Mathematics for Computer Science

MIT 6.042J/18.062J

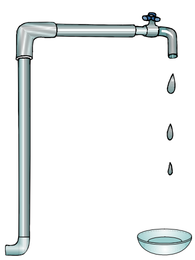
Computational Processes

Die Hard

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

Die Hard

Supplies:



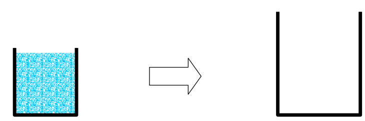
Water

3 Gallon Jug

5 Gallon Jug

Die Hard

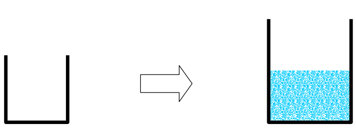
Transferring water:



3 Gallon Jug 5 Gallon Jug

Die Hard

Transferring water:



3 Gallon Jug 5 Gallon Jug

Die Hard

Psychopath's challenge:
Disarm bomb by putting 4 gallons of water on scale, or it will blow up.

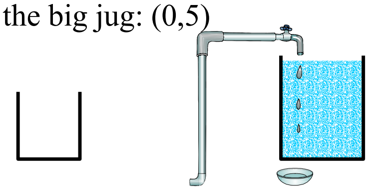
Question: How to do it?

Die Hard

Work it out now!

How to do it

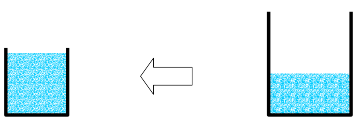
Start with empty jugs: (0,0)
Fill the big jug: (0,5)



3 Gallon Jug 5 Gallon Jug

How to do it

Pour from big to little: (3,2)



3 Gallon Jug 5 Gallon Jug

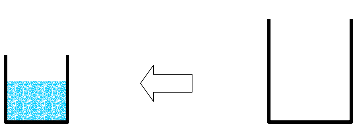
How to do it

Empty the little: (0,2)

3 Gallon Jug 5 Gallon Jug

How to do it

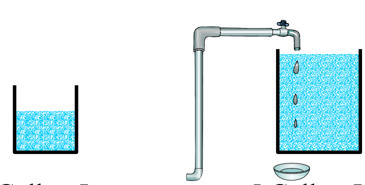
Pour from big to little: (2,0)



3 Gallon Jug 5 Gallon Jug

How to do it

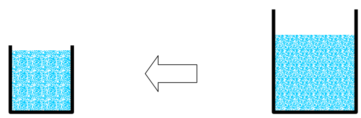
Fill the big jug: (2,5)



3 Gallon Jug 5 Gallon Jug

How to do it

Pour from big to little: (3,4)



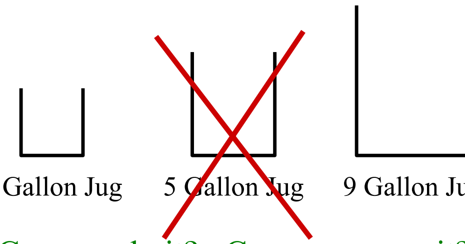
3 Gallon Jug 5 Gallon Jug

Done!!

 September 30, 2002

Die Hard once and for all

What if you have a 9 gallon jug instead?



3 Gallon Jug 5 Gallon Jug 9 Gallon Jug

Can you do it? Can you prove it?

 September 30, 2002

Die Hard

Work it out now!

 September 30, 2002

State machines

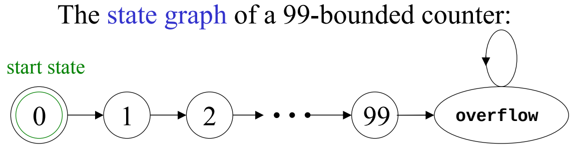
State machine:

Step by step procedure, possibly responding to input.

 September 30, 2002

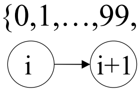
State machines

The state graph of a 99-bounded counter:

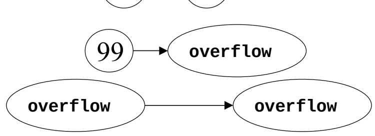


States: {0,1,…,99, `overflow`}

Transitions:



$0 \le i < 99$



 September 30, 2002

State machines

Die hard state machine

State = amount of water in the jug:

(b,l) where $0 \le b \le 5$ and $0 \le l \le 3$.

Start State = (0,0)

 September 30, 2002

State machines

Die Hard Transitions:

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

 September 30, 2002

State machines

5. Pour from big jug into little jug (for $b > 0$):
   (i) If no overflow, then $(b,l) \to (0\,,\ b+l)$,
   $b + l <= 3$
   (ii) otherwise $(b,l) \to (b-(3-l),\ 3)$.

