Assignment1215

Problem 1

符号执行

```
//@ require true

//@ ensure l * l <= n < (l + 1) * (l + 1)

x = n;

//@ generated x = n && true

l = 0;

//@ generated x = n && l = 0 && true

r = n + 1;

//@ generated x = n && l = 0 && r = n + 1 && true

//@ inv l * l <= n < r * r && l + 1 <= r && x == n

while (l + 1 < r) do {

//@ generated l * l <= n < r * r && l + 1 <= r && x == n && l + 1 < r

mid = (l + r) / 2;

//@ generated l * l <= n < r * r && l + 1 <= r && x == n && l + 1 < r && mid = (l + r) / 2

if (x < mid * mid)
  then {
//@ generated l * l <= n < r * r && l + 1 <= r && x == n && l + 1 < r && mid = (l + r) / 2 && x < mid * mid

  r = mid

//@ generated exists r', l * l <= n < r' * r' && l + 1 <= r' && x == n && l + 1 < r' && mid = (l + r') / 2 && x < mid *
mid && r = mid
  }

  else {
    //@ generated l * l <= n < r * r && l + 1 <= r && x == n && l + 1 < r && mid = (l + r) / 2 && x >= mid * mid

    l = mid

    //@ generated exists l',  l' * l' <= n < r * r && l' + 1 <= r && x == n && l' + 1 < r && mid = (l' + r) / 2 && x >=
mid * mid  && l = mid

  }
//@ target l * l <= n < r * r && l + 1 <= r && x == n
}

//@ generated l * l <= n < r * r && l + 1 <= r && x == n && l + 1 >= r
```

验证条件

```
x = n && l = 0 && r = n + 1 && true |-- l * l <= n < r * r && l + 1 <= r && x == n
```

```
exists r', l * l <= n < r' * r' && l + 1 <= r' && x == n && l + 1 < r' && mid = (l + r') / 2 && x < mid * mid && r =
mid
\/
exists l',  l' * l' <= n < r * r && l' + 1 <= r && x == n && l' + 1 < r && mid = (l' + r) / 2 && x >= mid * mid  && l =
mid |-- l * l <= n < r * r && l + 1 <= r && x == n

|-- l * l <= n < r * r && l + 1 <= r && x == n
```

```
l * l <= n < r * r && l + 1 <= r && x == n && l + 1 >= r |-- l * l <= n < (l + 1) * (l + 1)
```

Problem 2

符号执行

```
//@ require sll(x)
//@ ensure sll(x)

t = x;

//@generated sll(x) && t = x

//@inv sllseg(x,t) * sll(t)
while (t != 0) do {
//@generate t!=0 && sllseg(x,t) * sll(t)
//@aux  sllseg(x,t) * store(t, u) * store(t + 8, q) * sll(q)
t = * (t + 8)
//@generate t'!=0 && sllseg(x,t') * store(t', u) * store(t' + 8, q) * sll(q) && q = t
//@target sllseg(x,t) * sll(t)
}
//@generated sllseg(x,t) * sll(t) && t = 0
```

验证条件

```
sll(x) && t = x |-- sllseg(x,t) * sll(t)
```

```
t'!=0 && sllseg(x,t') * store(t', u) * store(t' + 8, q) * sll(q) && q = t |-- sllseg(x,t) * sll(t)
```

```
sllseg(x,t) * sll(t) && t = 0 |-- sll(x)
```