Specification

state space	memory	*int*; (0,..20); *char*; *rat*
state	memory contents	–2; 15; "A"; 3.14
prestate	initial state	$\sigma = \sigma_0; \sigma_1; \sigma_2; \sigma_3 = i\ ;\ n\ ;\ c\ ;\ x$
poststate	final state	$\sigma' = \sigma'_0; \sigma'_1; \sigma'_2; \sigma'_3 = i'\ ;\ n'\ ;\ c'\ ;\ x'$
addresses	low level	0 , 1 , 2 , 3
state variables	high level	$i\ ,\ n\ ,\ c\ ,\ x$
	initial values	$i\ ,\ n\ ,\ c\ ,\ x$
	final values	$i'\ ,\ n'\ ,\ c'\ ,\ x'$

For now: prestate, poststate

Later: time (termination = finite time), space, interaction, communication, ...

Specification

specification of computer behavior: a boolean expression

in variables σ and σ'

We provide a prestate as input.

A computation satisfies a specification by computing a satisfactory poststate as output.

The given prestate and computed poststate must make the specification true.

Specification

specification of computer behavior: a boolean expression

in the initial values x , y , ... and final values x' , y' , ... of some state variables

We provide initial values as input.

A computation satisfies a specification by computing satisfactory final values as output.

The given initial values and computed final values must make the specification true.

Specification

Specification S is **unsatisfiable** for prestate σ : $\quad ¢(§\sigma' \cdot S) \; < \; 1$

Specification S is **satisfiable** for prestate σ : $\quad ¢(§\sigma' \cdot S) \; \ge \; 1$

Specification S is **deterministic** for prestate σ : $\quad ¢(§\sigma' \cdot S) \; \le \; 1$

Specification S is **nondeterministic** for prestate σ : $\quad ¢(§\sigma' \cdot S) \; > \; 1$

Specification S is **satisfiable** for prestate σ : $\quad \exists \sigma' \cdot S$

Specification S is **implementable**: $\quad \forall \sigma \cdot \exists \sigma' \cdot S$

Specification

examples

$x' = x+1 \;\wedge\; y' = y$	implementable, deterministic
$x' > x$	implementable, nondeterministic
$\top$	implementable, extremely nondeterministic
$\bot$	unimplementable, overly deterministic
$x \geq 0 \;\wedge\; y'=0$	unimplementable, overly deterministic
$x \geq 0 \;\Rightarrow\; y'=0$	implementable, nondeterministic

$$ok \quad = \quad \sigma'=\sigma \quad = \quad x'=x \wedge y'=y \wedge \ldots$$

$$x{:=}\, e \quad = \quad \sigma' = \sigma \triangleleft \mathit{address}\ \text{"}x\text{"} \triangleright e \quad = \quad x'=e \wedge y'=y \wedge \ldots$$

$$x{:=}\, x+y \quad = \quad x'=x+y \wedge y'=y$$

if $x=y$ **then** $x{:=}\, x+y$ **else** $x'+y' = 3$

dependent composition

$$S.\,R \quad = \quad \exists x'', y'', \ldots \cdot \quad (\text{substitute } x'', y'', \ldots \text{ for } x', y', \ldots \text{ in } S)$$
$$\land \quad (\text{substitute } x'', y'', \ldots \text{ for } x, y, \ldots \text{ in } R)$$

In integer variable x

$$x'{=}x \lor x'{=}x{+}1 \;.\; x'{=}x \lor x'{=}x{+}1$$

$= \quad \exists x''\cdot\; (x''{=}x \lor x''{=}x{+}1) \land (x'{=}x'' \lor x'{=}x''{+}1)$ — distribute $\land$ over $\lor$

$= \quad \exists x''\cdot\; x''{=}x \land x'{=}x'' \lor x''{=}x{+}1 \land x'{=}x''$
$\lor\; x''{=}x \land x'{=}x''{+}1 \lor x''{=}x{+}1 \land x'{=}x''{+}1$ — distribute $\exists$ over $\lor$