6. Pour from little jug into big jug.
   Likewise.

 September 30, 2002

State Invariants

Die hard once and for all

Invariant:

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

$$P((b,l)) ::= (3 \mid b \wedge 3 \mid l)$$

 September 30, 2002

State Invariants

Floyd's Invariant Method

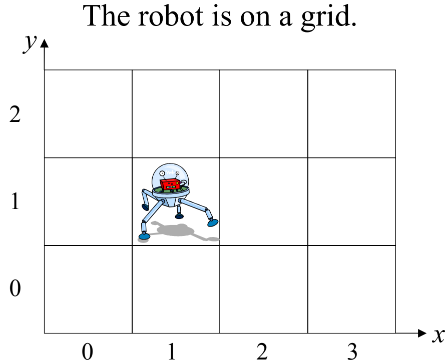
(just like induction)

1) Base case: Show $P(start)$.
2) Invariant case: Show
   if $P(q)$ and $q \longrightarrow r$, then $P(r)$.
3) Conclusion: P holds for *all reachable states*, including final state (if any).

 September 30, 2002

The Robot

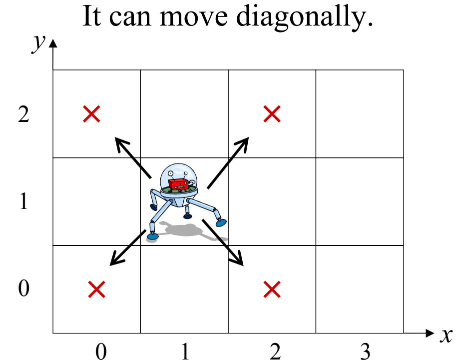
The robot is on a grid.



 September 30, 2002

The Robot

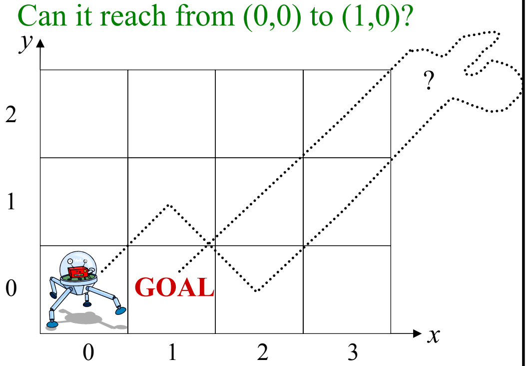
It can move diagonally.



 September 30, 2002

The Robot

Can it reach from (0,0) to (1,0)?



Robot Invariant

NO!

$P((x, y))$ ::= $x + y$ is even
$P((0, 0))$ is true.

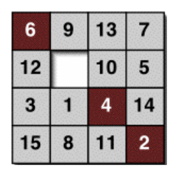
Transition adds ±1 to **both** x and y

Robot Invariant

So all positions (x, y) reachable by robot have $x + y$ even,
but $1 + 0 = 1$ is odd.

Therefore (1,0) is not reachable.

Class Problem 1



The Fifteen Puzzle Explained!

GCD correctness

The Euclidean Algorithm:

Computing GCD(a, b)

1. Set $x := a$, $y := b$.
2. If $y = 0$, return x & terminate;
3. else set $(x, y) := (y, \text{rem}(x,y))$ *simultaneously*;
4. Go to step 2.

GCD correctness

Example: GCD(414,662)

= GCD(662, 414)	since rem(414,662) = 414
= GCD(414, 248)	since rem(662,414) = 248
= GCD(248, 166)	since rem(414,248) = 166
= GCD(166, 82)	since rem(248,166) = 82
= GCD(82, 2)	since rem(166,82) = 2
= GCD(2, 0)	since rem(82,2) = 0

Return value: 2.

GCD correctness

Euclid Algorithm as State Machine:

- States ::= □ □ □ ,
- start ::= (a,b),
- state transitions defined by the rule

$(x,y) \rightarrow (y, \text{rem}(x,y))$ for $y \neq 0$.

GCD correctness

The Invariant is
$P((x,y)) ::= [\text{gcd}(a,b) = \text{gcd}(x,y)]$.

$P(start)$: at start $x = a$, $y = b$, so
$P(start) \equiv [\text{gcd}(a,b) = \text{gcd}(a,b)]$
which holds trivially.

GCD correctness

Transitions: $(x, y) \rightarrow (y, \text{rem}(x, y))$

Invariant holds by
Lemma: $\text{gcd}(x, y) = \text{gcd}(y, \text{rem}(x,y))$,
for $y \neq 0$.

GCD correctness

Conclusion: on termination
$x = \text{gcd}(a,b)$.

Proof: On termination, $y = 0$, so

$$x = \text{gcd}(x, 0) = \underbrace{\text{gcd}(x, y) = \text{gcd}(a,b)}_{\text{invariant}}$$

Class Problem 2

Robert Floyd (1934--2001)

Picture source: http://www.stanford.edu/dept/news/report/news/november7/floydobit-117.html

