Week-1: Introduction to model checking

B. Srivathsan

Chennai Mathematical Institute

NPTEL-course

July - November 2015

Module 3:

Modeling data-dependent programs

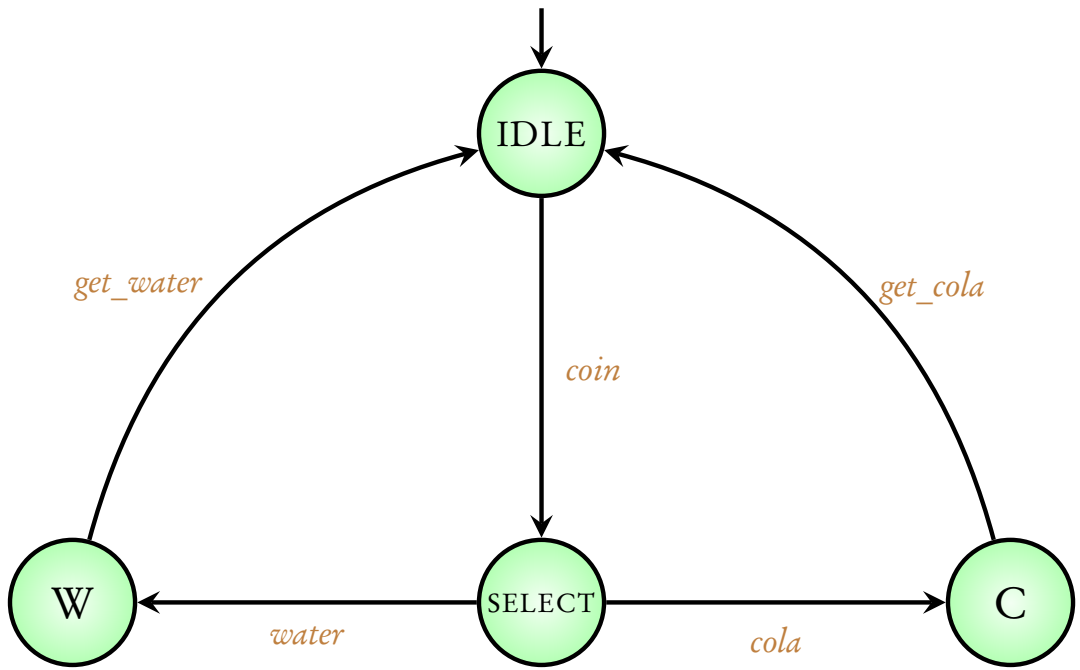
Data-dependent programs:

Variables + Conditional branching + Assignments

Data-dependent programs:

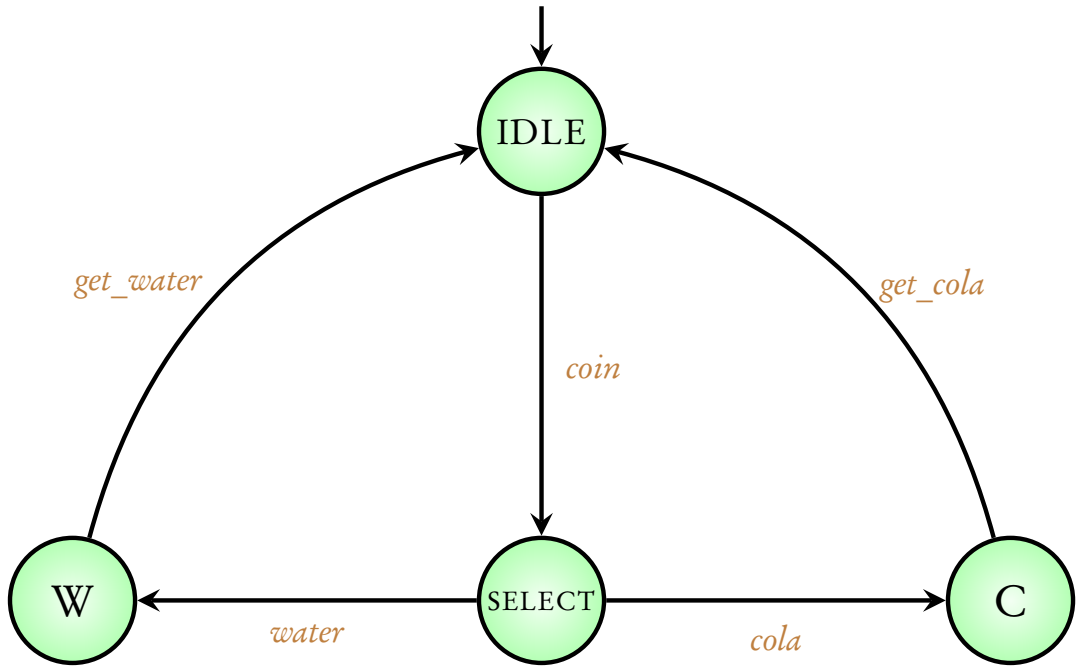
Variables + Conditional branching + Assignments

Coming next: vending machine revisited


IDLE
get_water
coin
get_cola
W
SELECT
C
water
cola

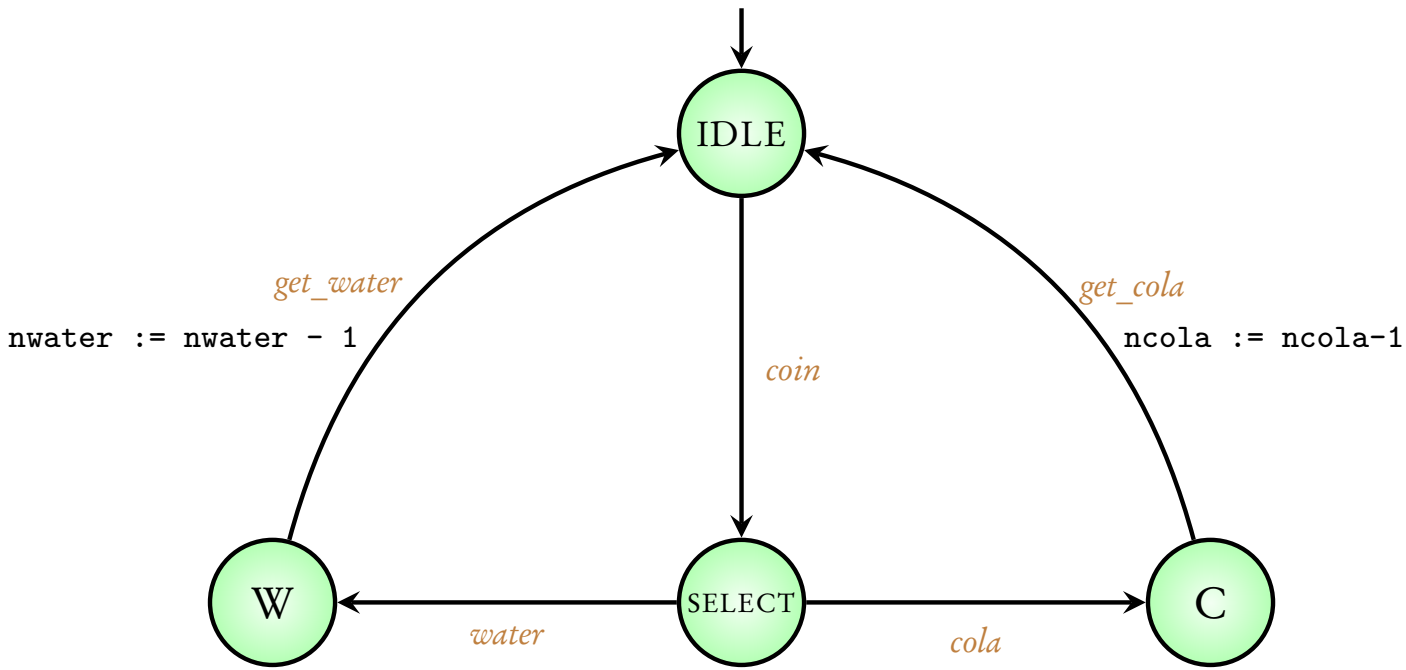
Variables:

