Mathematics for Computer Science

MIT 6.042J/18.062J

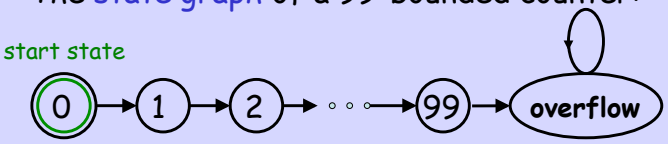
State Machines

State machines

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

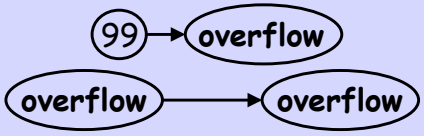
State machines

The state graph of a 99-bounded counter:



States: {0,1,…,99, **overflow**}

Transitions: $i \to i+1$ $0 \leq i < 99$



Die Hard

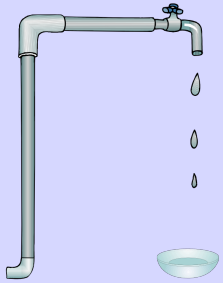
Picture source: http://movieweb.com/movie/diehard3/

Die Hard

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.

Die Hard

Supplies:



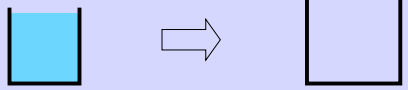
Water

3 Gallon Jug

5 Gallon Jug

Die Hard

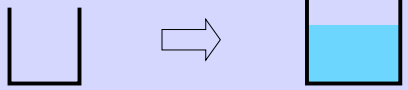
Transferring water:



3 Gallon Jug 5 Gallon Jug

Die Hard

Transferring water:



3 Gallon Jug 5 Gallon Jug

Die hard state machine

State:

amount of water in jugs: (b,l)

$0 \leq b \leq 5, 0 \leq l \leq 3$

Start State: (0,0)

State machines

Die Hard Transitions:

1. Fill little jug: (b, l) → (b, 3) for $l < 3$
2. Fill big jug: (b, l) → (5, l) for $b < 5$
3. Empty little jug: (b, l) → (b, 0) for $l > 0$
4. Empty big jug: (b, l) → (0, l) for $b > 0$

State machines

5. Pour big jug into little jug

(i) If no overflow, then (b,l)→(0,b+l)

$b+l \leq 3$

(ii) otherwise (b,l) →(b−(3−l),3)

6. Pour little jug into big jug.

Likewise

Die Hard

Simon's challenge:

Disarm the bomb by putting precisely 4 gallons of water on the scale, or it will blow up.

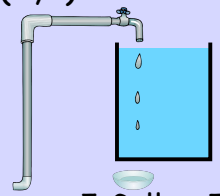
(You can figure out how)

Die Hard

Work it out now!

How to do it

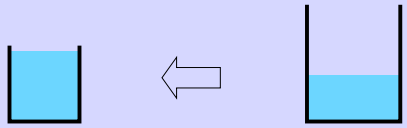
Start with empty jugs: (0,0)
Fill the big jug: (5,0)



3 Gallon Jug 5 Gallon Jug

How to do it

Pour from big to little: (2,3)



3 Gallon Jug 5 Gallon Jug

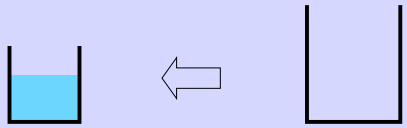
How to do it

Empty the little: (2,0)

3 Gallon Jug 5 Gallon Jug

How to do it

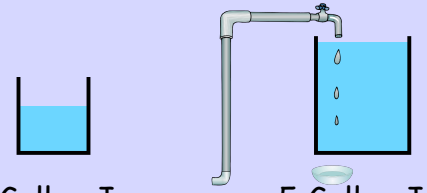
Pour from big to little: (0,2)



3 Gallon Jug 5 Gallon Jug

How to do it

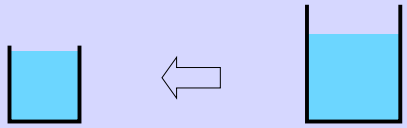
Fill the big jug: (5,2)



3 Gallon Jug 5 Gallon Jug

How to do it

Pour from big to little: (4,3)

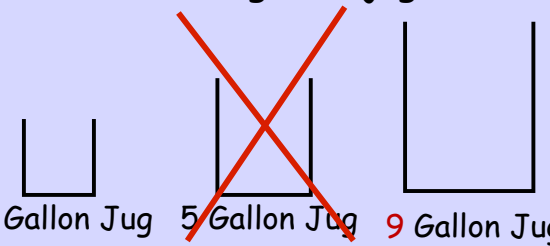


3 Gallon Jug 5 Gallon Jug

Done!