$= \quad (\exists x''\cdot\; x''{=}x \land x'{=}x'') \lor (\exists x''\cdot\; x''{=}x{+}1 \land x'{=}x'')$
$\lor\; (\exists x''\cdot\; x''{=}x \land x'{=}x''{+}1) \lor (\exists x''\cdot\; x''{=}x{+}1 \land x'{=}x''{+}1)$ — One-Point Law 4 times

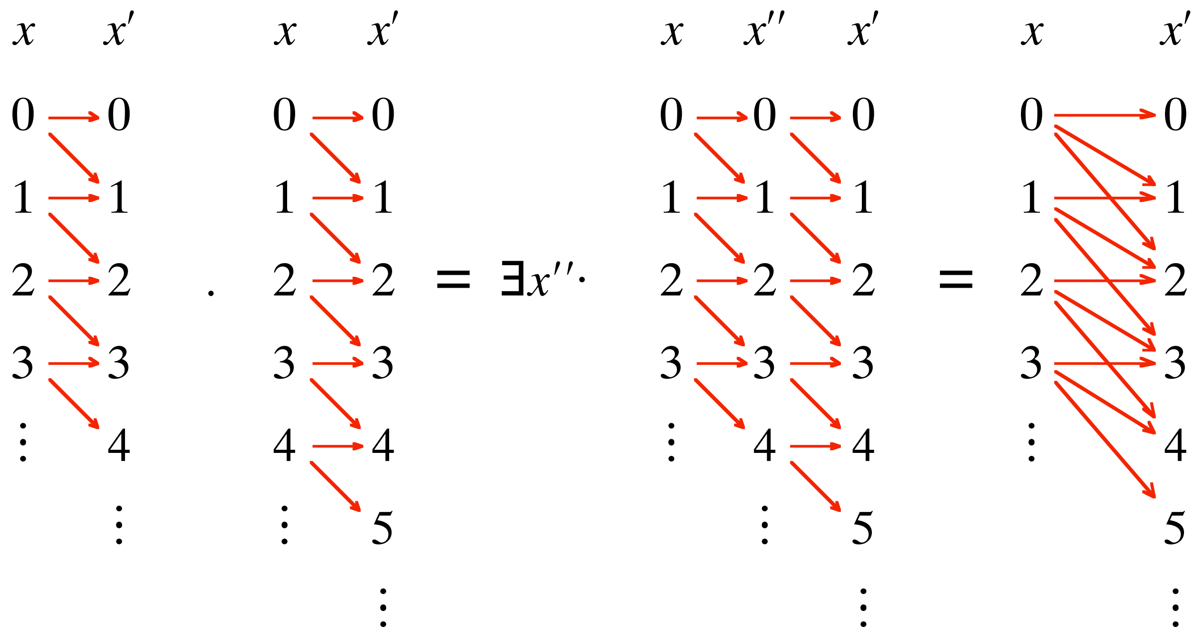
$= \quad x'{=}x \lor x'{=}x{+}1 \lor x'{=}x{+}2$

dependent composition

$$S.R \quad = \quad \exists x'', y'', ...\cdot \quad (\text{substitute } x'', y'', ... \text{ for } x', y', ... \text{ in } S)$$
$$\land \quad (\text{substitute } x'', y'', ... \text{ for } x, y, ... \text{ in } R)$$

In integer variable x

$$x'{=}x \lor x'{=}x{+}1 \ . \ x'{=}x \lor x'{=}x{+}1$$



dependent composition

$$S.R \quad = \quad \exists x'', y'', ...\cdot \quad (\text{substitute } x'', y'', ... \text{ for } x', y', ... \text{ in } S)$$

$$\land \quad (\text{substitute } x'', y'', ... \text{ for } x, y, ... \text{ in } R)$$

