Invariance Proof of Algorithm *Euclid*

THEOREM *PartialCorrectness* is an invariant of algorithm *Euclid*.

1. $Init \Rightarrow Inv$

   PROOF: By the definitions of *Init* and *Inv*, since *Init* implies $x = M$, $y = N$, and $pc \neq$ "Done".

2. $Inv \wedge Next \Rightarrow Inv'$

   2.1. CASE: $x = y$

   PROOF: In this case, *Next* implies $x = x'$ and $y = y'$, which imply $x' = y'$. We then deduce $x' = GCD(M, N)$ from *Inv* and *GCD*1, proving Inv'.

   2.2. CASE: $x < y$

   PROOF: In this case, *Next* implies $x' = x$, and $y' = y - x$, which by the case assumption imply $GCD(x', y') = GCD(x, y - x)$. This, *Inv*, and *GCD*3 imply $GCD(x', y') = GCD(x, y)$, and *Next* implies $pc' =$ "Lbl_1", so $pc' \neq$ "Done". Hence, Inv' is true.

   2.3. CASE: $x > y$

   PROOF: This proof is similar to the proof of step 2.2, except that both *GCD*2 and *GCD*3 are needed to prove $GCD(x', y') = GCD(x, y)$.

   2.4. Q.E.D.

   PROOF: By 2.1, 2.2, and 2.3, since the three cases cover all possibilities.

3. $Inv \Rightarrow PartialCorrectness$

   PROOF: It suffices to assume *Inv* and $pc =$ "Done" and prove $x = y$ and $x = GCD(M, N)$. The proof of $x = y$ is trivial, and $x = GCD(M, N)$ follows from $x = y$, the first conjunct of *Inv*, and *GCD*1.

4. Q.E.D.

   PROOF: By 1, 2, and 3 (which are conditions I1, I2, and I3).

CLOSE