

Reasoning about binary search

Here is the binary search for integer square root with all the assertions in place and fully spelled out. There is some additional commentary at the end.

```

0  {L2 ≤ n < U2 ∧ (0 ≤ L < U)} -- Invariant
1  while (U ≠ L+1) do
2    {L2 ≤ n < U2 ∧ (0 ≤ L < U) ∧ U ≠ L+1} -- Invariant and loop condition
2a  {L2 ≤ n < U2 ∧ (0 ≤ L < U) ∧ U ≥ L+2} -- Inv. and loop cond. rewritten
3    if (((L+U)/2)**2 ≤ n) then
4      {L2 ≤ n < U2 ∧ (0 ≤ L < U) ∧ U ≥ L+2 ∧ ((L+U)/2)2 ≤ n}
          -- Inv AND loop cond. AND if cond.
5      {(((L+U)/2)2 ≤ n < U2 ∧ (0 ≤ ((L+U)/2) < U)} -- wp(L=(L+U)/2, {invariant})
6      L = (L+U)/2
7      {L2 ≤ n < U2 ∧ (0 ≤ L < U)} -- invariant
8    else
9      {L2 ≤ n < U2 ∧ (0 ≤ L < U) ∧ U ≥ L+2 ∧ n < ((L+U)/2)2}
          -- Invariant AND loop cond. AND NOT if cond.
10     {L2 ≤ n < ((L+U)/2)2 ∧ (0 ≤ L < (L+U)/2)}
          -- wp(U = (L+U)/2, {invariant})
11     U = (L+U)/2
12     {L2 ≤ n < U2 ∧ (0 ≤ L < U)} -- invariant
13   fi
14   {L2 ≤ n < U2 ∧ (0 ≤ L < U)} -- invariant
15 end
16 {L2 ≤ n < U2 ∧ (0 ≤ L < U)} -- invariant
17 {L2 ≤ n < U2 ∧ (U == L+1) ∧ (0 ≤ L < U)}
    -- Invariant and not loop cond.
18 {L2 ≤ n < (L+1)2}
    -- postcondition for program

```

I've left off the initialization assignments for U and L which you should be comfortable with by now.

Explanations for steps

From 2 to 2a: $L < U \wedge U \neq L+1$ is the same as $L < U \wedge U \geq L+2$ which is the same as $U \geq L+2$.

Line 4 implies line 5 and line 9 implies line 10: generally just a rearrangement of terms along with dropping a some that are implied by others. For example, we drop the $L^2 \leq n$. You need one more observation however for these two steps: if two numbers are separated by at least 2 then their average is at least one smaller than the larger of the two numbers. That is $(U \geq L+2)$ implies $((U+L)/2) < U$. Similar reasoning in the else case allows us to conclude that $(U+L)/2 > L$. Furthermore, the average of two non-negative numbers is non-negative.

Line 17 implies line 18: substitute equals for equals and drop the unneeded conjuncts.