



Formal Methods for Probabilistic Systems

Annabelle McIver
Carroll Morgan

- Source-level program logic
- Meta-theorems for loops
- Examples
 - Probabilistic amplification
 - Uniform selection

Probabilistic amplification

There is a Boolean question Q that the program is to answer, in Boolean variable a .

But $a := Q$ is not allowed!

Instead, only $a := Q_{1/2} \oplus true$ can be used.

We must therefore “amplify” that 1/2 probability towards 1, for which we pay with execution time.

Is K prime?

$true \rightarrow$ “yes”
 $false \rightarrow$ “no”

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$a, n := true, N;$

do $n \neq 0 \wedge a \rightarrow$

$a := Q_{1/2} \oplus true;$

$n := n - 1$

od

$$\{ [a = Q] \}$$

The *Miller-Rabin* test “puts K to the Question”. If K is prime, it will never confess; but if it *is* composite, then it will confess with probability 1/2.

One confession is enough...

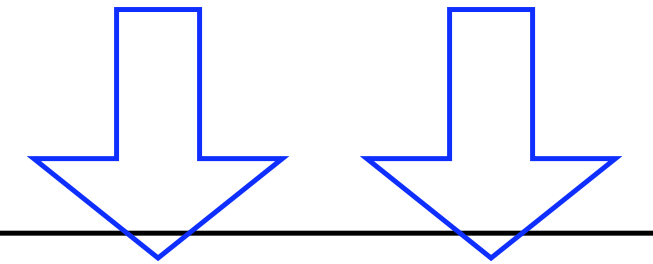
Probabilistic amplification interrogates K a number of times, to increase the probability of confession. (The real Inquisition allowed only three interrogations.)

Probabilistic amplification

The probability that $a = Q$ on termination...

is at least $1 - 1/2^N$...

provided $N \geq 0$ initially.



$\{ [N \geq 0] \times (1 - 1/2^N) \}$

$a, n := true, N;$

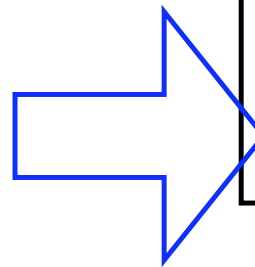
do $n \neq 0 \wedge a \rightarrow$

$a := Q_{1/2} \oplus true;$

$n := n - 1$

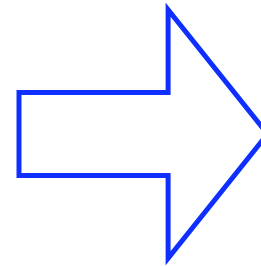
od

$\{ [a = Q] \}$



What is the invariant?

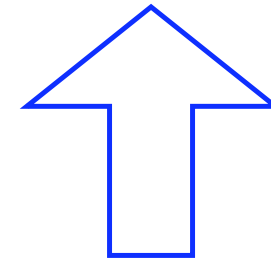
$a = Q$ finally?	Q	not Q
a	true	$1 - 1/2^n$
not a	false	true



```

do  $n \neq 0 \wedge a \rightarrow$ 
   $a := Q_{1/2} \oplus \text{true};$ 
   $n := n - 1$ 
od
{  $[a = Q]$  }

```



After some experimentation,

$$[a] \triangleleft Q \triangleright 1 - [a]/2^n$$

turns out to work well in the calculations.

Invariant is preserved

```

do  n ≠ 0 ∧ a →
    a := Q1/2 ⊕ true;
    n := n - 1
od
  
```

• Invariant "at end of loop body"

$$[a] \triangleleft Q \triangleright 1 - [a]/2^n$$

• $\equiv [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1}$

wp.(n := n - 1)

• $\equiv \frac{1}{2} \times ([Q] \triangleleft Q \triangleright 1 - [Q]/2^{n-1})$ *wp.(a := Q_{1/2} ⊕ true)*
 $+ \frac{1}{2} \times ([true] \triangleleft Q \triangleright 1 - [true]/2^{n-1})$

$\equiv \frac{1}{2} \times 1 + \frac{1}{2} \times (1 \triangleleft Q \triangleright 1 - 1/2^{n-1})$ *arithmetic*

$\equiv 1 \triangleleft Q \triangleright 1 - 1/2^n$ *arithmetic*

$\Leftarrow [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n)$ *[a] from guard*

Loop guard

Invariant "at beginning of loop body"

Invariant establishes overall post-expectation

Negated loop guard ↓ ↓ *Invariant "at end of loop body"*

$$[n=0 \vee ! a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n)$$

$$\Rightarrow [n=0 \vee ! a] \times ([a] \triangleleft Q \triangleright [! a]) \quad \text{arithmetic}$$

$$\Rightarrow [a] \triangleleft Q \triangleright [! a] \quad \text{drop guard}$$

$$\equiv [a=Q] \quad \text{arithmetic}$$

↑ *Overall post-expectation*

```

do  n ≠ 0 ∧ a →
    a := Q1/2 ⊕ true;
    n := n-1
od

