State Machines

State machines step by step processes (may step in response to input —not today)

Die Hard

Image removed due to copyright restrictions.
Simon says: On the fountain, there should be 2 jugs, do you see them? A 5-gallon and a 3-gallon. Fill one of the jugs with exactly 4 gallons of water and place it on the scale and the timer will stop. You must be precise; one ounce more or less will result in detonation. If you’re still alive in 5 minutes, we’ll speak.

Transferring water:

3 Gallon Jug 5 Gallon Jug

Supplies:

Water

3 Gallon Jug

5 Gallon Jug

Image by MIT OpenCourseWare.
Die hard state machine

State:
amount of water in jugs: \((b, l)\)
\[0 \leq b \leq 5, \quad 0 \leq l \leq 3\]
Start State: \((0,0)\)

Die Hard Transitions:
1. Fill little jug: \((b, l) \rightarrow (b, 3)\) for \(l < 3\)
2. Fill big jug: \((b, l) \rightarrow (5, l)\) for \(b < 5\)
3. Empty little jug: \((b, l) \rightarrow (b, 0)\) for \(l > 0\)
4. Empty big jug: \((b, l) \rightarrow (0, l)\) for \(b > 0\)

5. Pour big jug into little jug
   (i) If no overflow, then \((b, l) \rightarrow (0, b+l)\)
       \[b+l \leq 3\]
   (ii) otherwise \((b, l) \rightarrow (b-(3-l), 3)\)
6. Pour little jug into big jug.
   Likewise

Simon’s challenge:
Disarm the bomb by putting precisely 4 gallons of water on the scale, or it will blow up.
(You can figure out how)
Die Hard

Work it out now!

How to do it

Start with empty jugs: (0,0)
Fill the big jug: (5,0)

Pour from big to little: (2,3)

Empty the little: (2,0)
How to do it

Pour from big to little: (0,2)

---

How to do it

Fill the big jug: (5,2)

---

How to do it

Pour from big to little: (4,3)

---

Die Hard once and for all

What if have a 9 gallon jug instead?

---

Can you do it? Can you prove it?
Preserved Invariants

Die hard once and for all preserved invariant:

\[ P(\text{state}) ::= \text{“3 divides the number of gallons in each jug.”} \]

\[ P((b,l)) ::= (3 \mid b \text{ AND } 3 \mid l) \]

---

Preserved Invariants

Die hard once and for all preserved invariant:

\[ (b,l) \rightarrow (b-(3-l),3) \]

\[ P((b,l)) ::= (3 \mid b \text{ AND } 3 \mid l) \]

---

Die Hard Once & For All

Corollary: No state \((4,x)\) is reachable, so Bruce Dies!

---

Floyd's Invariant Principle

(induction for state machines)

Preserved Invariant, \(P(\text{state})\):

if \(P(q)\) and \(q \rightarrow r\), then \(P(r)\)

Conclusion: if \(P(\text{start})\), then \(P(r)\)
for all reachable states \(r\), including final state (if any)
The Diagonal Robot

the robot is on a grid

0          1            2        3

2
1
0

x

The Diagonal Robot

it can move diagonally

0          1            2        3

2
1
0

x

The Diagonal Robot

can it get from (0,0) to (1,0)?

Robot Preserved Invariant

NO! preserved invariant:

\[ P((x, y)) ::= x + y \text{ is even} \]

move adds ±1 to both \( x \) & \( y \), preserving parity of \( x+y \).
Also, \( P((0, 0)) \) is true.
Robot Preserved Invariant
So in all positions \((x,y)\)
reachable from \((0,0)\),
\(x+y\) stays even
But \(1+0=1\) is odd, so
\((1,0)\) is not reachable

The Fifteen Puzzle Explained!
--by similar reasoning
details in problem 2

Fast Exponentiation
compute \(a^b\) using registers \(X,Y,Z,R\)
\[X := a; \quad Y := 1; \quad Z := b;\]
\text{REPEAT:}
if \(Z=0\), then return \(Y\)
\[R := \text{remdr}(Z,2); \quad Z := \text{quotnt}(Z,2);\]
if \(R=1\), then \(Y := X \cdot Y\)
\[X := X^2\]

Fast Exponentiation
State Machine:
States ::= \(\mathbb{R} \times \mathbb{R} \times \mathbb{N}\)
start ::= \((a,1,b)\)
transitions ::= \((X,Y,Z) \rightarrow (X^2, Y, \text{quotnt}(Z,2))\) if \(Z>0\) is even
\((X^2, X \cdot Y, \text{quotnt}(Z,2))\) if \(Z>0\) is odd
Fast Exponentiation

Preserved Invariant: \( Y^X^Z = a^b \)
\[(X,Y,Z) \rightarrow [Z>0 \text{ is odd}]\]
\[(X^2, X \cdot Y, (Z-1)/2)\]
\[(X \cdot Y) (X^2)^{(Z-1)/2} = (X \cdot Y) X^{Z-1} = Y X^Z = a^b\]

Partial Correctness

Preserved invariant: \( Y^X^Z = a^b \)
at start \( 1 \cdot a^b = a^b \) OK
at end \( Z=0 \), so return \( Y = Y X^0 = a^b \) OK

Fast Termination

at each transition
\[ Z := \text{quotient}(Z,2) \]
\( Z = b \) at start, so \( Z = 0 \) in \( \leq \log_2(b) \) transitions

Robert W Floyd (1934–2001)

Photograph removed due to copyright restrictions.