다:

$$\begin{array}{lcl} E & \rightarrow & \dots \\ & | & E - E \\ & | & E \bmod E \\ & | & E \text{ and } E \\ & | & E \text{ or } E \\ & | & \text{not } E \\ & | & E = E \end{array}$$

2. 기초하는 디자인 스타일은 기계상태 전이과정(transition style)으로 한다.

3. 분석기 디자인의 안전성 증명이 두 가지가 별개로 이루어지도록 확인한다 (modular).

- 분석기 열개의(일반화된(generic) 버전의) 안전성 증명과
- 분석기 열개가 안전하기 위한 요약의미공간과 요약의미연산자들의 안전성 조건의 확인.

따라서, 새로운 분석기의 안전성은 새로운 요약의미공간과 요약의미연산자들의 안전성 조건만 확인하면된다.

4. 분석기의 구현도 두 가지를 별개로 구현해서 모듈화한다. 따라서, 새로운 분석기의 구현은 구현한 의미공간과 의미연산자만 모듈로 구현해서 끼워넣으면 된다.

5. “watercheck” 분석기 **wc**, “interval” 분석기 **tv**, 이 둘의 간추린곱 **wctv**를 각각 구현한다. 해당 요약 의미공간(abstract domains)과 요약 의미연산자(abstract semantic operators)를 정의하고 분석기 프로그램으로 구현한다.

세 분석기들은 모두 다음의 타입이다:

$$\text{dcommand} \times \text{Memory}^\# \rightarrow (\text{index} \times \text{Memory}^\#) \text{list}$$

입력으로 D 프로그램과 초기 요약 메모리(대개 $\perp$)를 받아서, 명령문 C_i 마다 그 명령문이 실행될때 발생하는 모든 시작메모리

$$\langle i, m_i^\# \rangle$$

를 어림잡는다.

6. 세 분석기들은 요약 메모리에 저장되는 요약 값들이 각각 다른 요약공간을 사용하게 된다. 인터벌로 정수값들을 요약하는 세계에서는 넓히기(축지법 widening)와 좁히기(narrowing) 연산자를 구현하고 필요한 곳에서 사용해야 한다.

7. **wc**와 **tv**의 간추린곱(reduced product) **wctv**는 두 개의 분석이 별도로 진행되면서 각자 나온 결과를 무조건 짝짓지않고 서로를 참고해서 더 정확한 짝으로 간추린다.

예를 들어, **wc**는

$$\mathbb{Z}^\# = 2^{\mathbb{Z}_{\text{mod}3}}$$

을 사용하고 `tv`는

$$\mathbb{Z}^\# = \text{Interval}$$

을 사용한다고 하자. 분석중에 $\langle \{1, 2\}, [9, 15] \rangle$ 이 나온다고 하자. 이 쌍을 그대로 사용하지 않고, 두 부품이 뜻하는 교집합 $\gamma\{1, 2\} \cap \gamma[9, 15]$ 에 최대한 가까운 짝으로 간추려서 $\langle \{1, 2\}, [10, 14] \rangle$ 를 사용하면 분석 정확도에 도움된다.

8. 제출할 것은 구현한 분석기들이다. 디자인 문서는 제출할 필요없다.

TA는 다음을 제공할 것이다:

- 확장한 D언어의 파서(parser)를 제공한다. 파서는 ASCII 코드 파일을 받아서 `dcommand` 타입의 데이터를 만들어준다.
- 분석기를 테스트 할 D프로그램들을 제공한다.
- 요약 의미공간 구현을 도와주는 일반화된모듈(parameterized module, functor)을 제공한다.