```

Invariant... established by initialisation

```

a,n:=true,N;
do n ≠ 0 ∧ a →
  a:= Q1/2⊕ true;
  n:= n-1
od
  
```

Termination condition

Invariant "at
beginning of loop
body"

$$[n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n)$$

$$\bullet \equiv [N \geq 0] \times ([true] \triangleleft Q \triangleright 1 - [true]/2^N)$$

wp.(a,n:=true,N)

$$\equiv [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N)$$

arithmetic

$$\Leftarrow [N \geq 0] \times (1 - 1/2^N)$$

sufficient

• *Probability of establishing Q=a is at least this...*

• *...provided termination is guaranteed.*

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

“postcondition”

$$\{ [a = Q] \}$$

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

invariant

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

"postcondition"

$$\{ [a = Q] \}$$

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee ! a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

invariant and
negated guard

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee ! a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

implies
postcondition

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

a, n := true, N;

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

a := $Q_{1/2} \oplus true$;

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

n := n - 1

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

invariant must
be maintained

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

work backwards

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [Q] \triangleleft Q \triangleright 1 - [Q]/2^{n-1} \quad 1/2^\oplus \quad [true] \triangleleft Q \triangleright 1 - [tru$$

work backwards

$$a := Q_{1/2}^\oplus true;$$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$$n := n - 1$$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$$a, n := true, N;$$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\mathbf{do} \quad n \neq 0 \wedge a \rightarrow$$

$$\{ [Q] \triangleleft Q \triangleright 1 - [Q]/2^{n-1} \quad 1/2^\oplus \}$$

$$a := Q_{1/2}^\oplus true;$$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$$n := n - 1$$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

$$\mathbf{od}$$

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

$$[true] \triangleleft Q \triangleright 1 - [true]/2^{n-1}$$

$$\}$$

work backwards

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [Q] \triangleleft Q \triangleright 1 - [Q]/2^{n-1} \quad 1/2^\oplus \}$$

$a := Q_{1/2^\oplus} true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

$$[true] \triangleleft Q \triangleright 1 - [true]/2^{n-1}$$

$$\}$$

should be
implied by
invariant and
guard

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

a, n := true, N;

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

simplify $\{ 1 \triangleleft Q \triangleright 1 - 0/2^{n-1} \quad 1/2^\oplus \quad 1 \triangleleft Q \triangleright 1 - 1/2^{n-1} \}$

a := Q_{1/2}[⊕] true;

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

n := n-1

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

simplify more

$$\{ 1 \triangleleft Q \triangleright (1 - 1/2 \oplus 1 - 1/2^{n-1}) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

and more

$$\{ 1 \triangleleft Q \triangleright 1 - 1/2^n \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

a, n := true, N;

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

a := $Q_{1/2} \oplus true$;

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

n := n-1

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

$$1 \triangleleft Q \triangleright 1 - 1/2^n$$

strengthen and
"massage"

Summary

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge [a] \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

is now of
the form
"guard and
invariant"

Summary

pre-expectation is
invariant *and*
termination
condition

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

Summary

backwards
through
initialisation

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

Summary

weaken, for
simplicity

$$\{ [N \geq 0] \times (1 - 1/2^N) \}$$

$$\{ [N \geq 0] \times (1 \triangleleft Q \triangleright 1 - 1/2^N) \}$$

$a, n := true, N;$

$$\{ [n \geq 0] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

do $n \neq 0 \wedge a \rightarrow$

$$\{ [a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$a := Q_{1/2} \oplus true;$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^{n-1} \}$$

$n := n - 1$

$$\{ [a] \triangleleft Q \triangleright 1 - [a]/2^n \}$$

od

$$\{ [n=0 \vee \neg a] \times ([a] \triangleleft Q \triangleright 1 - [a]/2^n) \}$$

$$\{ [a = Q] \}$$

Summary

overall
specification

```

{ [N ≥ 0] × (1 - 1/2N) }
{ [N ≥ 0] × (1 ◁ Q ▷ 1 - 1/2N) }
a, n := true, N;
{ [n ≥ 0] × ([a] ◁ Q ▷ 1 - [a]/2n) }
do n ≠ 0 ∧ a →
    { [a] × ([a] ◁ Q ▷ 1 - [a]/2n) }
    a := Q1/2 ⊕ true;
    { [a] ◁ Q ▷ 1 - [a]/2n-1 }
    n := n - 1
    { [a] ◁ Q ▷ 1 - [a]/2n }
od
{ [n = 0 ∨ ¬a] × ([a] ◁ Q ▷ 1 - [a]/2n) }
{ [a = Q] }

```

Summary

The probability that question Q is correctly answered by answer a is at least $1 - 1/2^N$, provided N is non-negative.

```

{  $[N \geq 0] \times (1 - 1/2^N)$  }
a,n := true, N;
do  $n \neq 0 \wedge a \rightarrow$ 
   $a := Q_{1/2} \oplus true;$ 
   $n := n - 1$ 
od
{  $[a = Q]$  }

```

The error probability is at most $1/2^N$.

