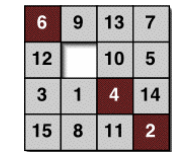


The Fifteen Puzzle Explained!

Wednesday, Team Problem 1

 March 2, 2007 lec 4F.1

Mathematics for Computer Science

MIT 6.042J/18.062J

State Machine Invariants, cont'd

 March 2, 2007 lec 4F.2

GCD correctness

The Euclidean Algorithm:

Computing GCD(a, b)

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

 March 2, 2007 lec 4F.3

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.

 March 2, 2007 lec 4F.4

GCD correctness

Euclid Algorithm as State Machine:

- States ::= $\mathbb{N}\times\mathbb{N}$,
- start ::= (a,b),
- state transitions defined by the rule

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

 March 2, 2007 lec 4F.5

GCD correctness

The Invariant is

$P((x,y))$ ::= $[\gcd(a,b) = \gcd(x,y)]$.

$P(start)$: at start $x = a$, $y = b$, so

$P(start) \equiv [\gcd(a,b) = \gcd(a,b)]$

which holds trivially.

 March 2, 2007 lec 4F.6

GCD correctness

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

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

Proof: $x = qy + \text{rem}$, so
any divisor of x, y divides rem;
any divisor of y,rem divides x

GCD correctness

Conclusion: on termination

$x = \gcd(a,b)$.

Proof: at termination, $y = 0$, so
$x = \gcd(x, 0) = \underbrace{\gcd(x, y) = \gcd(a,b)}_{\text{the invariant}}$

GCD Termination

y decreases at each step &
$y \in \mathbb{N}$ (another invariant).

Well Ordering implies
reaches minimum & stops.

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

Mathematics for Computer Science

MIT 6.042J/18.062J

State Machines: Derived Variables

Derived Variables

A *derived variable*, v, is a function giving a "value" to each state:

v: $Q \to$ Values.

If Values = $\mathbb{N}$, we'd say v was

"nonnegative-integer-valued," or
"$\mathbb{N}$-valued."

Derived Variables

Robot on the grid example:

States $Q = \mathbb{N}^2$.

Define the sum-value, σ, of a state:

$$\sigma(\langle x,y\rangle) ::= x+y$$

An $\mathbb{N}$-valued derived variable.

Derived Variables

Called "derived" to distinguish from *actual* variables that appear in a program.

For robot Actual: x, y

Derived: σ

Derived Variables

Another derived variable:

$$\pi ::= \sigma \pmod 2.$$

π is $\{0,1\}$-valued.

Derived Variables

For GCD, have (actual) variables x, y.

Proof of GCD termination:

y is strictly decreasing and natural number-valued.

Derived Variables

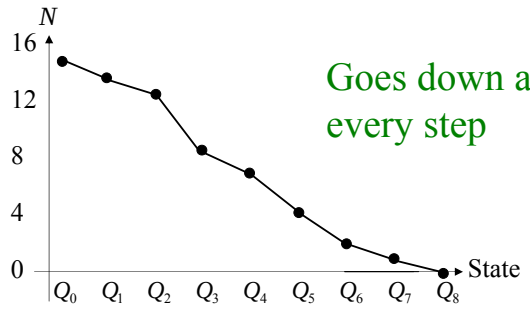
Termination followed by

Well Ordering Principle:

y must take a least value –

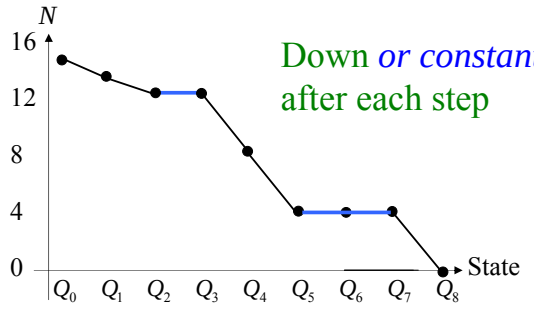
and then the algorithm is stuck.

Strictly Decreasing Variable



Goes down at every step

Weakly Decreasing Variable



Down *or constant* after each step

 March 2, 2007 lec 4F.19

σ, π for the *Diagonal Robot*

σ: up & down all over the place –
neither increasing nor decreasing.

π: is constant –
both increasing & decreasing
(weakly)

 March 2, 2007 lec 4F.20

Partial-order valued variables

Definitions of increasing/decreasing variables extend to variables with partially ordered values.
If a partial order has no infinite, decreasing chain (it is *well-founded*), then it can serve instead of $\mathbb{N}$ to

prove termination.

 March 2, 2007 lec 4F.23

Team Problems

Wednesday, Problem 2;
and today's

Problems 1& 2

 March 2, 2007 lec 4F.24