In integer variables x and y

$$x{:=}\ 3.\ \ y{:=}\ x{+}y \qquad \text{eliminate assignments first}$$

$$= \quad x'{=}3 \land y'{=}y.\ \ x'{=}x \land y'{=}x{+}y \qquad \text{then eliminate dependent composition}$$

$$= \quad \exists x'', y''{:}\ int\cdot\ x''{=}3 \land y''{=}y \ \land\ x'{=}x'' \land y'{=}x''{+}y'' \qquad \text{use One-Point Law twice}$$

$$= \quad x'{=}3 \ \land\ y' = 3{+}y$$

specification laws

$ok.\,P \;=\; P.\,ok \;=\; P$	Identity Law
$P.\,(Q.\,R) \;=\; (P.\,Q).\,R$	Associative Law
$\textbf{if } b \textbf{ then } P \textbf{ else } P \;=\; P$	Idempotent Law
$\textbf{if } b \textbf{ then } P \textbf{ else } Q \;=\; \textbf{if } \neg b \textbf{ then } Q \textbf{ else } P$	Case Reversal Law
$P \;=\; \textbf{if } b \textbf{ then } b \Rightarrow P \textbf{ else } \neg b \Rightarrow P$	Case Creation Law
$\textbf{if } b \textbf{ then } S \textbf{ else } R \;=\; b \wedge S \vee \neg b \wedge R$	Case Analysis Law
$\textbf{if } b \textbf{ then } S \textbf{ else } R \;=\; (b \Rightarrow S) \wedge (\neg b \Rightarrow R)$	Case Analysis Law
$P \vee Q.\,R \vee S \;=\; (P.\,R) \vee (P.\,S) \vee (Q.\,R) \vee (Q.\,\mathrm{S})$	Distributive Law
$(\textbf{if } b \textbf{ then } P \textbf{ else } Q) \wedge R \;=\; \textbf{if } b \textbf{ then } P \wedge R \textbf{ else } Q \wedge R$	Distributive Law
$(\textbf{if } b \textbf{ then } P \textbf{ else } Q).\,R \;=\; \textbf{if } b \textbf{ then } (P.\,R) \textbf{ else } (Q.\,R)$	Distributive Law
$x{:=}\ \textbf{if } b \textbf{ then } e \textbf{ else } f \;=\; \textbf{if } b \textbf{ then } x{:=}\,e \textbf{ else } x{:=}\,f$	Functional-Imperative Law
$x{:=}\,e.\,P \;=\; (\text{for } x \text{ substitute } e \text{ in } P\,)$	Substitution Law

substitution law

$$x{:=}\, e.\ P \quad = \quad (\text{for } x \text{ substitute } e \text{ in } P\,)$$

$$x{:=}\, y{+}1.\ \ y' > x' \quad = \quad y' > x'$$

$$x{:=}\, x{+}1.\ \ y'{>}x \land x'{>}x \quad = \quad y' > x{+}1 \ \land\ x' > x{+}1$$

$$x{:=}\, y{+}1.\ \ y' = 2{\times}x \quad = \quad y' = 2{\times}(y{+}1)$$

$$x{:=}\, 1.\ \ x{\ge}1 \Rightarrow \exists x\cdot\ y' = 2{\times}x \quad = \quad 1{\ge}1 \Rightarrow \exists x\cdot\ y' = 2{\times}x \quad = \quad \mathit{even}\ y'$$

$$x{:=}\, y.\ \ x{\ge}1 \Rightarrow \exists y\cdot\ y' = x{\times}y \quad = \quad x{:=}\, y.\ \ x{\ge}1 \Rightarrow \exists k\cdot\ y' = x{\times}k$$

$$= \quad y{\ge}1 \Rightarrow \exists k\cdot\ y' = y{\times}k$$

$$x{:=}\, 1.\ \ ok \quad = \quad x{:=}\, 1.\ \ x'{=}x \land y'{=}y \quad = \quad x'{=}1 \land y'{=}y$$

$$x{:=}\, 1.\ \ y{:=}\, 2 \quad = \quad x{:=}\, 1.\ \ x'{=}x \land y'{=}2 \quad = \quad x'{=}1 \land y'{=}2$$

