

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

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

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

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

The first part to be proven is

$$x=0 \Rightarrow m'=\infty \iff$$

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

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

and the last part is

$$x>0 \wedge s \leq m \leq s + \text{floor log } x \Rightarrow m' \leq s + \text{floor log } x \iff$$

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

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

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

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

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

$$\begin{aligned} & x=1 \wedge \text{ok} \Rightarrow (x=0 \Rightarrow m'=\infty) && \text{portation} \\ = & x=0 \wedge x=1 \wedge \text{ok} \Rightarrow m'=\infty \\ = & \perp \Rightarrow m'=\infty \\ = & \top \end{aligned}$$

First part, last case:

$$\begin{aligned} & x \neq 1 \wedge (x := \text{div } x \ 2. \ s := s+1. \ m := m \uparrow s. \ x=0 \Rightarrow m'=\infty. \ s := s-1. \ x := 2 \times x) \\ & \Rightarrow (x=0 \Rightarrow m'=\infty) && \text{substitution 3 times, and portation} \\ = & x=0 \wedge x \neq 1 \wedge (\text{div } x \ 2=0 \Rightarrow m'=\infty. \ s := s-1. \ x := 2 \times x) \Rightarrow m'=\infty \\ & \text{simplify, and perform sequential compositions} \\ = & x=0 \wedge (\text{div } x \ 2=0 \Rightarrow m'=\infty) \Rightarrow m'=\infty && \text{discharge} \\ = & x=0 \wedge m'=\infty \Rightarrow m'=\infty && \text{specialization} \\ = & \top \end{aligned}$$

Last part, first case:

$$\begin{aligned} & x=1 \wedge \text{ok} \Rightarrow (x>0 \wedge s \leq m \leq s + \text{floor log } x \Rightarrow m' \leq s + \text{floor log } x) \\ & \text{expand } \text{ok} \text{ , portation} \\ = & x=1 \wedge x'=x \wedge m'=m \wedge s'=s \wedge x>0 \wedge s \leq m \leq s + \text{floor log } x \Rightarrow m' \leq s + \text{floor log } x \\ & \text{context } m'=m \text{ and then drop unneeded parts of antecedent} \\ \iff & m \leq s + \text{floor log } x \Rightarrow m \leq s + \text{floor log } x && \text{reflexive} \\ = & \top \end{aligned}$$

Last part, last case:

$$\begin{aligned} & x \neq 1 \wedge (x := \text{div } x \ 2. \ s := s+1. \ m := m \uparrow s. \\ & \quad x>0 \wedge s \leq m \leq s + \text{floor log } x \Rightarrow m' \leq s + \text{floor log } x. \\ & \quad s := s-1. \ x := 2 \times x) \\ & \Rightarrow (x>0 \wedge s \leq m \leq s + \text{floor log } x \Rightarrow m' \leq s + \text{floor log } x) && \text{substitution 3 times,} \\ = & \quad x \neq 1 \\ & \quad \wedge (\quad x>0 \wedge s+1 \leq m \uparrow (s+1) \leq s+1 + \text{floor log } (\text{div } x \ 2) \\ & \quad \Rightarrow m' \leq s+1 + \text{floor log } (\text{div } x \ 2). \\ & \quad s := s-1. \ x := 2 \times x) \\ & \Rightarrow (x>0 \wedge s \leq m \leq s + \text{floor log } x \Rightarrow m' \leq s + \text{floor log } x) \\ & \text{sequential composition twice} \\ = & \quad x \neq 1 \\ & \quad \wedge (\quad x>0 \wedge s+1 \leq m \uparrow (s+1) \leq s+1 + \text{floor log } (\text{div } x \ 2) \\ & \quad \Rightarrow m' \leq s+1 + \text{floor log } (\text{div } x \ 2)) \\ & \Rightarrow (x>0 \wedge s \leq m \leq s + \text{floor log } x \Rightarrow m' \leq s + \text{floor log } x) && \text{portation} \end{aligned}$$

$$\begin{aligned}
&= \quad x \neq 1 \wedge x > 0 \wedge s \leq m \leq s + \text{floor } \log x \\
&\quad \wedge (\quad x > 0 \wedge s + 1 \leq m \uparrow (s + 1) \leq s + 1 + \text{floor } \log(\text{div } x \ 2) \\
&\quad \quad \Rightarrow m' \leq s + 1 + \text{floor } \log(\text{div } x \ 2)) \\
&\Rightarrow m' \leq s + \text{floor } \log x \\
&\quad \quad \text{use } s + 1 \leq m \uparrow (s + 1) \text{ and } s + 1 \leq s + 1 + \text{floor } \log(\text{div } x \ 2) \\
&= \quad x \neq 1 \wedge x > 0 \wedge s \leq m \leq s + \text{floor } \log x \\
&\quad \wedge (x > 0 \wedge m \leq s + 1 + \text{floor } \log(\text{div } x \ 2) \Rightarrow m' \leq s + 1 + \text{floor } \log(\text{div } x \ 2)) \\
&\Rightarrow m' \leq s + \text{floor } \log x \\
&\quad \quad \text{in context } x \geq 2, 1 + \text{floor } \log(\text{div } x \ 2) = \text{floor } \log x \\
&= \quad x \neq 1 \wedge x > 0 \wedge s \leq m \leq s + \text{floor } \log x \\
&\quad \wedge (x > 0 \wedge m \leq s + \text{floor } \log x \Rightarrow m' \leq s + \text{floor } \log x) \\
&\Rightarrow m' \leq s + \text{floor } \log x \quad \text{discharge} \\
&= \quad x \neq 1 \wedge x > 0 \wedge s \leq m \leq s + \text{floor } \log x \wedge m' \leq s + \text{floor } \log x \\
&\Rightarrow m' \leq s + \text{floor } \log x \quad \text{specialize} \\
&= \quad \top
\end{aligned}$$

The proof used a theorem that still needs to be proved: for $x: \text{nat} \wedge x \geq 2$ ($x: \text{nat} + 2$),
 $1 + \text{floor } \log(\text{div } x \ 2) = \text{floor } \log x$

Proof:

$$\begin{aligned}
&1 + \text{floor } \log(\text{div } x \ 2) \\
&= \text{floor}(1 + \log(\text{div } x \ 2)) \\
&= \text{floor } \log(2 \times \text{div } x \ 2) \\
&= \text{floor } \log(2 \times \mathbf{\text{if even } x \text{ then } x/2 \text{ else } (x-1)/2 \mathbf{fi}}) \\
&= \mathbf{\text{if even } x \text{ then } \text{floor } \log(2 \times x/2) \text{ else } \text{floor } \log(2 \times (x-1)/2) \mathbf{fi}} \\
&= \mathbf{\text{if even } x \text{ then } \text{floor } \log x \text{ else } \text{floor } \log(x-1) \mathbf{fi}}
\end{aligned}$$

To finish this proof, I need to show that for $x: \text{nat} \wedge x \geq 2 \wedge \text{odd } x$ ($x: 2 \times \text{nat} + 3$),
 $\text{floor } \log(x-1) = \text{floor } \log x$

It's true, but I don't see how to prove it.