290 Let x be a *nat* variable. In the refinement

$$P \Leftarrow \textbf{if } x{=}1 \textbf{ then } ok \textbf{ else } x{:=}\ div\ x\ 2.\ P.\ x{:=}\ x{\times}2 \textbf{ fi}$$

each call pushes a return address onto a stack, and each return pops an address from the stack. Add a space variable s and a maximum space variable m, with appropriate assignments to them in the program. Find and prove an upper bound on the maximum space used.

After trying the question, scroll down to the solution.

§ We add variables s, m: *xnat* . If $x{=}0$ then the maximum space used is infinite. If $x{>}0$ then the maximum space used is *floor log x* . We express this as a conjunction so we can use Refinement by Parts.

$(x{=}0 \Rightarrow m'{=}\infty) \wedge (x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x)$

The first part to be proven is

$x{=}0 \Rightarrow m'{=}\infty \Leftarrow$

if $x{=}1$ **then** *ok*

else $x{:=}\ \mathit{div}\ x\ 2.\ \ s{:=}\ s{+}1.\ \ m{:=}\ m{\uparrow}s.\ \ x{=}0 \Rightarrow m'{=}\infty.\ \ s{:=}\ s{-}1.\ \ x{:=}\ 2{\times}x$ **fi**

and the last part is

$x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x \Leftarrow$

if $x{=}1$ **then** *ok*

else $x{:=}\ \mathit{div}\ x\ 2.\ \ s{:=}\ s{+}1.\ \ m{:=}\ m{\uparrow}s.$

$x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x.$

$s{:=}\ s{-}1.\ \ x{:=}\ 2{\times}x$ **fi**

We prove each of these parts by cases. First part, first case:

$x{=}1 \wedge \mathit{ok} \Rightarrow (x{=}0 \Rightarrow m'{=}\infty)$ portation

$= \quad x{=}0 \wedge x{=}1 \wedge \mathit{ok} \Rightarrow m'{=}\infty$

$= \quad \bot \Rightarrow m'{=}\infty$

$= \quad \top$

First part, last case:

$x{\neq}1 \wedge (x{:=}\ \mathit{div}\ x\ 2.\ \ s{:=}\ s{+}1.\ \ m{:=}\ m{\uparrow}s.\ \ x{=}0 \Rightarrow m'{=}\infty.\ \ s{:=}\ s{-}1.\ \ x{:=}\ 2{\times}x)$

$\Rightarrow (x{=}0 \Rightarrow m'{=}\infty)$ substitution 3 times, and portation

$= \quad x{=}0 \wedge x{\neq}1 \wedge (\mathit{div}\ x\ 2{=}0 \Rightarrow m'{=}\infty.\ \ s{:=}\ s{-}1.\ \ x{:=}\ 2{\times}x) \Rightarrow m'{=}\infty$

simplify, and perform sequential compositions

$= \quad x{=}0 \wedge (\mathit{div}\ x\ 2{=}0 \Rightarrow m'{=}\infty) \Rightarrow m'{=}\infty$ discharge

$= \quad x{=}0 \wedge m'{=}\infty \Rightarrow m'{=}\infty$ specialization

$= \quad \top$

Last part, first case:

$x{=}1 \wedge \mathit{ok} \Rightarrow (x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x)$

expand *ok* , portation

$= \quad x{=}1 \wedge x'{=}x \wedge m'{=}m \wedge s'{=}s \wedge x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x$

context $m'{=}m$ and then drop unneeded parts of antecedent

$\Leftarrow \quad m \le s + \mathit{floor\ log}\ x \Rightarrow m \le s + \mathit{floor\ log}\ x$ reflexive

$= \quad \top$

Last part, last case:

$x{\neq}1 \wedge (\ x{:=}\ \mathit{div}\ x\ 2.\ \ s{:=}\ s{+}1.\ \ m{:=}\ m{\uparrow}s.$

$x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x.$

$s{:=}\ s{-}1.\ \ x{:=}\ 2{\times}x)$

$\Rightarrow (x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x)$ substitution 3 times,