substitution law

$$x{:=}\, e.\ P \quad = \quad (\text{for } x \text{ substitute } e \text{ in } P\,)$$

$$x{:=}\,1.\ \ y{:=}\,2.\ \ x{:=}\,x{+}y$$

$$=\qquad x{:=}\,1.\ \ y{:=}\,2.\ \ x' = x{+}y \ \land\ y'{=}y$$

$$=\qquad x{:=}\,1.\ \ x' = x{+}2 \ \land\ y'{=}2$$

$$=\qquad x'{=}3 \land y'{=}2$$

$$x{:=}\,1.\ \ x' > x.\ \ x' = x{+}1$$

$$=\qquad x' > 1.\ \ x' = x{+}1$$

$$=\qquad \exists x'', y''\cdot\ x''{>}1 \ \land\ x' = x''{+}1$$

$$=\qquad \exists x''\cdot\ x''{>}1 \ \land\ x' = x''{+}1$$

$$=\qquad \exists x''\cdot\ x''{>}1 \ \land\ x'' = x'{-}1$$

$$=\qquad x'{-}1 > 1$$

$$=\qquad x'{>}2$$

Refinement

Specification P (the problem) is **refined** by specification S (the solution) if and only if P is satisfied whenever S is satisfied.

$$\forall \sigma, \sigma' \cdot P \Leftarrow S$$

$$x' > x \quad \Leftarrow \quad x' = x+1 \wedge y' = y \quad = \quad x := x+1$$

$$x' \le x \quad \Leftarrow \quad \textbf{if } x=0 \textbf{ then } x'=x \textbf{ else } x'<x \quad = \quad x=0 \wedge x'=x \ \vee \ x \ne 0 \wedge x'<x$$

$$\begin{aligned} x' > y' > x \quad &\Leftarrow \quad y := x+1.\ \ x := y+1 \\ &= \quad y := x+1.\ \ x' = y+1 \wedge y' = y \\ &= \quad x' = x+2 \wedge y' = x+1 \end{aligned}$$

condition: specification that refers to (at most) one state

initial condition, precondition: refers to (at most) the initial state (prestate)

final condition, postcondition: refers to (at most) the final state (poststate)

exact precondition for P to be refined by S : $\forall\sigma'\cdot P \Leftarrow S$

exact postcondition for P to be refined by S : $\forall\sigma\cdot P \Leftarrow S$

sufficient $\Rightarrow$ exact $\Rightarrow$ necessary (the exact precondition for $x'{>}5$ to be refined by $x{:=}\ x{+}1$)

$= \quad \forall x' \cdot\ x'{>}5 \Leftarrow (x{:=}\ x{+}1)$

$= \quad \forall x' \cdot\ x'{>}5 \Leftarrow x'{=}x{+}1$ One-Point Law

$= \quad x{+}1 > 5$

$= \quad x > 4$

$x{>}4 \Rightarrow x'{>}5 \quad \Leftarrow \quad x{:=}\ x{+}1$

one-point laws

$\exists v \cdot\ v{=}e \wedge P \quad = \quad$ (replace v with e in P)

$\forall v \cdot\ v{=}e \Rightarrow P \quad = \quad$ (replace v with e in P)

(the exact postcondition for $x>4$ to be refined by $x:= x+1$)