`nwater, ncola, max`



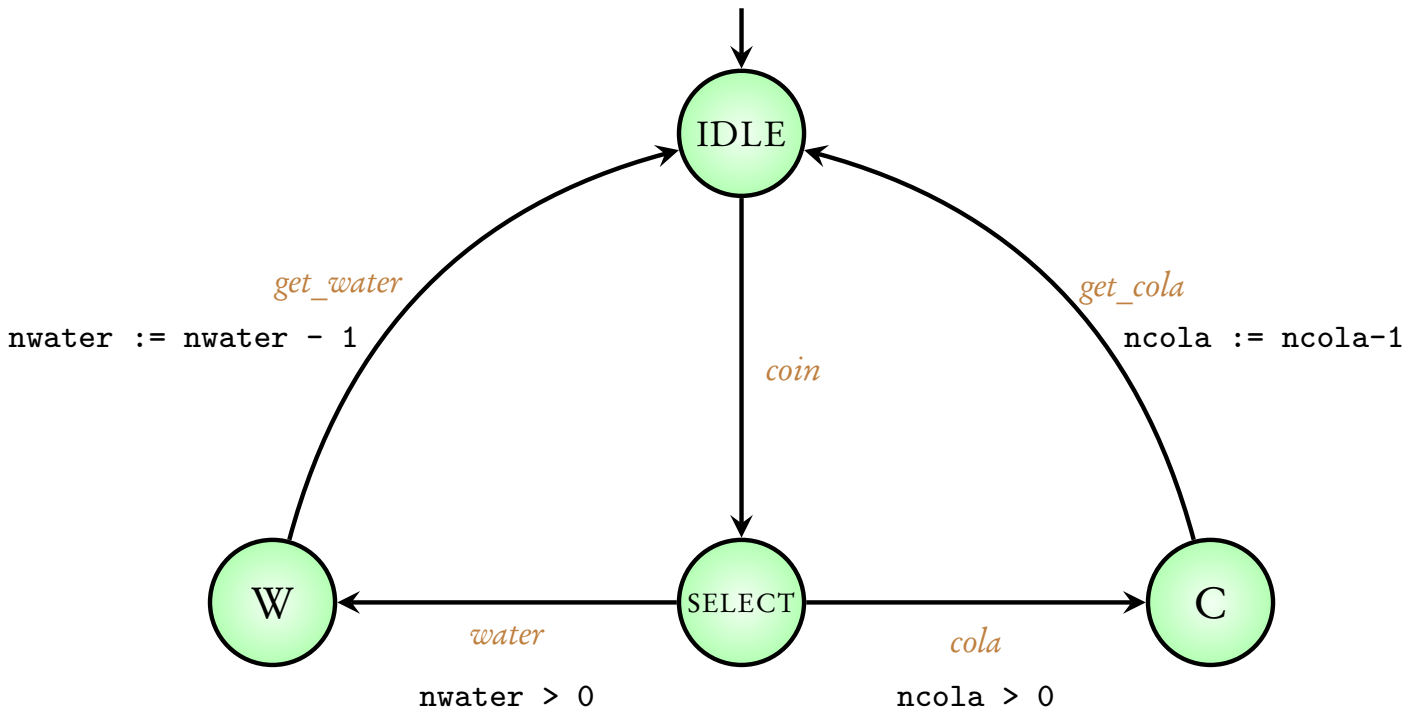
Variables:

`nwater, ncola, max`



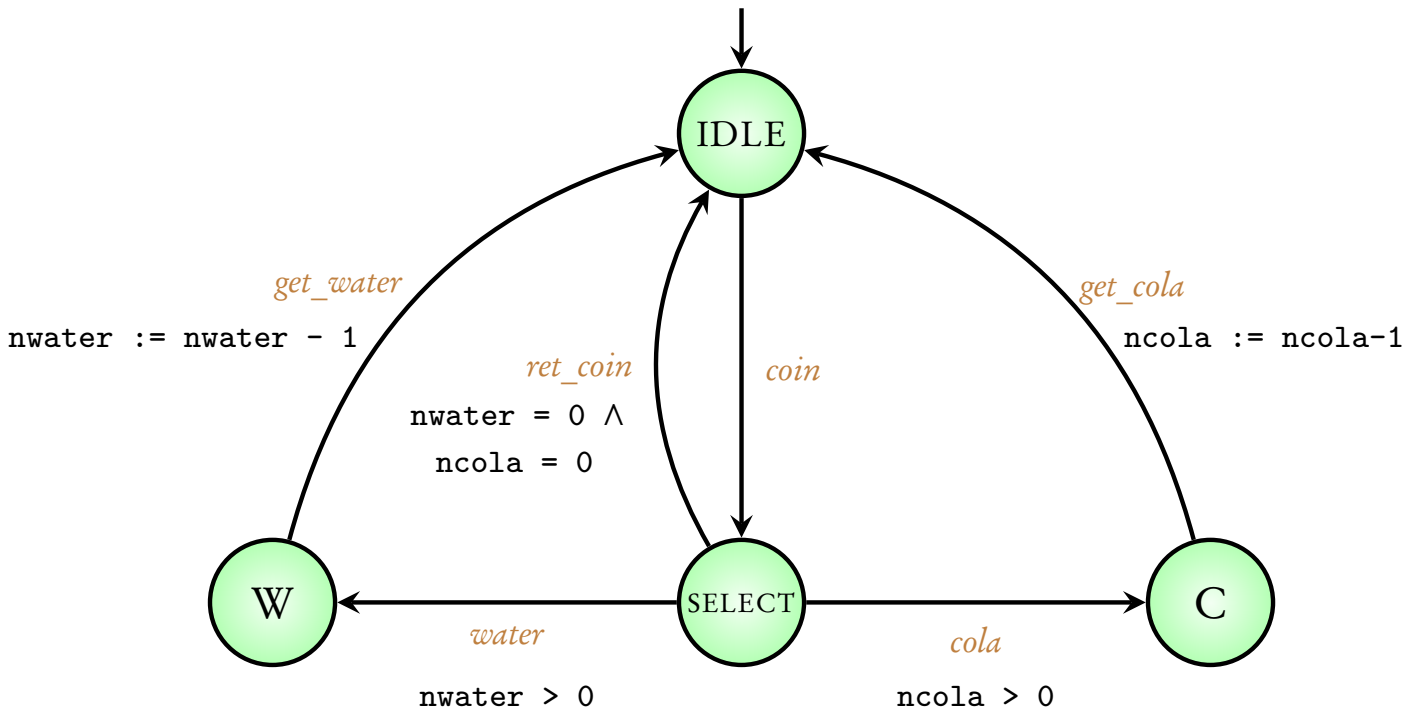
Variables:

`nwater, ncola, max`



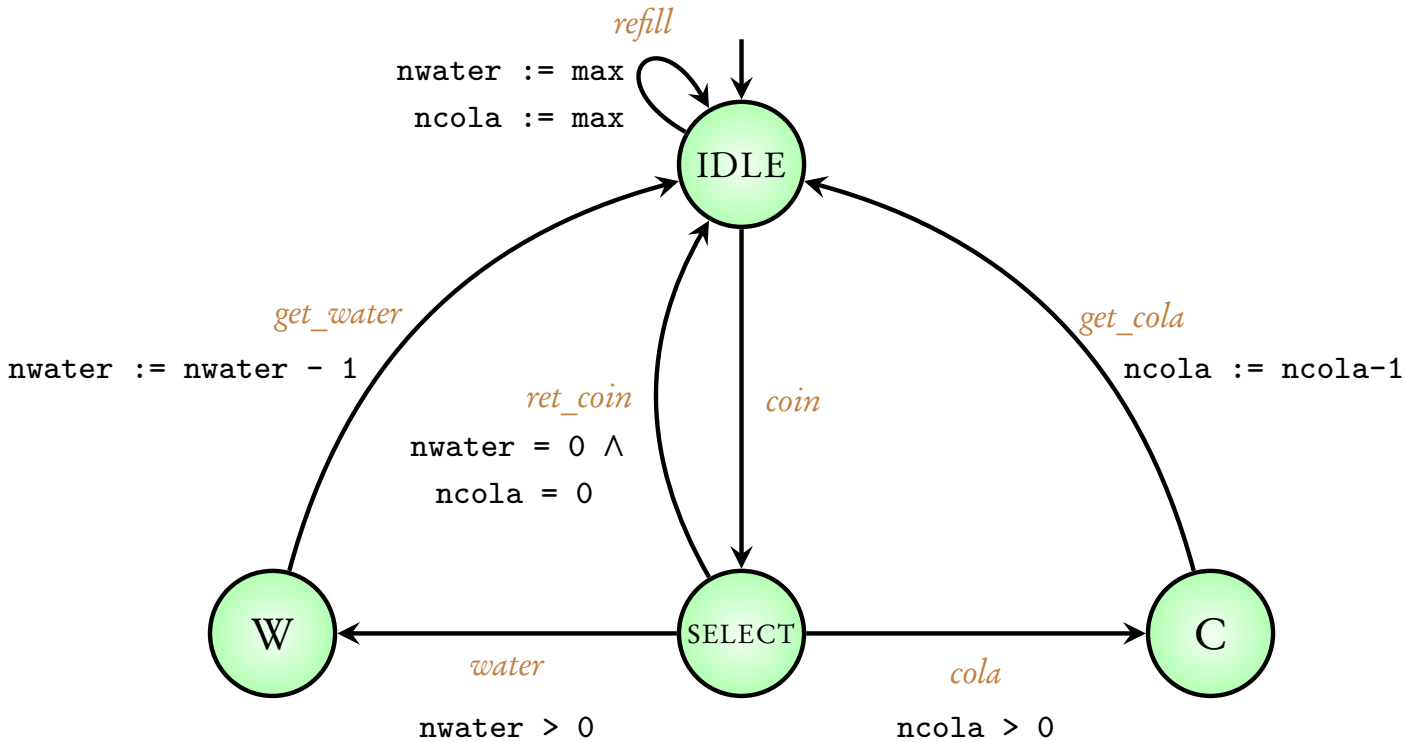
Variables:

