1

a.

$tc\text{-}s(c) \equiv \forall x \in SV(c): (vtype(x,c) = t \wedge simple(t) \Rightarrow$
$\Rightarrow c.m(x) \in ra(t))$

$tc\text{-}p(c) \equiv \forall x \in SV(c): (vtype(x,c) = t'* \wedge c.m(x) \neq null \Rightarrow$
$\Rightarrow c.m(x) \in SV(c) \wedge vtype(c.m(x), c) = t')$

$p\text{-}targets(c) \equiv \forall x \in SV(c): (pointer(x,c) \wedge c.m(x) \neq null \Rightarrow$
$\Rightarrow ingm(c.m(x), c) \wedge onheap(c.m(x), c))$

We say that $inv\text{-}pr(c)$ holds if the following conditions are fulfilled:

1. $\#\{i \mid c.pr[i] \in L(rSt)\} = c.rd + 1$
2. $last(c.pr) \in L(rSt)$
3. $j \in [0:c.rd] \wedge k \in Irt(j,c) \Rightarrow c.pr[k] \in c.st(j)$

We say that $inv\text{-}rds(c)$ holds if for all $i \in [1:c.rd]$ the following conditions are fulfilled:

1. $vtype(c.rds(i), c) = ft(c.st(i)).t$
2. $c.rds(i) = x \Rightarrow onheap(x,c) \vee ingm(x,c) \vee \exists s \in S^*, j < i: x = ST(j,c)s.$

2.

a) $e = e'.n$

There are types $t_1, t_2, \ldots, t_s \in EF \cup TN$ such that: $etype(e', f) = \{t_1\ n_1; t_2\ n_2; \ldots; t_s\ n_s\}$, $\exists j : n = n_j$ we define

$lv(e,c) = lv(e',c).n$

$etype(e,f) = t_j$

$va(e,c) = \cancel{va(e'.n, c)}\ va(e',c).n$

b)

$e = false$

$lv(e,c) = \perp$

$etype(e,f) = bool$

$va(e,c) = 0$

c)

$e = null$

$lv(e,c) = \perp$

$etype(e,f) = \perp$

$va(e,c) = 0$

3.

a) $e = e' \,!\!= e''$

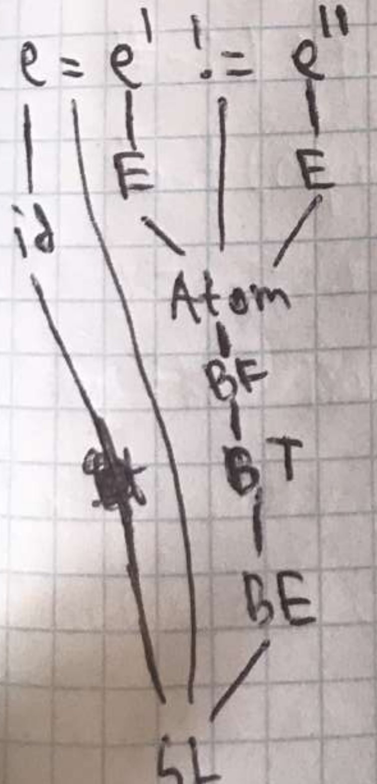
$t' = etype(e'', f) \vee pointer(t') \wedge e'' = null \wedge simple(t')$

where $t' = etype(e', f)$

$etype(e, f) = bool$

$lv(e, c) \in S(c)$

$$va(e, c) = \begin{cases} 1 & va(e', c) \neq va(e'', c) \\ 0 & va(e', c) = va(e'', c) \end{cases}$$



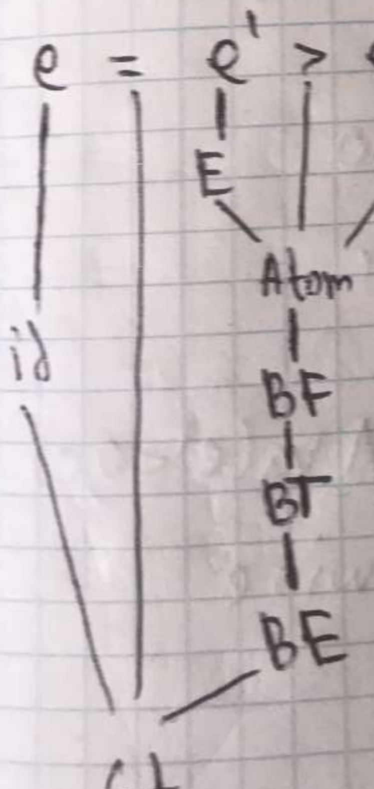
3.6

$etype(e', f) = etype(e'', f) \wedge etype(e', f) \in \{int, uint\}$

$etype(e, f) = bool$

$lv(e, c) \in SV(c)$

$$va(e,c) = \begin{cases} 1 & va(e', c) < va(e'', c) \\ 0 & \cancel{va(e} \text{ otherwise} \end{cases}$$



4. a

$\cancel{e = e' \geq e'' \&\&}$

$e = e' \geq e'' \;\&\&\; e' < 0$

$etype(e', f) = etype(e'', f) \in \{int, uint\}$

$etype(e' \geq e'', f) = bool \wedge etype(e' < 0, f) = bool \Rightarrow$
$\Rightarrow etype(e, f) = bool$

$lv(e, c) \in SV(c)$

$$va(e' \geq e'', c) = \begin{cases} 1 & va(e', c) \geq va(e'', c) \\ 0 & \text{otherwise} \end{cases}$$

$$va(e' < 0, c) = \begin{cases} 1 & va(e', c) < 0 \\ 0 & \text{otherwise} \end{cases}$$

$$va(e, c) = \begin{cases} 1 & va(e' \geq e'', c) \wedge va(e' < 0, c) \\ 0 & \text{otherwise} \end{cases}$$