$=\quad \forall x\cdot\ x>4 \Leftarrow (x:= x+1)$

$=\quad \forall x\cdot\ x>4 \Leftarrow x'=x+1$

$=\quad \forall x\cdot\ x>4 \Leftarrow x=x'-1$ One-Point Law

$=\quad x'-1 > 4$

$=\quad x' > 5$

$x'>5 \Rightarrow x>4 \quad \Longleftarrow \quad x:= x+1$

$x\le 4 \Rightarrow x'\le 5 \quad \Longleftarrow \quad x:= x+1$

contrapositive law

$a\Rightarrow b \quad = \quad \neg b\Rightarrow\neg a$

condition laws

$$C \wedge (P.\,Q) \quad \Leftarrow \quad C{\wedge}P.\,Q$$

$$C \Rightarrow (P.Q) \quad \Leftarrow \quad C{\Rightarrow}P.\,Q$$

$$(P.Q) \wedge C' \quad \Leftarrow \quad P.\,Q{\wedge}C'$$

$$(P.Q) \Leftarrow C' \quad \Leftarrow \quad P.\,Q{\Leftarrow}C'$$

$$P.\,C{\wedge}Q \quad \Leftarrow \quad P{\wedge}C'.\,Q$$

$$P.\,Q \quad \Leftarrow \quad P{\wedge}C'.\,C{\Rightarrow}Q$$

precondition law

C is a sufficient precondition for P to be refined by S

if and only if $C{\Rightarrow}P$ is refined by S .

postcondition law

C' is a sufficient postcondition for P to be refined by S

if and only if $C'{\Rightarrow}P$ is refined by S .

A **program** is an implemented specification.

ok	booleans
$x:= e$	numbers
if b **then** P **else** Q	characters
$P.Q$	lists

An implementable specification that is refined by a program is a program.

Recursion is allowed.

$x\ge 0 \Rightarrow x'=0 \quad \Leftarrow \quad$ **if** $x=0$ **then** ok **else** $(x:= x-1.\ \ x\ge 0 \Rightarrow x'=0)$

refinement by steps

If $A \Leftarrow$ **if** b **then** C **else** D and $C \Leftarrow E$ and $D \Leftarrow F$,

then $A \Leftarrow$ **if** b **then** E **else** F .

If $A \Leftarrow B.C$ and $B \Leftarrow D$ and $C \Leftarrow E$, then $A \Leftarrow D.E$.

If $A \Leftarrow B$ and $B \Leftarrow C$, then $A \Leftarrow C$.

refinement by parts

If $A \Leftarrow$ **if** b **then** C **else** D and $E \Leftarrow$ **if** b **then** F **else** G ,

then $A \wedge E \Leftarrow$ **if** b **then** $C \wedge F$ **else** $D \wedge G$.

If $A \Leftarrow B.C$ and $D \Leftarrow E.F$, then $A \wedge D \Leftarrow B \wedge E.\, C \wedge F$.

If $A \Leftarrow B$ and $C \Leftarrow D$, then $A \wedge C \Leftarrow B \wedge D$.

refinement by cases

$P \Leftarrow$ **if** b **then** Q **else** R

if and only if $P \Leftarrow b \wedge Q$ and $P \Leftarrow \neg b \wedge R$

List Summation

List of numbers L ; number variable s .

$s' = \Sigma L \quad \Leftarrow \quad s{:=}\ 0.\ \ n{:=}\ 0.\ \ s' = s + \Sigma\, L\, [n;..\#L]$

$s' = s + \Sigma\, L\, [n;..\#L] \quad \Leftarrow$

if $n{=}\#L$ **then** $n{=}\#L \;\Rightarrow\; s' = s + \Sigma\, L\, [n;..\#L]$

else $n{\neq}\#L \;\Rightarrow\; s' = s + \Sigma\, L\, [n;..\#L]$

$n{=}\#L \;\Rightarrow\; s' = s + \Sigma\, L\, [n;..\#L] \quad \Leftarrow \quad ok$

$n{\neq}\#L \;\Rightarrow\; s' = s + \Sigma\, L\, [n;..\#L] \quad \Leftarrow \quad s{:=}\ s{+}Ln.\ \ n{:=}\ n{+}1.\ \ s' = s + \Sigma\, L\, [n;..\#L]$

compilation

$A \Leftarrow s:=0.\ \ n:=0.\ \ B$

$B \Leftarrow \textbf{if } n=\#L \textbf{ then } C \textbf{ else } D$

$C \Leftarrow ok$

$D \Leftarrow s:=s+Ln.\ \ n:=n+1.\ \ B$

Refinement by Steps = in-line macro-expansion

$B \Leftarrow \textbf{if } n=\#L \textbf{ then } ok \textbf{ else } (s:=s+Ln.\ \ n:=n+1.\ \ B)$

translation

```
void A(void) {s = 0;  n = 0;  B( );}

void B(void) {if (n==sizeof(L)/sizeof(L[0])); else {s+=L[n];  n++;  B( );}}


s = 0;  n = 0;

B: if (n==sizeof(L)/sizeof(L[0])); else {s+=L[n];  n++;  goto B;}
```

Binary Exponentiation

Given natural variables x and y, write a program for $y' = 2^x$.