`nwater, ncola, max`



Variables:

`nwater, ncola, max`

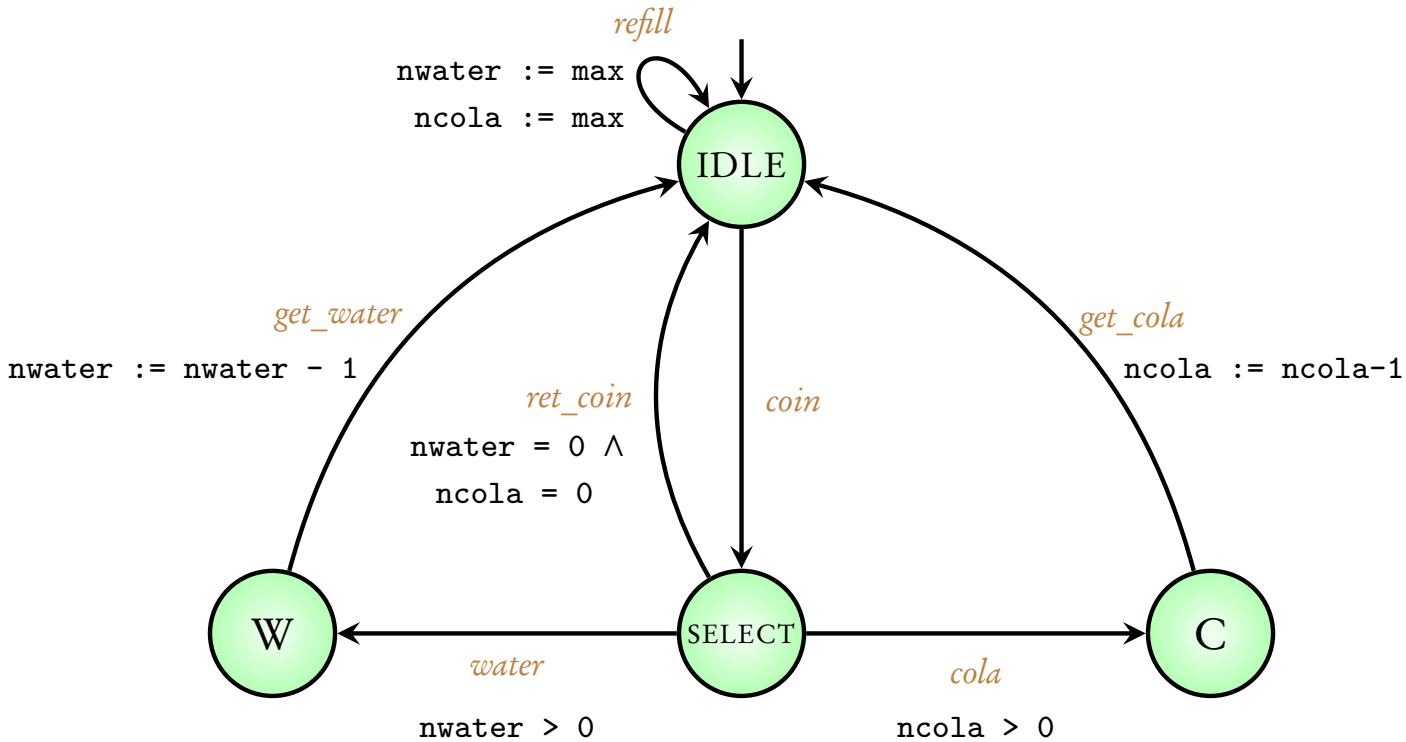


Initial condition:

`nwater = max, ncola = max`

Variables:

`nwater, ncola, max`

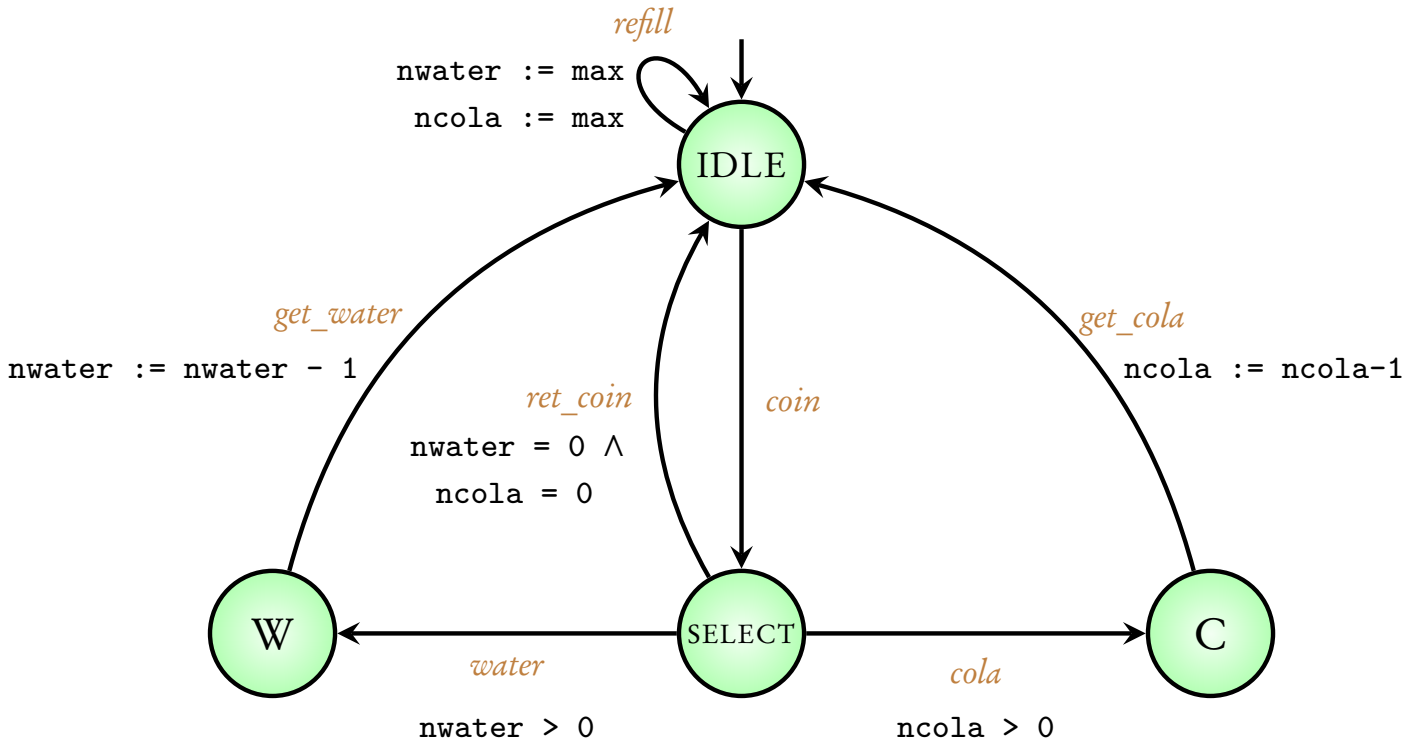


Initial condition:

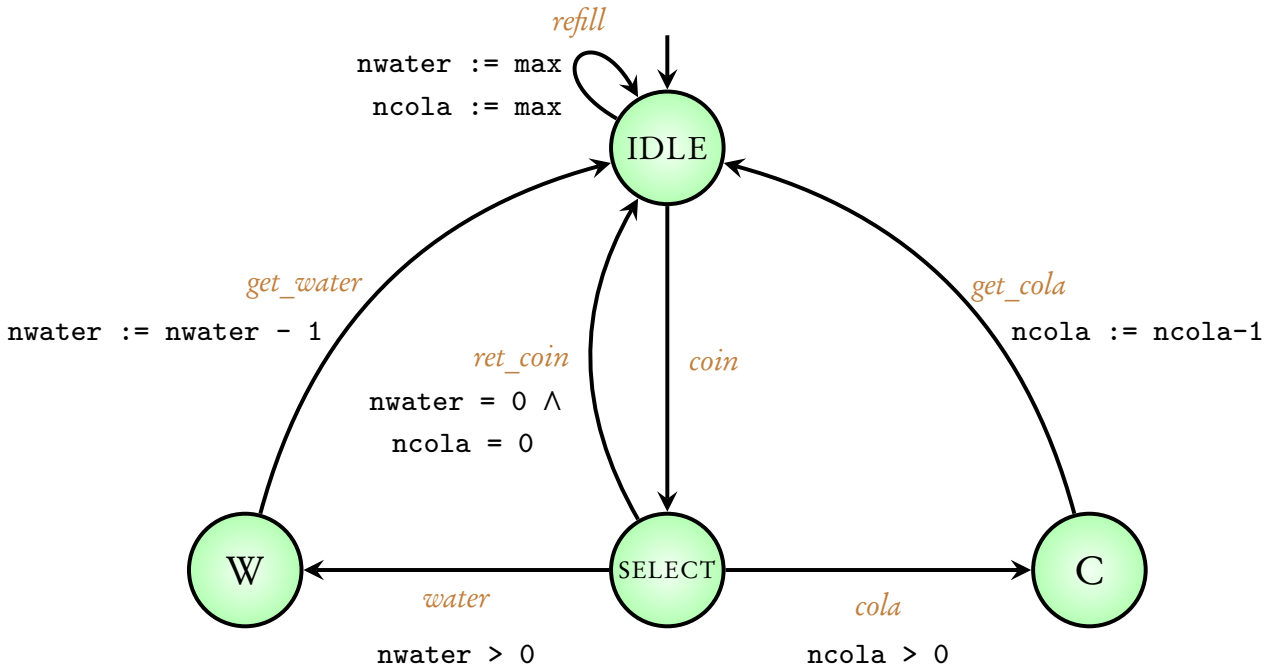
`nwater = max, ncola = max`

Variables:

