Computer Science 81, Spring 2009
Assignment 8
Due Mon. April 6

1. [50 points] Prove the total correctness of the following program in the "Japeish" language, presented here as a Hoare triple. **All variables are integers**.

{n = n0 ∧ n0 ≥ 0 ∧ b > 0}

```
(s := b; r := 1)
while n > 0
      do
      if mod(n, 2) = 1
            then r := r × s
            else skip
      fi;
      n := n ÷ 2;
      s := s × s
      od
```

{r = pow(b, n0)}

Here *pow* is the power function, that is pow(b, n0) = b^{n0}, while *mod* is the modulus or remainder function, that is, mod(n, d) is the remainder of dividing n by d.

The first task is to figure out for yourself how this program works.

Next devise an appropriate invariant and verify it informally.

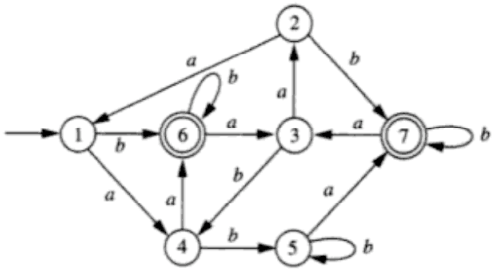
Finally, using that invariant, enter the program with the invariant embedded into JAPE as a conjecture and use JAPE to edit the proof. Any facts that you use that are not built into JAPE's Hoare logic should be expressed either using the Obviously rule or as Lemmas (the proofs of which can use the Obviously rule). For each use of the Obviously rule, you should give an argument to say why it is true.

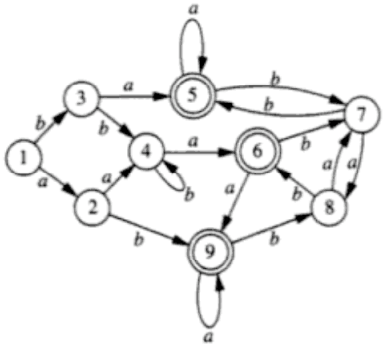
Below is the incantation that should be entered into JAPE as a conjecture, except you will have to insert your invariant, replace the various symbols with the ones from JAPE's symbol repertoire and this will all be on one line:

```
WHERE DISTINCT b, n, n0, pow, r, s IS
{n=n0 ∧ n0 ≥ 0 ∧ b>0} (s:=b; r:=1)
{… your invariant here …}
while n > 0 do if mod(n,2)=1 then r:=r×s else skip fi; n:=n÷2; s := s×s od
{r = pow(b, n0)}
```

Note that you would start the proof using JAPE's Ntuple rule.

2. [10 points] Using the algorithm discussed in the lecture, compute the state equivalence classes for the following DFAs.





3. [10 points] Construct the minimal equivalent DFAs for the above.

4. [30 points] Give the Myhill-Nerode equivalence classes for the following languages, together with state diagrams suggestive of the transitions between classes.

   - $L = \{x \in \{0, 1\}^* \mid |\#_1(x) - \#_0(x)| \leq 1\}$ (Here $|n|$ is the absolute value of n.)
   - $N = \{ x \in \{0, 1\}^* \mid$ for every prefix $y \leq x$ $|\#_1(y) - \#_0(y)| \leq 1 \}$
   - $P = \{ x \in \{1\}^* \mid \#_1(x)$ is a prime number $\}$
   - $Q = \{ x \in \{1\}^* \mid \#_1(x)$ is an even prime number $\}$