Program Verification Assignment

Each group must solve this assignment.
Deadline is either 30.05.2019 or 6.06.2019, at the seminar or course.
After 6.06.2019, the assignment cannot be submitted anymore.

HOARE LOGIC

Problem1: Determine the invariant and variant and prove the total correctness for the following factorial program:
Precondition: $x = n \wedge n > 0$
y := 1;
while x > 0 do { y := y $*$ x; x := x − 1 }
Postcondition: y = n!

Problem2: Consider the following fragment program:
Precondition: x>0
while (x > 0) {
y = y + x
x = x - 3
}
Determine the invariant and variant, the postcondition and prove the total correctness.

Problem3: Consider the following Hoare triples:
a. [x = 2] x := y + 1 [y = 1]
b. [y = y + 1] x := y + 1 [y = x]
c. [true] x := y + 1 [false]
d. [true] x := y + 1 [z = 1]
Which of these triples are valid?

Problem4: Determine the invariant and variant and prove the total correctness for the following program:
[x>0]
a := x;
y := 0;
while a /= 0 do
begin
y := y + 1 ; a := a − 1
end
[x=y]

Problem5: Consider the program
while X<0 do
begin
X:=X+1;
Y:=Y-2
end
Determine the weakest precondition wp of the program for the postcondition is Y>=0.

Problem6: Consider the program
[n>=0]
X:=1;
Y:=0;
while Y< n do
begin
X:=m*X;
Y:=Y+1
end
[X=m^n]
Determine the invariant and variant and prove the total correctness.

Problem7: Consider the program
[n>0]
X:=n;
Y:=1;
Z:=1;
while X>1 do
X:=X-1;
Y:=Y+2;
Z:=Y+Z
end
[Z=n^2]
Determine the invariant and variant and prove the total correctness.

SEPARATION LOGIC

Problem8: Compute the frame of the following entailments:

a) z|->nil* x|->y*y|->nil |- z|->nil

b) z|->nil* x|->y*y|->nil |- z|->nil*y|->nil

c) z|->nil* x|->y*y|->nil |- z|->nil*y|->nil*x|->y

d) list(x) *lseg(y,x) |- list(y)

e) list(x) *lseg(y,x) |- list(x)

Problem9: Using symbolic heaps, compute the symbolic execution of the following program:

t:=p;
p:=c;
c:=[c];
[p]:=t;
starting with precondition c|->c'*c'|->nil

Problem10: Using symbolic heaps, compute the symbolic execution of the following program:

t:=p;
p:=c;
c:=[c];
[p]:=t;
starting with precondition list(c).

Problem11: Using symbolic heaps, compute the symbolic execution of the following program:

y:=x;
x:=[x+1];
dispose(y);
dispose(y+1);
y=new(5,5);
[y+1]:=x;
starting with precondition list (a::S) x * list (b::S') z.