`nwater, ncola, max`

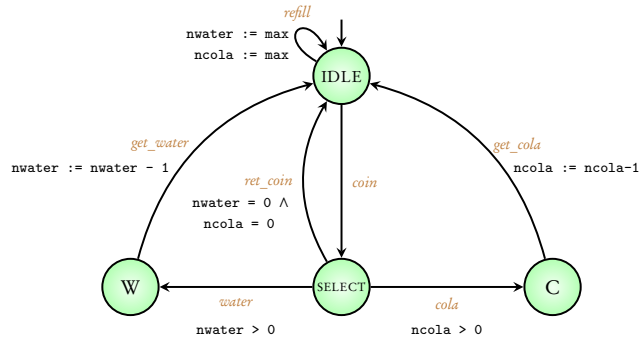


Program graph

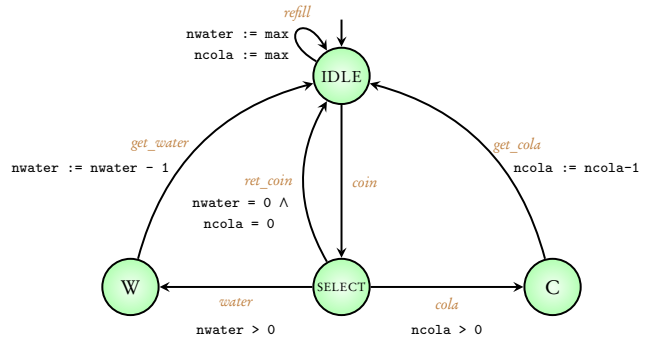


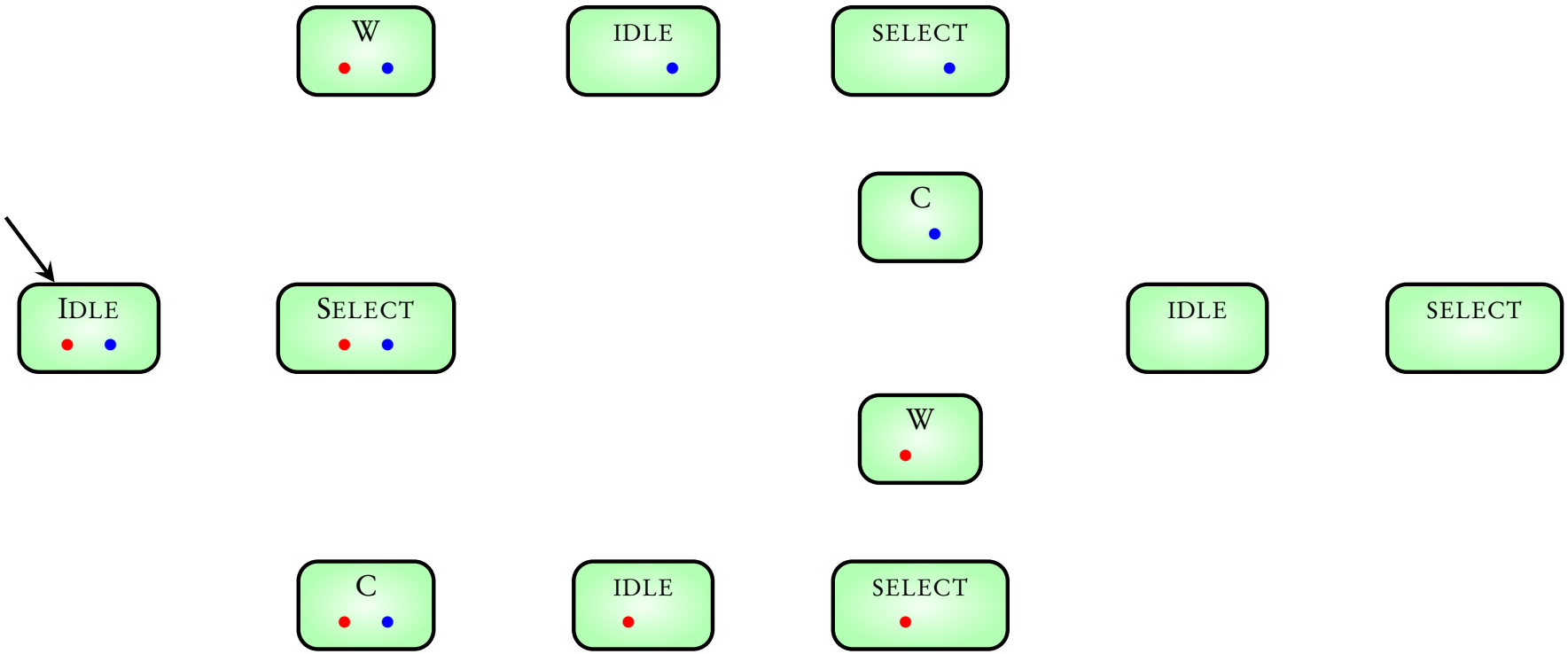
Coming next: Transition system corresponding to `max` = 1

