CAP - Exercise: abstract interpretation (chapter 9)

Laure Gonnord

Dec. 2016

EXERCISE ▶ **Alpha, Gamma and all that**
Properly define the interval abstract domain.

EXERCISE ▶ **Intervals for arrays**
On the following (Pascal-like) list of instructions :

```
t : array [-5 .. 5] of integer;
assume (x in -5..5,y in 10..20);

if x<=0
then y:= x+y
else y := -(x+y)
end;
t[y] :=1;
```

— Add an assertion to verify the access `t[y] :=1;`

— Propagate intervals to decide if the program is correct

EXERCISE ▶ **Intervals and Planes - 1**

In a big program, we find :

```
i=0;
while (true) {
  /* pilot the plane */
  /* without touching variable i */

  i++;
  if (i >= 20) {
    i=0;
  }
}
```

Somewhere in the loop there are some accesses `t[i]` in a circular buffer implemented as an array `t`, and the correct indices are 0..19. We thus have to print warnings if we cannot prove that they indeed are in this interval.

— Compute the sucessive iterations for intervals on `i`, with the standard widening. what interval do you find ?

— apply one more loop iteration from the invariant you obtained. It is satisfying ?

EXERCISE ▶ **Intervals and planes - 2**

```
i=0;
while (true) {
  /* pilot the plane */
  /* without touching variable i */


  i++;
  if (i == 20) {
    i=0;
  }
}
```

Same questions. Give a cheap solution to the problem.

EXERCISE ▶ **A lack of relationship**

```
/* x is in  -3, 6 */

y = x;

/* bla bla */

z = 1+x*y;
y = sqrt(z);
```

Compute intervals (forwards) for y, z ? Will there be a warning for taking the square root of a possibly negative number ? Is there a problem ?