

Reasoning about binary search

In class today at the end I was a bit hurried and glossed over some of the steps in the axiomatic analysis of the binary search algorithm. Here is the algorithm with all the assertions in place and fully spelled out. There is some additional commentary at the end.

```

0  { $L^2 \leq n < U^2 \wedge (0 \leq L < U)$ }
1  while  $U! = L + 1$  do
2    { $L^2 \leq n < U^2 \wedge (0 \leq L < U) \wedge U! = L + 1$ } -- I and B
2a  { $L^2 \leq n < U^2 \wedge (0 \leq L < U) \wedge U \geq L + 2$ } -- I and B rewritten
3    if  $((L+U)/2)^2 \leq n$  then
4      { $L^2 \leq n < U^2 \wedge (0 \leq L < U) \wedge U \geq L + 2 \wedge ((L+U)/2)^2 \leq n$ } -- I and B and iftest
5      { $((L+U)/2)^2 \leq n < U^2 \wedge (0 \leq ((L+U)/2) < U)$ } -- wp( $L = (L+U)/2$ , {I})
6       $L = (L+U)/2$ 
7      { $L^2 \leq n < U^2 \wedge (0 \leq L < U)$ } -- invariant I
8    else
9      { $L^2 \leq n < U^2 \wedge (0 \leq L < U) \wedge U \geq L + 2 \wedge n < ((L+U)/2)^2$ }
        -- I and B and not iftest
10     { $L^2 \leq n < ((L+U)/2)^2 \wedge (0 \leq L < (L+U)/2)$ } -- wp( $U = (L+U)/2$ , {I})
11      $U = (L+U)/2$ 
12     { $L^2 \leq n < U^2 \wedge (0 \leq L < U)$ } -- invariant I
13   fi
14   { $L^2 \leq n < U^2 \wedge (0 \leq L < U)$ } -- invariant I
15 end
16 { $L^2 \leq n < U^2 \wedge (0 \leq L < U)$ } -- invariant I
17 { $L^2 \leq n < U^2 \wedge (U == L + 1) \wedge (0 \leq L < U)$ } -- I and not B
18 { $L^2 \leq n < (L + 1)^2$ } -- postcondition for program Q

```

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

Explanations for steps

From 2 to 2a: $L < U \wedge U! = L + 1$ 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.