$\texttt{max} = 1$

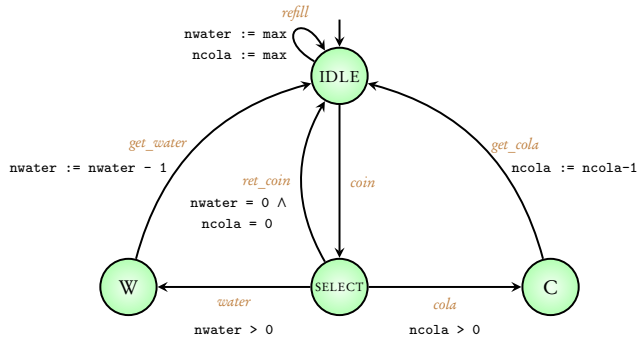

refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0

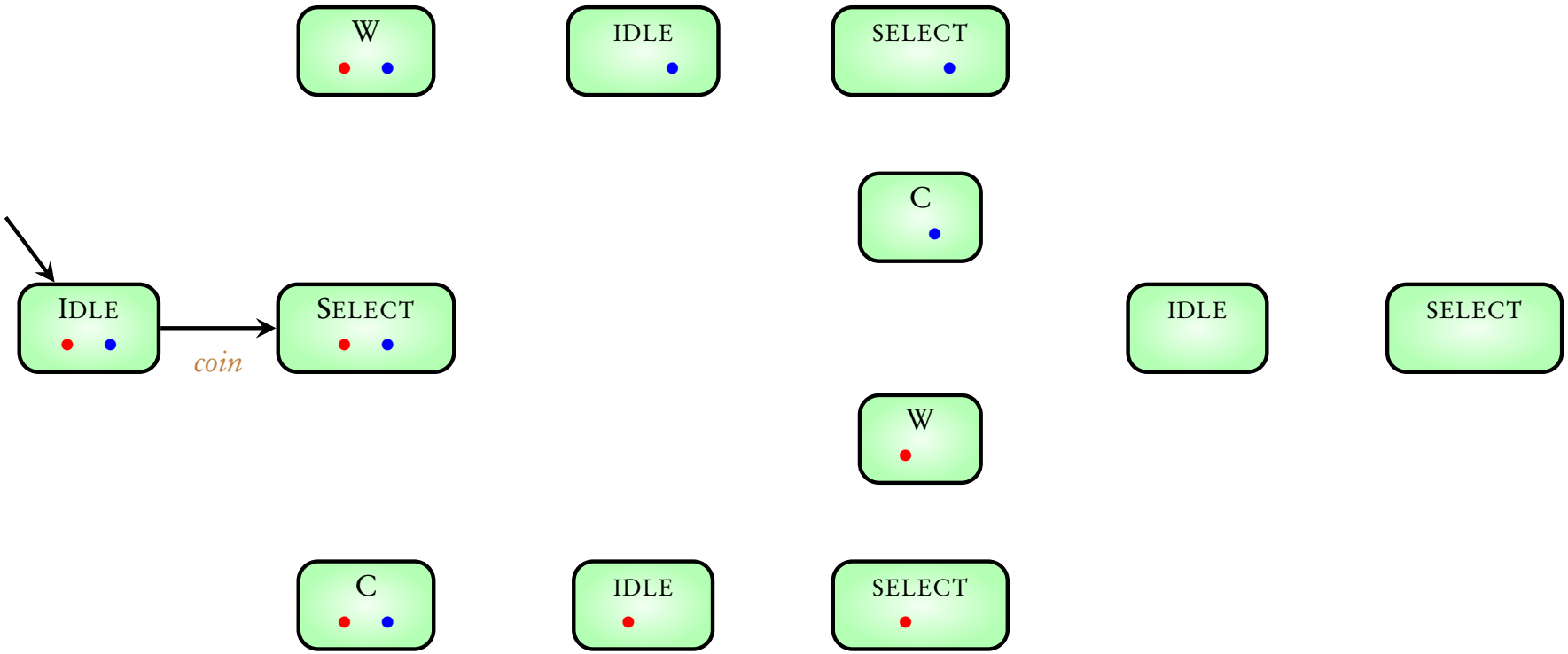
$\texttt{max} = 1$


refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0

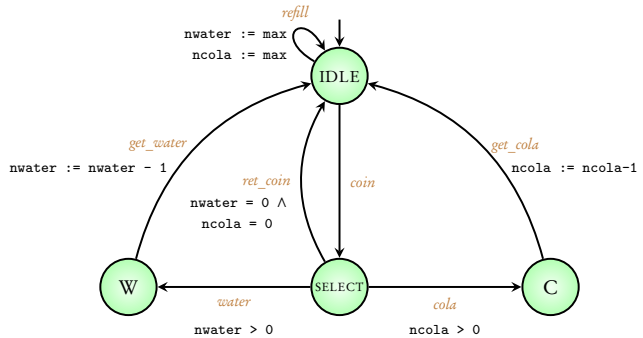

W
IDLE
SELECT
C
IDLE
SELECT
IDLE
SELECT
W
C
IDLE
SELECT

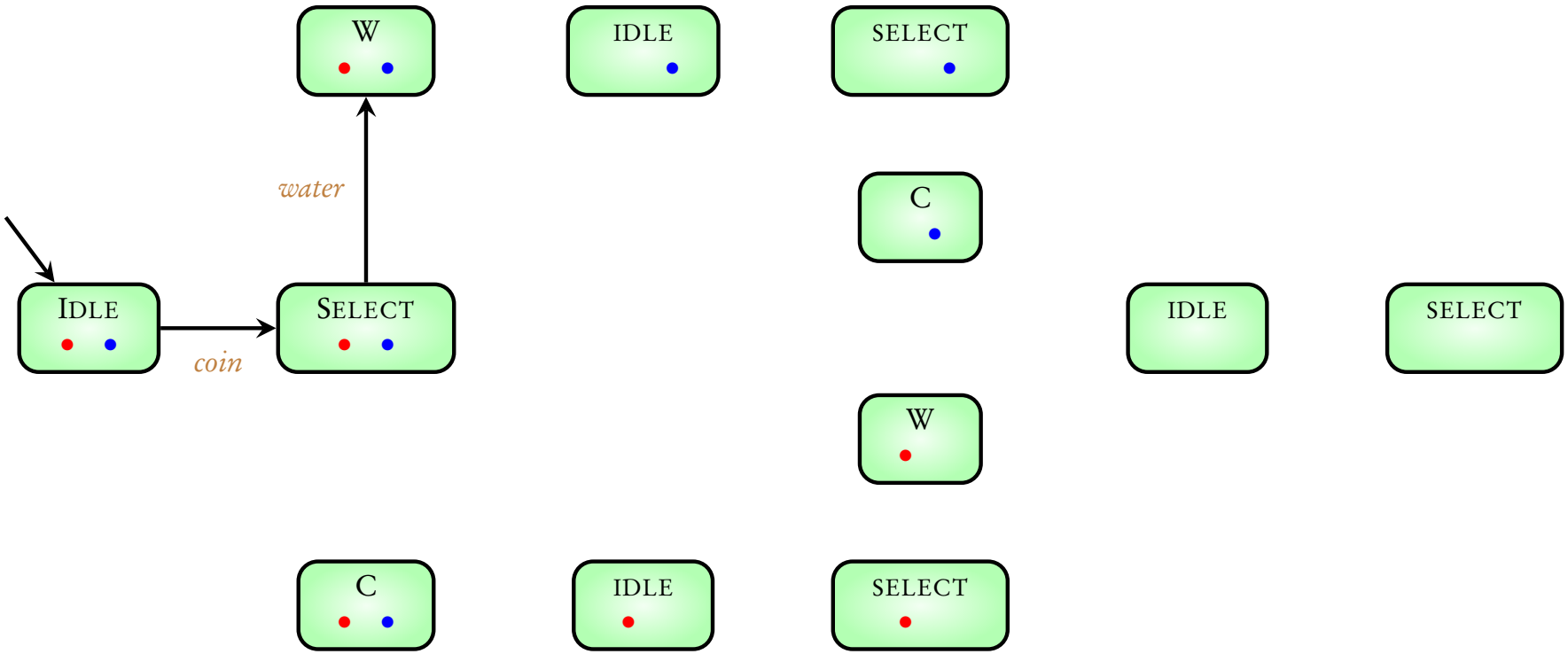
$\texttt{max} = 1$


refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0

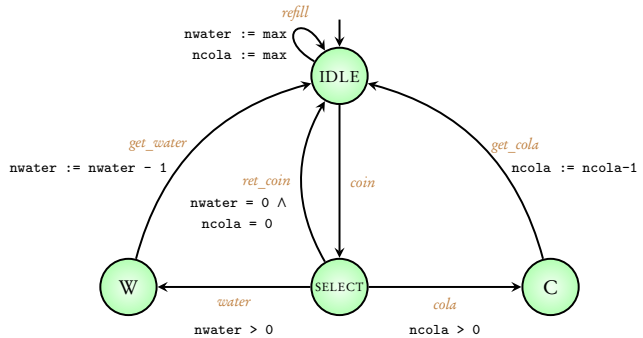

W
IDLE
SELECT
C
IDLE
SELECT
coin
IDLE
SELECT
W
C
IDLE
SELECT

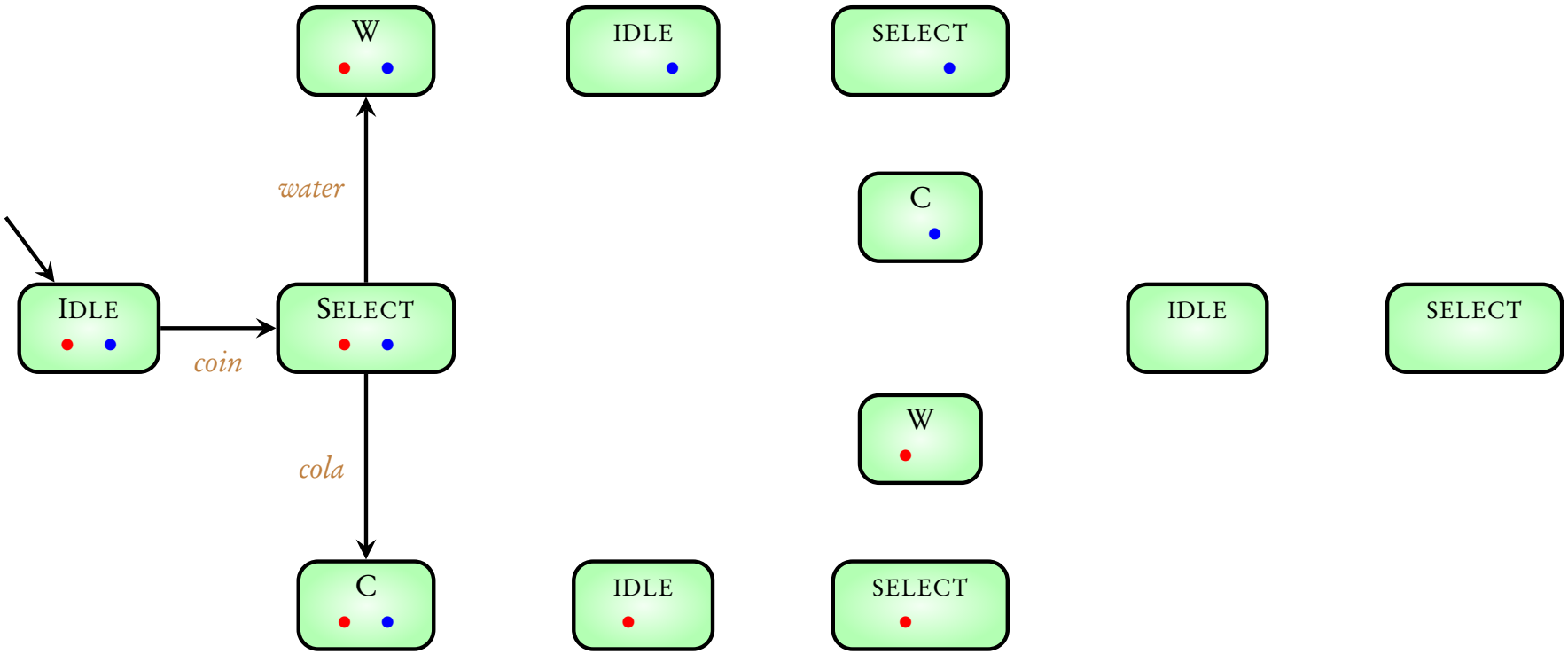
$\texttt{max} = 1$


refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0

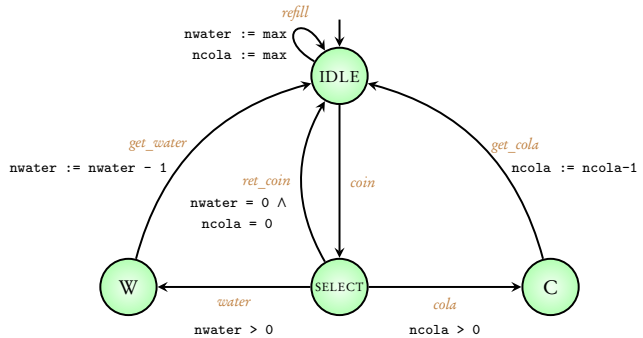

W
IDLE
SELECT
water
C
IDLE
SELECT
coin
W
C
IDLE
SELECT

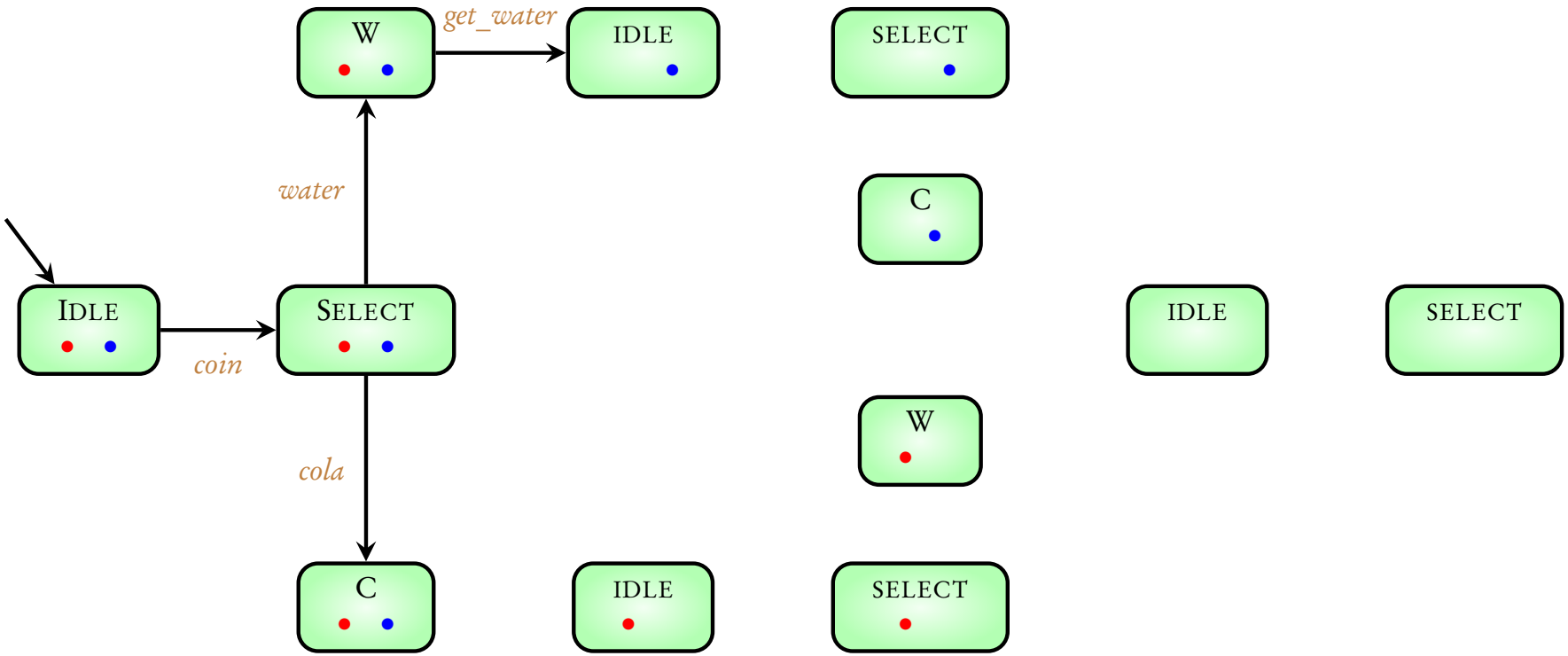
$\texttt{max} = 1$


refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0

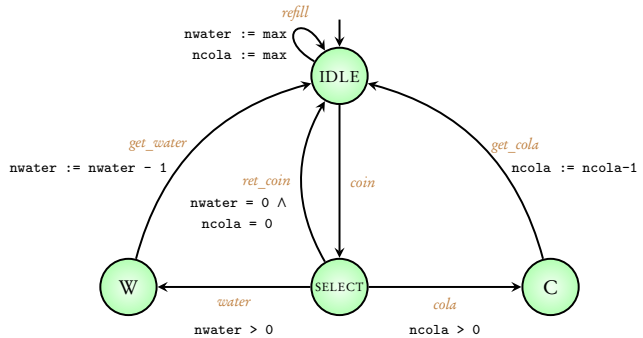

W
IDLE
SELECT
water
C
IDLE
SELECT
IDLE
coin
SELECT
cola
W
C
IDLE
SELECT

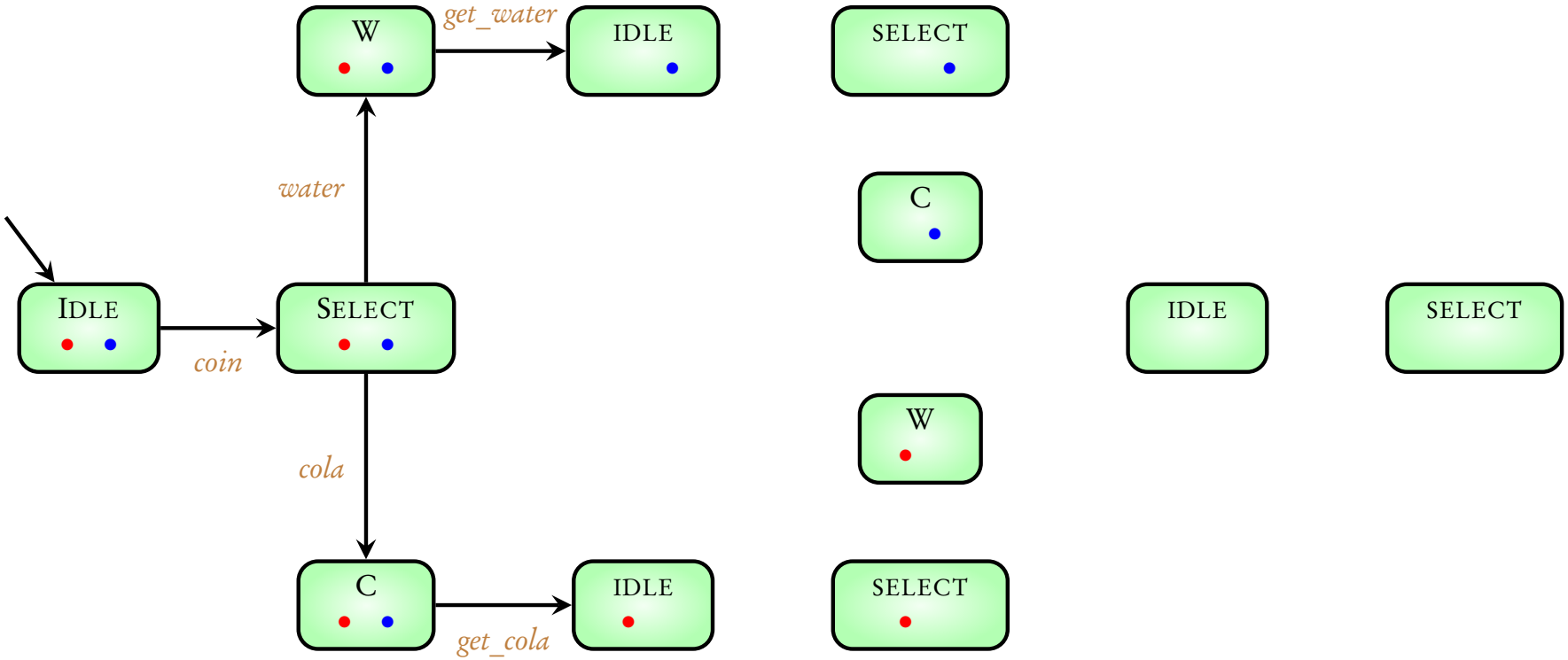
$\texttt{max} = 1$


refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0

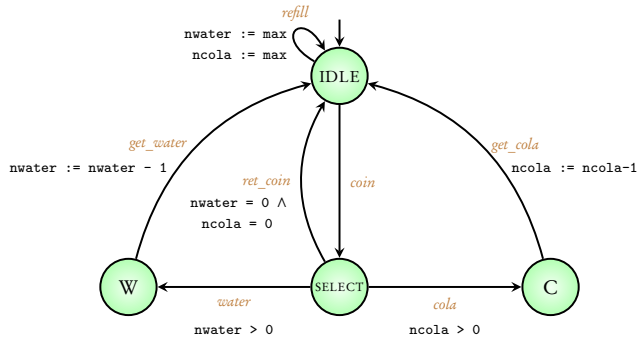

W
get_water
IDLE
SELECT
water
C
IDLE
coin
SELECT
IDLE
SELECT
cola
W
C
IDLE
SELECT