Die Hard once and for all

What if have a 9 gallon jug instead?



3 Gallon Jug 5 Gallon Jug 9 Gallon Jug

Can you do it? Can you prove it?

Preserved Invariants

Die hard once and for all

preserved invariant:

P(state) ::= "3 divides the number of gallons in each jug."

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

Preserved Invariants

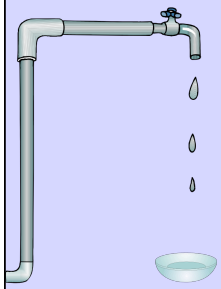
Die hard once and for all

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

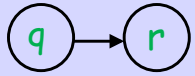


Corollary: No state (4,x) is reachable, so Bruce Dies!

Floyd's Invariant Principle

(induction for state machines)

Preserved Invariant, P(state):

if P(q) and 

, then P(r)

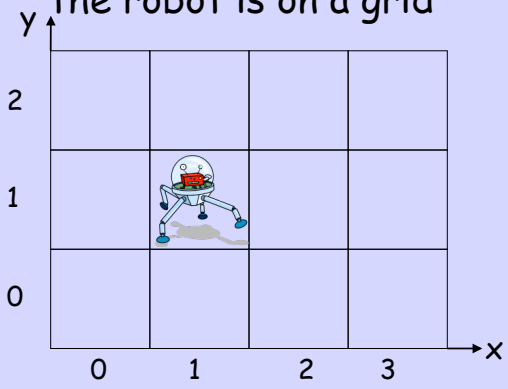
Conclusion: if P(start), then P(r)

for all reachable states r,

including final state (if any)

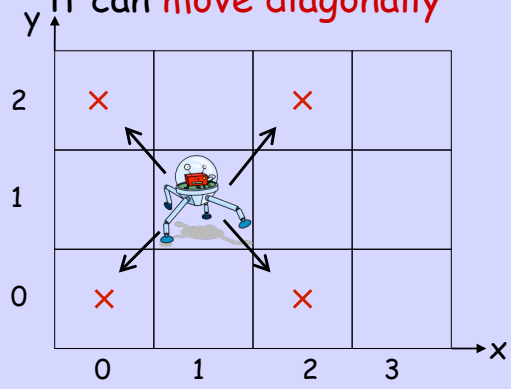
The Diagonal Robot

the robot is on a grid



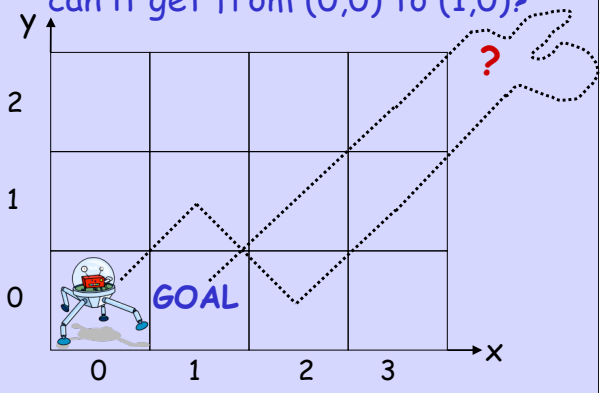
The Diagonal Robot

it can move diagonally



The Diagonal Robot

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



Robot Preserved Invariant

NO! preserved invariant:

P((x, y)) ::= x + y 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;  Y:= 1;  Z:= b;
REPEAT:
if Z=0, then return Y
R:= remdr(Z,2); Z:= quotnt(Z,2)
if R=1,then Y:= X·Y
X:= X²
```


Fast Exponentiation

State Machine:

States ::= $\mathbb{R} \times \mathbb{R} \times \mathbb{N}$

start ::= (a,1,b)

transitions ::= (X,Y,Z) →

(X^2, Y , quotnt(Z,2)) if Z>0 is even

(X^2, X·Y, quotnt(Z,2)) if Z>0 is odd

Fast Exponentiation

Preserved Invariant: $YX^Z = a^b$

$(X,Y,Z) \rightarrow$ [Z>0 is odd]
$(X^2, X \cdot Y, (Z-1)/2)$

$(X \cdot Y)(X^2)^{(Z-1)/2} = (X \cdot Y)X^{Z-1}$
$= YX^Z = a^b$

Partial Correctness

preserved invariant: $YX^Z = a^b$
at start $1 \cdot a^b = a^b$

at end Z=0, so return
$Y = YX^0 = a^b$

Fast Termination

at each transition
Z:= quotient(Z,2)
Z= b at start, so Z= 0
in $\leq \log_2(b)$ transitions

Robert W Floyd (1934–2001)

Eulogy by Knuth: http://www.acm.org/pubs/membernet/stories/floyd.pdf
Picture source: http://www.stanford.edu/dept/news/report/news/november7/floydobit-117.html