Girish Rajani (A20503736) CS 536: Science of Programming Homework S: Loop Invariants and Acof Outlines 1. Minimal and Full Proof Outlines Task 1.1 (Written, 10 points) {x7,0} i:= 0; EinvisxAx=i!} while ica do x:x\*i; i:=i+1 { 3 k.x=k!} Apply rule 9: Add conditions to a loop based on the invariant {27,0} i:=0; Ein isan x=i!} {iszn=i!nica} while ixx do oci=oc ki; 2 i ≤ ox ∧ ox = i!} 1:=1+1 名i sanx=i!ni7,x3 60 {1k.x=k!} We have a proof obligation: {i \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \) \( \ Since is a and ina, we have 12=i. {x= ain x=i!} =7{1 + x= k!}

When x=i, this obligation holds because then x=i!=) x=k!

- Step 1 (two applications): Use wip to propagate the postcondition of the loop body backwards.

{270}

i:=0; {invisana=i!3

while  $i(\infty do)$   $2i(\infty n \infty = i! ni(\infty))$   $2i+1(x*in \infty * i = i+1!)$   $\alpha := \alpha * i;$  i := i+1  $2i(\infty n \infty = i!)$   $2i(\infty n \infty = i! ni \times \infty)$   $3i(\infty n \infty = i! ni \times \infty)$   $3i(\infty n \infty = i! ni \times \infty)$   $3i(\infty n \infty = i! ni \times \infty)$ 

We have a proof obligation: {i < x x x = i! x i < x } = 2i + 1 < x x i x x x i = i + 1! }

> i(x =7 i+1(x => i+1(x\*i x=i! # x\*i=i+1!

To get it!! we need (i+1)\*i!. Since x=i!, we instead need (i+1)\*x to prove this obligations but instead, our proof gave x\*i=i+!!. Hence it is not provable. This probably means our loop invariant is incorrect.

```
Perform Step 1 againi
                      {2,0} {05x1x=0!}
                       Zisocnoc=il3
        1:=0:
       Einu is x 1x=i!}
       while ica do ?isxna=i!nica} $ \\ 2i+1\sa*inx*i=i+1!}
          x= xxi; Zi+1 \x x x=i+1:}
       is=i+T EisxAx=i!}
                      {isanx=i!ni7,x}
       60
                      = 27 k. x = k!}
     have another proof obligation:

\{x,03 \Rightarrow \{0 \le x \land x = 0!\}
We
Using simplify rule we can say that:
              {x7,0} =7 {0(x}
Final
    completed proof outline:
                           8 x 7,03
                        => { 0 < x x = 0! }
      1:=0;
                           Sisanx=il3
    Zinv isxxx=i!3
                          {isanx=i! nica} #7 {i+1 < x*inx*i=i+1.}
    while ix x do
    x:=x*i;
                         {i+16x1x=i+1}}
     i := i + ī
                         Eisana=i!3
                          £i < x / x = i! / i > x }
    00
                        =721k.x=k.3
```

T.

```
Task 1-2 (Written, 12 points)
                                  {x7,0}
         1:= 0.
       Sinv iEXA = i!}
        while icx do
           i= i+T;
         r:= r * i
       00
                                  { r= x! }
Apply rule 9: Add conditions to a loop based on the invariant
                                {x7,0}
         i: = 0.
                                Eisanr=i!nica}
        Einv isxAr=i!}
        while ica do
                                Eisznr=i!}
         i:=i+1;
                                Eisxnr=i!ninz}
           r: = r *i
                                & r=x!}
         60
We have a proof obligation:

{isxr=i!ni7;x} => {r=x!}
            Since icx Airix:
                    i=x so r=i! => r=x!
```

20

- Step 1 (two applications): Use w/p to propagate the postcondition of the loop body backwords. 27,03 1:=5; ordelig and orner EINU ISONT=1!} while ico do ?ison rei! nico ?itison reit = i+1! }
i:=i+i; ?ison rai=i!} r:=rai { {isan r=i!}}

od { {isan r=i! ni7, x}} > { r=x ! } We have a proof obligation: ZiExAr=ilnicx} => Zi+16xArAi+1=i+1!} i(x => i+16x Based on factorial rule: i+1! = i+1 \* i! since r=i! then r=i!=>i! xi+1 => T xi+1=i+1! hence Step 1: {xn0} {05x1=0!} 名にとなれには3 i:=0; 315x1=113 r:=1: EINVISORNEI! 3 Zisznrzi!nicz3 => Zitisznrni+1=i+1!3 while ixxdo Eisanni-il} 1: =1 +1; 215x 1 1=1:3 ristking ELEXAPPILAITIZE 08 => {r=x!} We have a proof obligation: 2×703=> 205×1=0!3

{27,03 = 20623

13

9

2

4

Final completed proof outline: 2×7,03 7205x1=01.3 {ilxn1=i!} 1:=0: 216x 1 = i! 3 rist; Zinv isa Arail3 while ixx do 2ixxx=i!nixx3=72i+1xxxxxi+1=i+1:3 名に幺×ハイヤルニにしる じょニはむ : r:rki 2i = x r = i! 3 えらエハトニンハンフェ3 50 => 2r=x!3 Task 3.1