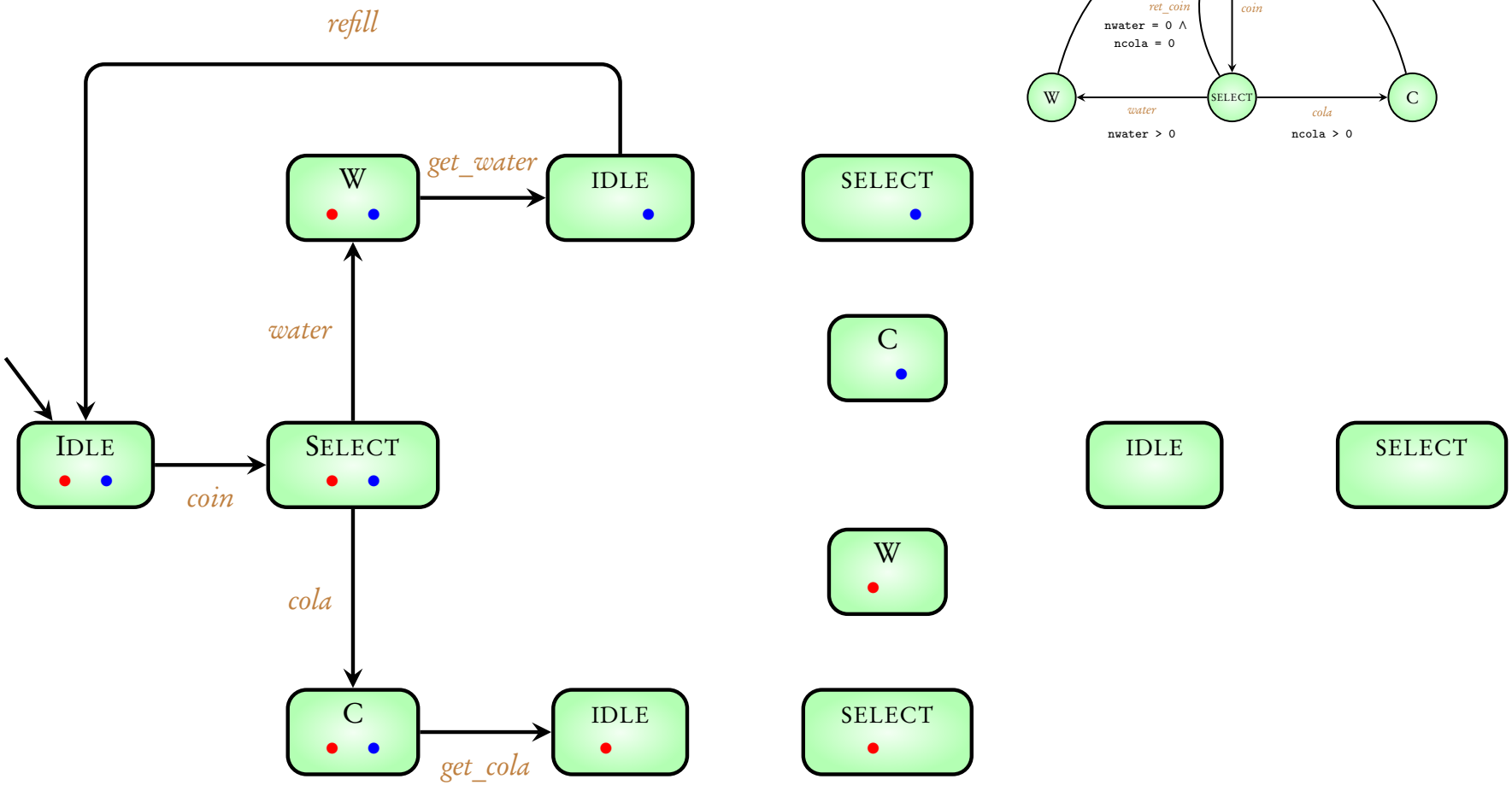
$\texttt{max} = 1$


refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0

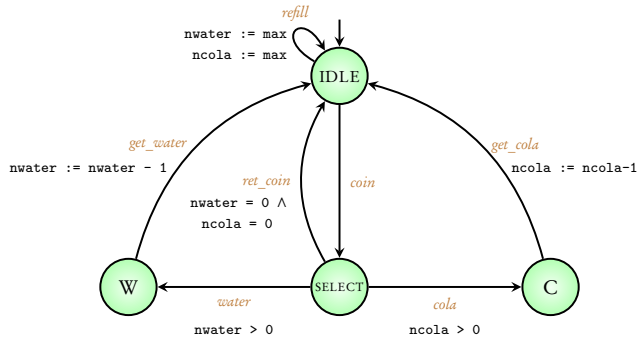

W
get_water
IDLE
SELECT
water
C
IDLE
coin
SELECT
IDLE
SELECT
cola
W
C
IDLE
SELECT
get_cola

$\texttt{max} = 1$


refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0


refill
W
get_water
IDLE
SELECT
water
C
IDLE
SELECT
IDLE
coin
SELECT
cola
W
C
IDLE
SELECT
get_cola

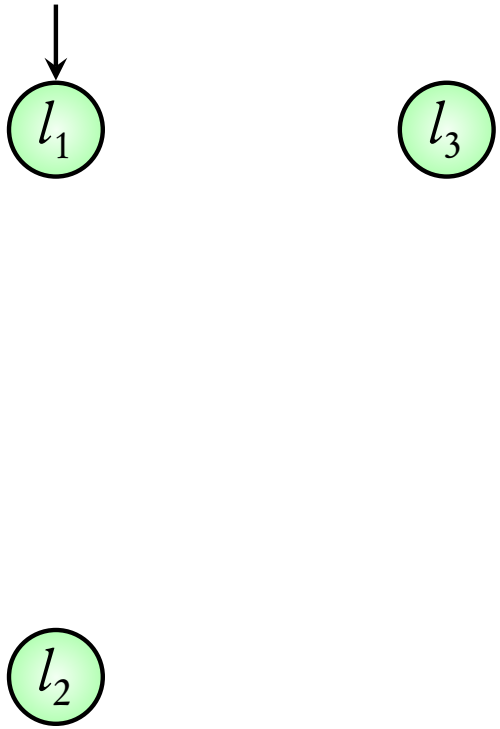
$\texttt{max} = 1$


refill
nwater := max
ncola := max
IDLE
get_water
nwater := nwater - 1
ret_coin
nwater = 0 ∧
ncola = 0
coin
get_cola
ncola := ncola-1
W
SELECT
C
water
nwater > 0
cola
ncola > 0

refill
W
get_water
IDLE
coin
SELECT
cola
C
get_cola
refill
water
IDLE
coin
SELECT
coin
cola
W
get_water
ret_coin
water
C
get_cola
IDLE
coin
SELECT
refill
refill

```
    ...
while (x > 0)
    if (x mod 2 = 0)
        x := x - 2
    else  x:= x - 1
    ...
```

```
...
l1: while (x > 0)
    if (x mod 2 = 0)
l2:     x := x - 2
    else x:= x - 1
...
l3:
```



...