4.6

$$etype(e, f) = etype(e', f) = etype(e'', f) = etype(e''', f) \in \{int, uint\}$$

$$lv(e, c) \in SV(c)$$

$$va(e' * e'', c) = \begin{cases} va(e', c) * va(e'', c) \text{ tmod } 2^{32}, & etype(e', f) = int \\ va(e', c) * va(e'', c) \bmod 2^{32}, & etype(e', f) = uint \end{cases}$$

~~va((e'*e''~~

$$va(e, f) = \begin{cases} (va(e' * e'', c) - va(e''', c)) \text{ tmod } 2^{32}, & etype(e''', f) = int \\ (va(e' * e'', c) - va(e''', c)) \bmod 2^{32}, & etype(e''', f) = uint \end{cases}$$

4.c

$etype(e', f) = etype(e'', f) \in \{int, uint\}$

$etype(e, f) = t'$ where $etype(x, e) = t'[n]$

$va(e' * e'', c) \in [0 : n-1]$

$lv(e, c) = lv(x, c)[va(e' * e'', c)]$

$va(e, c) = va(x, c)[va(e' * e'', c)]$

5. a

$e = e' \& *$

$lv(e', c) \neq \perp \wedge (ingm(lv(e', c), c) \vee onheap(lv(e', c), c))$

$va(e'\&, c) = lv(e', c)$

$etype(e'\&, e) = etype(e', \cancel{e})*$

$lv(e'\&, c)$ is not defined

$lv(e, c) = va(e'\&, c) = lv(e', c) \in SV(c)$

$etype(e, f) = etype(e', f)$

~~va(e)~~ $va(e, c) = va(e', c)$

5.6

$e = e'^{*}.n$ &

$va(e', c) \neq null$

$t^{*} = etype(e', f) =$

$etype(e'^{*}, f) = t$

$lv(e'^{*}, c) = va(e', c) \in SV(c)$

$va(e'^{*}, c) = va(va(e', c), c)$

$lv(e'^{*}.n, c) = lv(e'^{*}, c).n$

$etype(e'^{*}, c) = \{t_1\ n_1; t_2\ n_2; \cdots t_s\ n_s\}\ \exists j : n = n_j$

then $etype(e'^{*}.n, f) = t_j$

$va(e'^{*}.n, c) = va(e'^{*}, c).n$

$va(e, c) = lv(e'^{*}.n, c) = lv(e'^{*}, c).n = va(e', c).n \in$

$etype(e, f) = etype(e'^{*}.n, f)^{*} = t_j^{*}$

$lv(e, c)$ is not defined

6.

```
uint fc(uint n) {
  uint result;
  if n == 0 {
    result = 1
  }
  else {
    result = fc(n-1);
    result = result * n.
  }
  return result
}
```

7.

we know by definition that $\forall i: c.pr[i] \in L(st) \cup L(rst)$

so $hd(c.pr) \in L(st) \cup L(rst)$

but from the second condition of $inv\text{-}pr(c)$ we know that $last(c.pr) \in L(rst)$ and when $hd(c.pr) = last(c.pr)$ $hd(c.pr) \notin L(st)$

~~we can~~ for example program with only main function and a return statement will disprove that $hd(c.pr) \in L(st)$

```
int main() {
    return 0
}
```

because here $hd(c^0.pr) = last(c^0.pr) \notin L(st)$

8)

proof of 1) $\$f = \{t_1\ h_1, t_2\ h_2, \ldots, t_s\ h_s\}$

$\$gm = \{t'_1\ h'_1, t'_2\ h'_2, \ldots, t'_r\ h'_r\}$

$x = y$

$$etype(X, f) = \begin{cases} t_i, & X = h_i \wedge X \in ft(f).VN \\ t'_i, & X = h'_i \wedge X \in VN \setminus ft(f).VN \end{cases}$$

$$lv(X, c) = \begin{cases} top(c).X, & X \in ft(f).VN \\ gm.X, & \text{otherwise} \end{cases}$$

since $top(c) \in SV(c) \wedge gm \in SV(c) \Rightarrow$

$\Rightarrow lv(X, c) \in SV(c)$

proof of 2)

if $X \in ft(f).VN$ let $X = h_i$

then: $vtype(lv(X,c),c) = vtype(top(c).X,c) =$

$= vtype((f,c.rd).h_i,c) = t_i = etype(X,f)$

otherwise let $X = h_i'$ then:

$vtype(lv(X,c),c) = vtype(gm.X,c) = vtype(gm.h_i',c) =$

$= t_i' = etype(X,f)$.

what we wanted to prove.

proof of 3)

Let $y = lv(X,c)$

by definition of $va(X,c)$ and invariant

$tc(c)$ we have: $va(X,c) = c.m(y) \in ra(vtype(y,c))$

now from ② we have:

$vtype(y,c) = etype(X,f)$ so:

$va(X,c) \in ra(etype(X,f))$

proof of 4)

Let $etype(X, f) = t^*$ and $y = lv(X, c)$ and assume $va(X, c) \neq null$

$$t^* = etype(X, f) = vtype(y, c) \quad \text{(from 2)}$$

$$va(X, c) = c.m(y) \in SV(c) \quad \text{(invariant tc-p(c))}$$

$$vtype(va(X, c), c) = vtype(c.m(y), c) = t' \quad \text{(invariant tc-p(c))}$$

proof of 5)

Let $etype(X, f) = t^*$ and $va(X, c) = c.m(y) \neq null$ where $y = lv(X, c)$. Invariant p-targets(c) gives:

$$ingm(c.m(y), c) \vee onheap(c.m(y), c)$$

which is equivalent to:

$$ingm(va(X, c), c) \vee onheap(va(X, c), c)$$