Uniform selection

Given a positive integer N ,
choose uniformly an integer I
such that $0 \leq I < N$.

Demonic choice of m .

"Expanded"
syntax for
probabilistic
choice.

```
{ [0 ≤ K < N] / N }
```

```
l, h := 0, N;
```

```
do l ≠ h-1 →
```

```
  m: { l < m < h };
```

```
  | l := m    @ (h-m) / (h-l)
```

```
  | h := m    @ (m-l) / (h-l)
```

```
od
```

```
{ [I = K] }
```

Uses expected $2 \lg N$ unbiased bits
if the demonic choice is implemented
as a binary chop $m := (h-l) \div 2$.

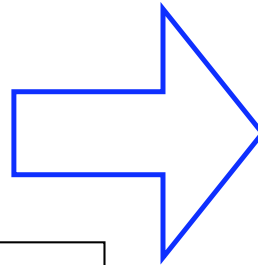
What is the invariant?

A pretty clear guess is $[l \leq K < h] / (h-l)$.

The invariant is preserved

$m: \{l < m < h\};$
$l := m \quad @ (h-m)/(h-l)$
$h := m \quad @ (m-l)/(h-l)$

$$\begin{aligned}
 & [l \leq K < h] / (h-l) \\
 \bullet \equiv & \quad (h-m)/(h-l) \times [m \leq K < h] / (h-m) && wp(\dots | @ \dots) \\
 & + \quad (m-l)/(h-l) \times [l \leq K < m] / (m-l) \\
 \equiv & \quad ([l \leq K < m] + [m \leq K < h]) / (h-l) && \text{arithmetic} \\
 \Leftarrow & \quad [l < m < h] \times [l \leq K < h] / (h-l) && \text{arithmetic} \\
 \bullet \equiv & \quad [l \leq K < h] / (h-l) && wp(m: \{l < m < h\}) \\
 & \text{and standard invariant } l < h
 \end{aligned}$$



```
{ [0 ≤ K < N] / N }
```

```
l, h := 0, N;
```

```
do l ≠ h-1 →
```

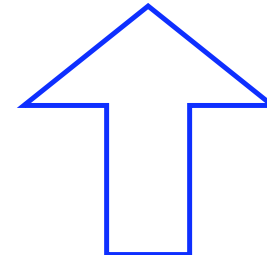
```
  m: { l < m < h };
```

```
  | l := m    @ (h-m)/(h-l)
```

```
  | h := m    @ (m-l)/(h-l)
```

```
od
```

```
{ [l = K] }
```



The invariant is preserved

```

m: {l < m < h};
| l := m    @ (h-m)/(h-l)
| h := m    @ (m-l)/(h-l)

```

$$[l \leq K < h] / (h-l)$$

- \equiv

$$(h-m)/(h-l) \times [m \leq K < h] / (h-m)$$

$$+ (m-l)/(h-l) \times [l \leq K < m] / (m-l)$$
wp.(... | @ ...)
- \equiv

$$([l \leq K < m] + [m \leq K < h]) / (h-l)$$
arithmetic
- \Leftarrow

$$[l < m < h] \times [l \leq K < h] / (h-l)$$
arithmetic
- \equiv

$$[l \leq K < h] / (h-l)$$
wp.(m: {l < m < h})
and standard invariant $l < h$

Summary


```

{ [0 ≤ K < N] / N }
l, h := 0, N;
{ [l ≤ K < h] / (h-l) }
do l ≠ h-1 →
  { [l ≠ h-1 ∧ l ≤ K < h] / (h-l) }
  m := {l < m < h};
  { [l < m < h] × [l ≤ K < h] / (h-l) }
  | l := m    @ (h-m)/(h-l)
  | h := m    @ (m-l)/(h-l)
  { [l ≤ K < h] / (h-l) }
od
{ [l = h-1 ∧ l ≤ K < h] / (h-l) }
{ [l = K] }

```

Summary

overall
specification



```

{ [0 ≤ K < N] / N }
l, h := 0, N;
{ [l ≤ K < h] / (h - l) }
do l ≠ h - 1 →
  { [l ≠ h - 1 ∧ l ≤ K < h] / (h - l) }
  m := {l < m < h};
  { [l < m < h] × [l ≤ K < h] / (h - l) }
  | l := m    @ (h - m) / (h - l)
  | h := m    @ (m - l) / (h - l)
  { [l ≤ K < h] / (h - l) }
od
{ [l = h - 1 ∧ l ≤ K < h] / (h - l) }
{ [l = K] }

```