$y'=2^x \Leftarrow$ **if** $x=0$ **then** $x=0 \Rightarrow y'=2^x$ **else** $x>0 \Rightarrow y'=2^x$

$x=0 \Rightarrow y'=2^x \Leftarrow y:= 1.\ x:= 3$

$x>0 \Rightarrow y'=2^x \Leftarrow x>0 \Rightarrow y'=2^{x-1}.\ y'=2\times y$

$x>0 \Rightarrow y'=2^{x-1} \Leftarrow x'=x-1.\ y'=2^x$

$y'=2\times y \Leftarrow y:= 2\times y.\ x:= 5$

$x'=x-1 \Leftarrow x:= x-1.\ y:= 7$

Binary Exponentiation

Given natural variables x and y, write a program for $y' = 2^x$.

$A \Leftarrow$ **if** $x{=}0$ **then** B **else** C

$B \Leftarrow y{:=}\ 1.\ \ x{:=}\ 3$

$C \Leftarrow D.\ \ E$

$D \Leftarrow F.\ \ A$

$E \Leftarrow y{:=}\ 2{\times}y.\ \ x{:=}\ 5$

$F \Leftarrow x{:=}\ x{-}1.\ \ y{:=}\ 7$

$A \Leftarrow$ **if** $x{=}0$ **then** $(y{:=}\ 1.\ \ x{:=}\ 3)$ **else** $(x{:=}\ x{-}1.\ \ y{:=}\ 7.\ \ A.\ \ y{:=}\ 2{\times}y.\ \ x{:=}\ 5)$

```
int x, y;
void A (void) {if (x==0) {y = 1;  x = 3;} else {x = x–1;  y = 7;  A( );  y = 2*y;  x = 5;}}
x = 5;  A( );  printf ("%i", y);
```

Time

$\sigma \;=\; t\,;\; x\,;\; y\,;\; \ldots$

state = time variable; memory variables

t is the time at which execution starts

t' is the time at which execution ends

$t, t' : xnat$ or $xint$ or $xrat$ or $xreal$

Specification S is **implementable** if and only if

$\forall\sigma\cdot\ \exists\sigma'\cdot\ S \land t' \ge t$

real time

$t{:=}\ t+$(the time to evaluate and store e). $x{:=}\ e$

$t{:=}\ t+$(the time to evaluate b and branch). **if** b **then** P **else** Q

$t{:=}\ t+$(the time for the call and return). P

$$t' = t + f\,\sigma$$

$$t' \le t + f\,\sigma$$

$$t' \ge t + f\,\sigma$$

real time

$P \Leftarrow t{:=}\ t+1.\ \textbf{if}\ x=0\ \textbf{then}\ ok\ \textbf{else}\ (t{:=}\ t+1.\ x{:=}\ x-1.\ t{:=}\ t+1.\ P)$

is a theorem when

$P = x'=0$

$P = \textbf{if}\ x\ge 0\ \textbf{then}\ t'=t+3\times x+1\ \textbf{else}\ t'=\infty$

$P = \textbf{if}\ x\ge 0\ \textbf{then}\ x'=0 \land t'=t+3\times x+1\ \textbf{else}\ t'=\infty$

$P = x'=0 \land \textbf{if}\ x\ge 0\ \textbf{then}\ t'=t+3\times x+1\ \textbf{else}\ t'=\infty$

recursive time

- Each recursive call costs time 1.
- All else is free.

