Example Axiomatic Proof

The Fibonacci numbers are a sequence of integers defined recursively by

fib(1) = fib(2) = 1, and

fib(N) = fib(N-1)+fib(N-2), for N>2.

When defined in this usual way, the naturally corresponding recursive program is clearly correct but highly inefficient. We prove that the following iterative program fragment is correct — it's totally correct, but we only exhibit the partial correctness proof.

```
     { N≥1 }
NEW:= 1;  OLD:= 1;  I:= 2;
   { ℙ }
   while I<N do
   begin  I:= I+1;  NEW:= NEW+OLD;
   OLD:= NEW-OLD  end
     { NEW = fib(N) }
```

Proof:

<u>Step 1</u>: discover the loop invariant $\mathbb{P}$

Take $\mathbb{P} \equiv (2 \le I \le N \wedge NEW=fib(I) \wedge OLD=fib(I-1)) \vee (I=2 \wedge N=1 \wedge NEW=1)$

<u>Step 2:</u> Show $\vdash$ **{** N≥1 **}** NEW:=1; OLD:=1; I:=2 **{** $\mathbb{P}$ **}**

Try these details as an exercise - just uses Assign and SEQ.

<u>Step 3</u>: Show $\vdash$ **{** $\mathbb{P}$ **} while** .... **{** NEW=fib(N) **}**

This step is established through several intermediate steps.

<u>Step 3A</u>: Find $\mathbb{Q}_1$ and $\mathbb{Q}_2$ to show

$\vdash$ **{** $\mathbb{P} \wedge$ I<N **}**

begin I:=I+1;

{ $\mathbb{Q}_1$ **}** NEW:= NEW+OLD;

{ $\mathbb{Q}_2$ **}** OLD:= NEW-OLD

end

{ $\mathbb{P}$ **}**

<u>Step 3Ai</u>: formulate $\mathbb{Q}_1$

Take $\mathbb{Q}_1 \equiv 3 \le I \le N \wedge NEW=fib(I-1) \wedge OLD=fib(I-2)$

<u>Step 3Aii:</u> Show $\vdash$ **{** $\mathbb{P} \wedge I< N$ **}** I:= I+1 **{** $\mathbb{Q}_1$**}**

It can be seen that $(\mathbb{P} \wedge I<N) \Rightarrow \mathbb{Q}_1[I \to I+1]$ so by Assign axiom and rule for and Strengthening pre-conditions, step 3Aii holds.

<u>Step 3Aiii</u>: formulate $\mathbb{Q}_2$

Take $\mathbb{Q}_2 \equiv 3 \le I \le N \wedge NEW=fib(I) \wedge OLD=fib(I-2)$

<u>Step 3Aiv:</u> show $\vdash$ **{** $\mathbb{Q}_1$ **}** NEW:= NEW+OLD **{** $\mathbb{Q}_2$ **}**

Try this - direct application of Assign axiom.

<u>Step 3Av:</u> show $\vdash$ **{** $\mathbb{Q}_2$ **}** OLD:= NEW-OLD **{** $\mathbb{P}$ **}**

One can see that $\mathbb{Q}_2 \Rightarrow \mathbb{P}[OLD \to NEW-OLD]$ so that by Assign axiom and rule for Strengthening pre-conditions, this step is proven

<u>Step 3Avi:</u> by steps 3Aii, 3Aiv, and 3Av and the rule for sequential execution (applied twice), the proof of step 3A is complete.

<u>Step 3B</u>: by step 3A and the rule for while loops we have $\vdash$ **{** $\mathbb{P}$ **} while** I<N **do begin ... end {** $\mathbb{P} \wedge I \ge N$ **}**. Now, $\mathbb{P} \wedge I \ge N$ implies either

$I=2 \wedge N=1 \wedge NEW=1$, and hence $NEW=fib(N)$

or

$2 \le I=N \wedge NEW=fib(I) \wedge OLD=fib(I-1)$, and hence $NEW=fib(N)$

<u>Step 4</u>: By steps 2 and 3 and the post-condition Weakening rule , the program is proven.