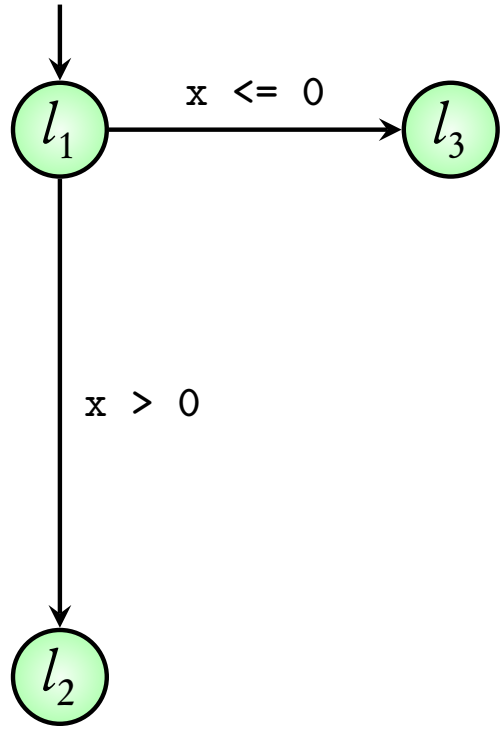
l_1: **while** (x > 0)

l_2:

```
if (x mod 2 = 0)
    x := x - 2
else x:= x - 1
```

...

l_3:



...

l_1: **while** (x > 0)

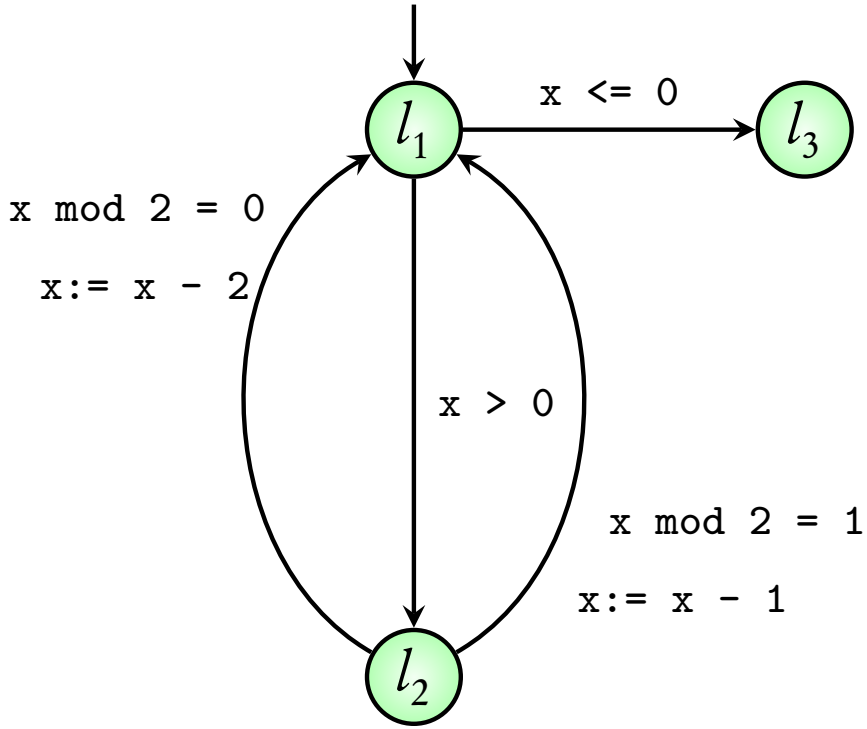
if (x mod 2 = 0)

l_2: x := x - 2

else x:= x - 1

...

l_3:



...

l_1: **while** (x > 0)

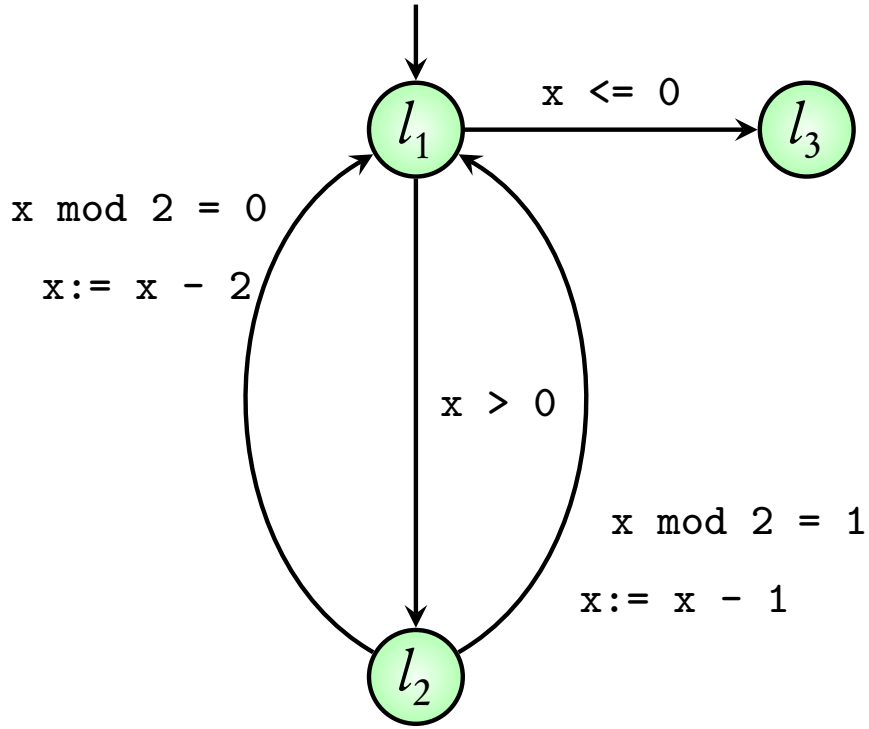
if (x mod 2 = 0)

l_2: x := x - 2

else x:= x - 1

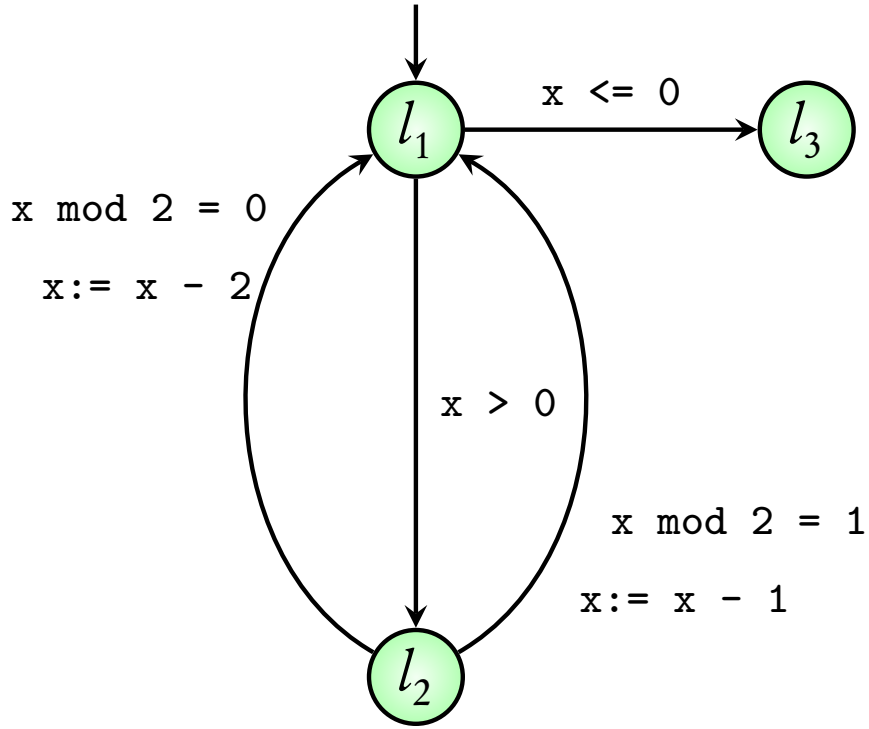
...

l_3:



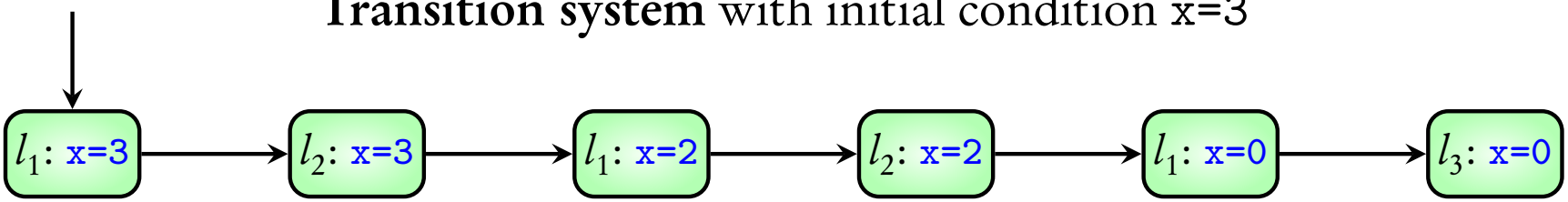
Program graph

```
...
l1: while (x > 0)
        if (x mod 2 = 0)
l2:         x := x - 2
        else x:= x - 1
...
l3:
```



Program graph

Transition system with initial condition x=3



Summary

Data-dependent programs

Program graphs

Transition systems of program graphs

Reference: Principles of Model Checking, *Baier and Katoen*, MIT Press (2008)

Pages 29 - 34