Lab 3 - Program Verification
Prepared by : Ms. K.P. Jevitha

Concepts:

- Weakest Preconditions

Tools Required:

- Alt-Ergo Theorem Prover
  Available online : https://alt-ergo.ocamlpro.com/try.html

Instructions:

1. Every question provides 3 components :
   a. Input condition - I
   b. Statement - S
   c. Post-condition - O
2. Steps to solve :
   a. Manually derive the weakest precondition for the given statement **S - wp(S,O)**
   b. For the given input condition I, using Alt-Ergo tool find whether **I ⇒ wp(S,O)**
3. If I ⇒ wp(S,O) is valid, provide the explanation

Summary :

- To prove that a program P is correct with respect to its **contract** which is stated as a **pre-condition I** and **post-condition O**.
- The Weakest Precondition of a **statement S** w.r.t. a **post-condition O** is written as **wp(S, O)**.
- If the **input condition** for program P is **I**, then we want the following theorem to be true:
  I ==> wp(S, O)
- Weakest Preconditions to be done for the following code constructs :
  - **Assignment Statement S : wp(S, O)**
    - ***wp (x = expr, O) = O [x← expr]*** (replace all occurrences of x in O by expr.)
  - **Sequence of Statements S1;S2; : wp(S1 ; S2, O).**
    - ***wp (S1;S2; , O) = wp (S1, wp(S2,O))***

Sequence of Statements :

Eg:

x = 2*y;
y = 5+z+x;
O: y > 0

S1: x = 2*y;
S2: y = 5+z +x;
wp (S1;S2; , O) = wp (S1, wp(S2,O))

wp(S2,O):
y=5+z
=> y > 0 {y = 5+z+x}
=> 5+z +x> 0
wp(S1,wp(S2,O))
=> wp(x=2*y, 5+z +x> 0)
=> 5+z+x>0 {x=2*y}
=> 5 +z+2*y > 0
Required WP is 5+z+2*y > 0

Worked Exercise - 1 (Assignment Expressions)

1)

a) Given S: x = y+1 , O : x > 0, derive the weakest precondition wp(S,O).

b) For the input conditions I given below, check whether I ⇒ wp(S,O) in alt-ergo

i) I : y > 0
ii) I : y = 0
iii) I : y < 0
iv) I : y = 100000
v) I : x = 0
vi) I : x < 0
vii) I : x > 0

Solution:

Weakest Precondition Derivation:

Given:
O: x>0
y+1>0
z+2+1>0

S : x= y +1
O : x > 0

Weakest precondition for assignment : ***wp (x = expr, O) = O [x← expr]***

wp(x =y+1, x>0)
=> y + 1 > 0
Hence, the weakest precondition for the given statement S and post condition O is wp(S,O) = y+1 > 0.

(i) I : y > 0

a. Alt-ergo :

```
goal a:
   forall x,y : int.
        y > 0 ->
        y +1 > 0
```

```
goal a:
  forall x,y : int.
     y > 0 ->
     y +1 > 0

# [answer] Valid (0.0220 seconds) (2 steps)
```

b. Explanation based on Set Theory:

Y > 0 → {1,2,3….} - smaller set (A)

Y > -1 → {0,1,2,3…} - larger set (B)

The set y>0 is contained in set y>-1. **Hence valid**

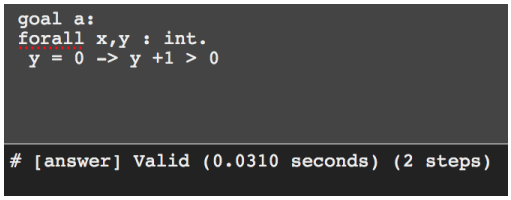
(ii) I : y = 0

a. Alt-ergo :

goal a:

forall x,y : int.

y = 0 -> y +1 > 0



b. Explanation based on Set Theory :

Y = 0 → {0} - smaller set (A)

Y > -1 → {0,1,2,3…} - larger set (B)

The set y>0 is contained in set y>-1. **Hence valid.**

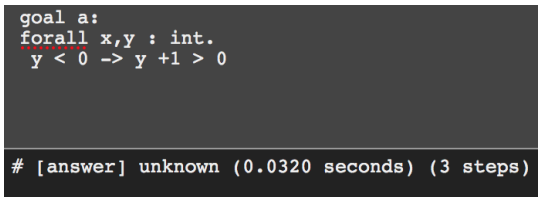
(iii) I : y < 0

a. Alt-Ergo :

goal a:

forall x,y : int.

y < 0 -> y +1 > 0



b. Set Theory Explanation :

Y < 0 → {-1,-2,...}

Y > -1 → {0,1,2,3…}

Since the sets are not comparable, it is not valid.

(vi) I : x < 0

goal a:
forall x,y : int.
x<0 -> y +1 > 0

```
goal a:
  forall x,y : int.
    x<0 ->  y +1 > 0

# [answer] unknown (0.0330 seconds) (3 steps)
```

Set Theory Explanation :
X < 0 → X = {-1,-2,...}, when only x is known in the input condition, we cannot tell anything about the value of Y.

Y > -1 → Y = {0,1,2,3…}
Since the sets are not comparable, it is not valid.

Lab Exercises to be completed

1)

a) Given S: x = y+1 , O : x < 10, derive the weakest precondition wp(S,O).
b) For the input conditions I given below, check whether I ⇒ wp(S,O) in alt-ergo and provide the explanations as shown in example based on set theory and truth table
   i) I : y > 0
   ii) I : y = 0
   iii) I : y < 0
   iv) I : y <> 0
   v) I : y = -100
   vi) I : x = 0

2)

a) Given S: x = 5*y + 20 , O : x + y < 100, derive the weakest precondition wp(S,O).
b) For the input conditions I given below, check whether I ⇒ wp(S,O) in alt-ergo and provide the explanations as shown in example based on set theory and truth table

   i) I : y > 0
   ii) I : y = 0
   iii) I : y < 0
   iv) I : y = -100
   v) I : x > 0

3)

a) Given S: x = y*y , O : x > 1000, derive the weakest precondition wp(S,O).
b) For the input conditions I given below, check whether I ⇒ wp(S,O) in alt-ergo and provide the explanations as shown in example based on set theory and truth table

i) I : y <> 0
ii) I: y > 0
iii) I : y = 100
iv) I : y = -20
v) I : y < -10
vi) I : y > 10

4)

a) Given S: x = y*y + z , O : x > 10, derive the weakest precondition wp(S,O).
b) For the input conditions I given below, check whether I ⇒ wp(S,O) in alt-ergo and provide the explanations as shown in example based on set theory and truth table

i) I : y > 0 and z = 1
ii) I : y = 10 and z = 0
iii) I : y = -20
iv) I : y < -10 and z < 10
v) I : y > 10 and z = 5
vi) I : y > 20 and z < 5

5)

a) Given S: x = 2*y + z ; y = x+5.
O: y > 20
Derive the weakest precondition wp(S,O).
b) For the input conditions I given below, check whether I ⇒ wp(S,O) in alt-ergo and provide the explanations as shown in example based on set theory and truth table

i) I : y > 0 and z = 1
ii) I : y = 10 and z = 0
iii) I : y = -20
iv) I : y < -10 and z < 10
v) I : y > 10 and z = 5
vi) I : y > 20 and z < 5