SNU 4541.664A Program Analysis, Spring 2005
Homework 4

Printed report: **due 5/19 13:00**
Implementation email: **due 5/18 24:00**

Exercise 1 "Redo"
중간고사 시험 문제 7번.

Exercise 2 "Abstract interpreter"

For this problem, you can team with others (team size ≤ 2).

Consider the imperative language C-- of the previous homework (excluding the local blocks):

$$
\begin{array}{llcl}
\text{program} & pgm & \rightarrow & c \\
\text{command} & c & \rightarrow & x := e \mid c \; ; \; c \\
& & \mid & \texttt{if } e \texttt{ then } c \texttt{ else } c \\
& & \mid & \texttt{while } e \texttt{ do } c \texttt{ end} \\
\text{expression} & e & \rightarrow & \texttt{readint} \mid z \mid x \\
& & \mid & e + e \mid e - e \mid e * e \\
& & \mid & e < e \mid e = e
\end{array}
$$

Command changes the memory. Expression computes a value. Command assigns a value to a memory location denoted by a variable, does a sequence of commands, branches based on condition's zero-ness, or repeats the while-body while condition value is non zero. Expression reads an integer from the outside world, is a constant integer, is the value of a variable, or is one of the usual integer or boolean operations.

Implement an abstract interpreter `analyze`

$$\texttt{analyze} : Program \rightarrow (PgmPoint \times Memory) \; table$$

that estimates program variable's integer values by the interval domain. The abstract interpreter must be correct and always terminate.

For example, consider the following program.

```
1:
    x := 1;
2:
```

```
        while x < 1000 do
3:
            x := x+1
4:
        end
5:
```

Your analyzer may conclude that for the program points the integer intervals of x are:

$$
\begin{array}{ll}
1: & undefined \\
2: & [1,1] \\
3: & [1,999] \\
4: & [2,1000] \\
5: & [1000,1000]
\end{array}
$$

As another example, consider the following program.

```
1:
    x := 1;
2:
    y := 2;
3:
    if x
4:                           5:
    then z := x + y          else w := y * -1
6:                           7:
8: (* after the two branches *)
```

Your analyzer may conclude that for each program point the integer interval of the variables are:

$$
\begin{array}{ll}
1: & undefined \\
2: & \{\mathtt{x} \mapsto [1,1]\} \\
3: & \{\mathtt{x} \mapsto [1,1], \mathtt{y} \mapsto [2,2]\} \\
4: & \{\mathtt{x} \mapsto [1,1], \mathtt{y} \mapsto [2,2]\} \\
5: & \{\mathtt{x} \mapsto [0,0], \mathtt{y} \mapsto [2,2]\} \\
6: & \{\mathtt{x} \mapsto [1,1], \mathtt{y} \mapsto [2,2], \mathtt{z} \mapsto [3,3]\} \\
7: & \{\mathtt{x} \mapsto [0,0], \mathtt{y} \mapsto [2,2], \mathtt{w} \mapsto [-2,-2]\} \\
8: & \{\mathtt{x} \mapsto [0,1], \mathtt{y} \mapsto [2,2], \mathtt{w} \mapsto [-2,-2], \mathtt{z} \mapsto [3,3]\}
\end{array}
$$

- Write a report that defines its design and its implementation algorithm.

- Email your implementation to kwang@ropas.snu.ac.kr.

□