Exercise session
Fixpoints, abstract interpretation

1.1 Fixpoints

We recall the course definition of reachable states as the limit of the sequence: $Z_n = \{\sigma \mid \exists \sigma_0 \,.\, \sigma_0 \rightarrow^k \sigma \wedge k \leq n\}$.

Question 1. Show that the set of reachable set of a given system with initial set Σ_0 with the transition relation T is the limit of the increasing sequence:

$$Y_0 = \Sigma_0 \ \ldots \ Y_{n+1} = \Sigma_0 \cup R(Y_n)$$

with $R(Y) = \{y \in \Sigma \mid \exists x \in Y\,(x,y) \in T\}$.

Question 2. Same question for $Y_{n+1} = Y_n \cup \{y \mid \exists x\ (x,y) \in T \wedge x \in Y_n\}$.

Question 3. Show that the smallest fixpoint of an increasing function (*monotone*) $f : X \rightarrow X$ where all subsets of X have a lower bound, is the lower bound of the set $\{X \mid f(X) \leq X\}$.

Let us now fix X the set of all subsets of Σ with the $\subseteq$ order, thus $f \leq g$ is equivalent to $\forall x \subseteq \Sigma,\ f(x) \subseteq g(x)$.

Question 4. Let f and g be two monotone functions such that $f \leq g$. Show (with the help of the previous question) that $\mathrm{lfp}\, f \leq \mathrm{lfp}\, g$, $\mathrm{lfp}\, f$ being the least fixpoint of f.

1.2 Intervals

Question 5. Let $x \in a..b$ and $y \in c..d$. Give the intervals for $x + y$ et $-x$.

Question 6. Let $x \in a..b$ and $y \in c..d$ and the following instruction:

/* assertion 1 : $x \in a..b$ */
if $x \leq d$
then
- /* assertion 2 : $x \in \ldots$ */
$\mathscr{I}_1$
/* assertion 3 : $x \in A..B$ */
else
- /* assertion 4 : $x \in \ldots$ */
$\mathscr{I}_2$
/* assertion 5 : $x \in C..D$ */
end ;
/* assertion 6 : $x \in \ldots$ */

where $\mathscr{I}_1$ and $\mathscr{I}_2$ are unknown instructions. Complete assertions $2, 4, 6$ with intervals associated to x.

Question 7. 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

1.3 Widenings

Easy case

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.

Question 8. Compute the sucessive iterations for intervals on `i`, with the standard widening. what interval do you find ? Then apply one more loop iteration from the invariant you obtained. It is satisfying ?

A more difficult case

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


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

Question 9. Same questions. Give a cheap solution to the problem.

Another difficult case

```
while (true) {
  /* piloter l'avion */
  /* sans toucher la variable i */

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

Question 10. Same questions

1.4 A lack of relationship

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

y = x;

/* bla bla */

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

Question 11. 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 ?

1.5 Backward analysis

Study the following program:

```
if (toto) {
  /* code putting x between  500 and 1000 */
} else {
  /* code putting x between  -800 et -100 */
}

/* Some code here*/

/* point A */
if (x >= 0) {
  y = x;
} else {
  y = -x;
}
double z = 1.0 / y;
```

Question 12. What is the interval of X at control point A ? Is an interval forward propagation enough to avoid a division by zero warning on the last line?

Question 13. Do backward propagation to find x values that can arrive on $y = 0$. Conclude.

1.6 Matrices

In the following program:

```
for(int i=0; i<n; i++) {
  for(int j=i+1; j<n; j++) {
    t[i][j] = 5;
  }
}
```

The array `t` is indexed by $0..n-1 \times 0..n-1$. A warning will be launched if we cannot prove that all accesses are inside bounds.

Question 14. Will we manage to do that with intervals? with inequalities of the form $x_{\min} \leq\leq x_{\max}$ et $x - y \leq C_{xy}$?

Question 15. Try with polyhedra, internal loop with the standard widening (draw it!) then one more loop to narrow.

Question 16. Same for the external loop.

Question 17. Give a evolution domain for (i, j).

1.7 Polyedra

Here are the operation we need on polyhedra:

- Intersection of a polyhedron with a test $x \leq y$.
- Compute the image of a polyhedron by an assignment $x := L$, where x is a variable and L a linear expression.
- Compute convex hulls to do tests.

We have the choice to represent polyhedron with inegalities or generators (see the course)

Question 18. Is it possible that a polyhedron has an exponential number of vertices (in its number of faces) ?