A Program Proving Subtlety

Consider the proof of the program assertion {X ≥ 0} X := X+1 {X > 0}.

It is clear that this assertion is true, and so we want our deduction system to provide its proof. Using the axiom of assignment we have
|— {X+1 > 0} X := X+1 {X > 0}

Now X+1 > 0 is logically equivalent to X > -1, and if the domain for the variable X is the Integers then X > -1 is in turn logically equivalent to X ≥ 0, and hence the assertion is proven in this one step for the Integer domain.

However, if the domain for variable X is the real numbers (or float), then X > -1 is *not* logically equivalent to X ≥ 0 (e.g., -0.5 > -1 is true, but –0.5 ≥ 0 is not). But for the real number domain, we do have that |— X ≥ 0   X > -1. Therefore, we must use another proof step of strengthening the pre-condition in the first step to generate a valid proof for this domain.