COMPUTER SCIENCE 20, SPRING 2012
DISCRETE MATHEMATICS FOR COMPUTER SCIENCE

Class #15 (States and Invariants)

Homework, due in hard copy Monday 3/5/2012 at 10:10am

Please write your TF's name on your homework, and list the names of any students with whom you collaborated.

1. Multiplying and dividing an integer n by 2 only requires a one digit left or right shift of the binary representation of n, which are hardware-supported fast operations on most computers. Here is a state machine, R, that computes the product of two nonnegative integers x and y using just these shift operations, along with integer addition:*

$$\text{states} ::= \mathbb{N}^3$$

(triples of nonnegative integers)

$$\text{start state} ::= (x, y, 0)$$

$$\text{transitions} ::= (r, s, a) \to \begin{cases} (2r, s/2, a) & \text{for even } s > 0, \\ (2r, (s-1)/2, a+r) & \text{for odd } s > 0. \end{cases}$$

   (a) Verify that $P((r, s, a)) ::= [rs + a = xy]$ is a preserved invariant of R.

   (b) Prove that R is partially correct: if R reaches a final state—a state from which no transition is possible—then $a = xy$.

*Credit: Adapted from Albert R. Meyer / MIT 6.042