$= \quad x{\neq}1$

$\wedge (\quad x{>}0 \wedge s{+}1 \le m{\uparrow}(s{+}1) \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2)$

$\Rightarrow m' \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2).$

$s{:=}\ s{-}1.\ \ x{:=}\ 2{\times}x)$

$\Rightarrow (x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x)$

sequential composition twice

$= \quad x{\neq}1$

$\wedge (\quad x{>}0 \wedge s{+}1 \le m{\uparrow}(s{+}1) \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2)$

$\Rightarrow m' \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2))$

$\Rightarrow (x{>}0 \wedge s \le m \le s + \mathit{floor\ log}\ x \Rightarrow m' \le s + \mathit{floor\ log}\ x)$ portation

$=$ $x\neq 1 \ \wedge\ x>0 \ \wedge\ s \le m \le s + \mathit{floor\ log}\ x$
$\wedge\ (\ x>0 \wedge s+1 \le m\uparrow(s+1) \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2)$
$\Rightarrow\ m' \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2))$
$\Rightarrow\ m' \le s + \mathit{floor\ log}\ x$

use $s+1 \le m\uparrow(s+1)$ and $s+1 \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2)$

$=$ $x\neq 1 \ \wedge\ x>0 \ \wedge\ s \le m \le s + \mathit{floor\ log}\ x$
$\wedge\ (\ x>0 \ \wedge\ m \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2) \ \Rightarrow\ m' \le s + 1 + \mathit{floor\ log}(\mathit{div}\ x\ 2))$
$\Rightarrow\ m' \le s + \mathit{floor\ log}\ x$

in context $x\ge 2$, $1 + \mathit{floor\ log}(\mathit{div}\ x\ 2) \ =\ \mathit{floor\ log}\ x$

$=$ $x\neq 1 \ \wedge\ x>0 \ \wedge\ s \le m \le s + \mathit{floor\ log}\ x$
$\wedge\ (\ x>0 \ \wedge\ m \le s + \mathit{floor\ log}\ x \ \Rightarrow\ m' \le s + \mathit{floor\ log}\ x)$
$\Rightarrow\ m' \le s + \mathit{floor\ log}\ x$ discharge

$=$ $x\neq 1 \ \wedge\ x>0 \ \wedge\ s \le m \le s + \mathit{floor\ log}\ x \ \wedge\ m' \le s + \mathit{floor\ log}\ x$
$\Rightarrow\ m' \le s + \mathit{floor\ log}\ x$ specialize

$=$ $\top$

The proof used a theorem that still needs to be proved: for x: $\mathit{nat} \wedge x\ge 2$ (x: $\mathit{nat}+2$),
$1 + \mathit{floor\ log}(\mathit{div}\ x\ 2) \ =\ \mathit{floor\ log}\ x$
Proof:
$1 + \mathit{floor\ log}(\mathit{div}\ x\ 2)$
$= \mathit{floor}(1 + \mathit{log}(\mathit{div}\ x\ 2))$
$= \mathit{floor\ log}(2 \times \mathit{div}\ x\ 2)$
$= \mathit{floor\ log}(2 \times$ **if** $\mathit{even}\ x$ **then** $x/2$ **else** $(x-1)/2$ **fi**$)$
$=$ **if** $\mathit{even}\ x$ **then** $\mathit{floor\ log}(2 \times x/2)$ **else** $\mathit{floor\ log}(2 \times (x-1)/2)$ **fi**
$=$ **if** $\mathit{even}\ x$ **then** $\mathit{floor\ log}\ x$ **else** $\mathit{floor\ log}(x-1)$ **fi**
To finish this proof, I need to show that for x: $\mathit{nat} \wedge x\ge 2 \wedge \mathit{odd}\ x$ (x: $2\times\mathit{nat} + 3$),
$\mathit{floor\ log}(x-1) \ =\ \mathit{floor\ log}\ x$
It's true, but I don't see how to prove it.