

Mathematics for Computer Science
MIT 6.042J/18.062J

State Machines: Derived Variables



Albert R Meyer, March 5, 2010

lec 5F.1

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Euclidean Algorithm

--for $GCD(a, b)$

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



Albert R Meyer, March 5, 2010

lec 5F.2

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

GCD correctness

Example: $GCD(662,414)$
 $= GCD(414, 248)$ since $\text{rem}(662,414) = 248$
 $= GCD(248, 166)$ since $\text{rem}(414,248) = 166$
 $= GCD(166, 82)$ since $\text{rem}(248,166) = 82$
 $= GCD(82, 2)$ since $\text{rem}(166,82) = 2$
 $= GCD(2, 0)$ since $\text{rem}(82,2) = 0$
 return value: 2



Albert R Meyer, March 5, 2010

lec 5F.3

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Euclid Algorithm State Machine

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

start $::= (a,b)$

state transitions defined by

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



Albert R Meyer, March 5, 2010

lec 5F.4

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

GCD correctness

preserved invariant $P(x,y)$:

$$[gcd(a,b) = gcd(x,y)]$$



Albert R Meyer, March 5, 2010

lec 5F.5

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

GCD correctness

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

P is preserved because:

$$gcd(x,y) = gcd(y, \text{rem}(x,y))$$

for $y \neq 0$


Proof: $x = qy + \text{rem}.$

any divisor of 2 of these 3 terms divides all 3.



Albert R Meyer, March 5, 2010


lec 5F.6



GCD correctness

P is true at start:
 $x = a, y = b$, so $P(\text{start}) \equiv$
 $[\text{gcd}(a,b) = \text{gcd}(a,b)]$


Albert R Meyer, March 5, 2010 lec 5F.7



GCD correctness

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

Albert R Meyer, March 5, 2010 lec 5F.8



GCD Termination

y decreases at each step
 $y \in \mathbb{N}$ (another invariant)
 Well Ordering implies
 reaches minimum & stops

Albert R Meyer, March 5, 2010 lec 5F.9

Derived Variables

A derived variable, v , is a function assigning a "value" to each state:
 $v: \text{States} \rightarrow \text{Values}$
 If $\text{Vals} = \mathbb{N}$, say v is " \mathbb{N} -valued"
 or "nonnegative-integer-valued"

Albert R Meyer, March 5, 2010 lec 5F.10

Derived Variables

Robot on the grid example:
 States = \mathbb{N}^2 . Define the
 sum-value, σ , of a state:
 $\sigma(x,y) ::= x+y$
 an \mathbb{N} -valued derived variable

Albert R Meyer, March 5, 2010 lec 5F.11

Derived Variables

Called *derived* to distinguish
 from *actual* variables that
 appear in a program.
 For robot **Actual:** x, y
Derived: σ

Albert R Meyer, March 5, 2010 lec 5F.12

Derived Variables

Another derived variable:

$$\pi ::= \sigma \pmod{2}$$

π is $\{0,1\}$ -valued



Albert R Meyer, March 5, 2010

lec 5F.13

Derived Variables

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

Proof of GCD termination:
 y is strictly decreasing & natural number-valued



Albert R Meyer, March 5, 2010

lec 5F.14

Derived Variables

Termination followed by

Well Ordering Principle:

y must take a least value.

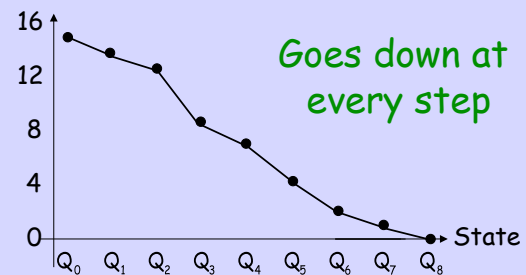
then the algorithm is stuck



Albert R Meyer, March 5, 2010

lec 5F.15

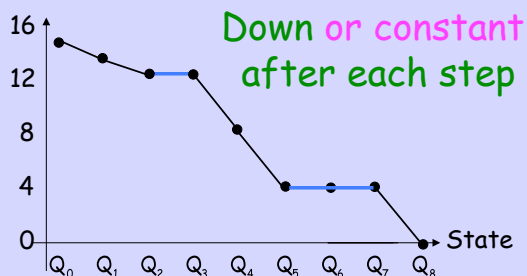
Strictly Decreasing Variable



Albert R Meyer, March 5, 2010

lec 5F.16

Weakly Decreasing Variable



Albert R Meyer, March 5, 2010

lec 5F.17

Diagonal Robot variables

σ : up & down all over the place

neither increasing
nor decreasing

π : is constant

both weakly increasing
& weakly decreasing



Albert R Meyer, March 5, 2010

lec 5F.18

Partial-order valued variables

Defs of increasing/decreasing variables extend to variables with **partially ordered** values.



Albert R Meyer, March 5, 2010

lec 5F.22

6	13	7
12	10	5
3	1	14
15	8	11

Team Problems

Problems 1-3



Albert R Meyer, March 5, 2010

lec 5F.25

MIT OpenCourseWare
<http://ocw.mit.edu>

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.