$P \Leftarrow$ **if** $x=0$ **then** ok **else** $(x:= x-1.\ \ t:= t+1.\ \ P)$

is a theorem when

$P = x'=0$

$P =$ **if** $x\ge 0$ **then** $t'=t+x$ **else** $t'=\infty$

$P =$ **if** $x\ge 0$ **then** $x'=0 \wedge t'=t+x$ **else** $t'=\infty$

$P = x'=0 \ \wedge$ **if** $x\ge 0$ **then** $t'=t+x$ **else** $t'=\infty$

Recursion can be direct or indirect.

In every loop of calls, there must be a time increment of at least one time unit.

Prove $\quad R \quad \Leftarrow \quad \textbf{if } x{=}1 \textbf{ then } ok \textbf{ else } (x{:=}\ div\ x\ 2.\ \ t{:=}\ t{+}1.\ \ R)$

where $\quad R \quad = \quad x'{=}1 \land \textbf{if } x{\ge}1 \textbf{ then } t' \le t + log\ x \textbf{ else } t'{=}\infty$

$\qquad\qquad\quad = \quad x'{=}1 \land (x{\ge}1 \ \Rightarrow\ t' \le t + log\ x) \land (x{<}1 \Rightarrow t'{=}\infty)$

use Refinement by Parts; prove:

$x'{=}1 \quad \Leftarrow \quad \textbf{if } x{=}1 \textbf{ then } ok \textbf{ else } (x{:=}\ div\ x\ 2.\ \ t{:=}\ t{+}1.\ \ x'{=}1)$

$x{\ge}1 \ \Rightarrow\ t' \le t + log\ x \quad \Leftarrow \quad \textbf{if } x{=}1 \textbf{ then } ok \textbf{ else } (x{:=}\ div\ x\ 2.\ \ t{:=}\ t{+}1.\ \ x{\ge}1 \Rightarrow t' \le t + log\ x)$

$x{<}1 \ \Rightarrow\ t'{=}\infty \quad \Leftarrow \quad \textbf{if } x{=}1 \textbf{ then } ok \textbf{ else } (x{:=}\ div\ x\ 2.\ \ t{:=}\ t{+}1.\ \ x{<}1 \Rightarrow t'{=}\infty)$

Prove $\quad R \;\Leftarrow\; \textbf{if } x{=}1 \textbf{ then } ok \textbf{ else } (x{:=}\ div\ x\ 2.\ \ t{:=}\ t{+}1.\ \ R)$

where $\quad R \;=\; x'{=}1 \wedge \textbf{if } x{\ge}1 \textbf{ then } t' \le t + log\ x \textbf{ else } t'{=}\infty$

$\qquad\qquad\quad = \; x'{=}1 \wedge (x{\ge}1 \;\Rightarrow\; t' \le t + log\ x) \wedge (x{<}1 \Rightarrow t'{=}\infty)$

use Refinement by Parts and Cases; prove:

$$x'{=}1 \;\Leftarrow\; x{=}1 \wedge ok$$

$$x'{=}1 \;\Leftarrow\; x{\ne}1 \wedge (x{:=}\ div\ x\ 2.\ \ t{:=}\ t{+}1.\ \ x'{=}1)$$

$$x{\ge}1 \;\Rightarrow\; t' \le t + log\ x \;\Leftarrow\; x{=}1 \wedge ok$$

$$x{\ge}1 \;\Rightarrow\; t' \le t + log\ x \;\Leftarrow\; x{\ne}1 \wedge (x{:=}\ div\ x\ 2.\ \ t{:=}\ t{+}1.\ \ x{\ge}1 \Rightarrow t' \le t + log\ x)$$

$$x{<}1 \;\Rightarrow\; t'{=}\infty \;\Leftarrow\; x{=}1 \wedge ok$$

$$x{<}1 \;\Rightarrow\; t'{=}\infty \;\Leftarrow\; x{\ne}1 \wedge (x{:=}\ div\ x\ 2.\ \ t{:=}\ t{+}1.\ \ x{<}1 \Rightarrow t'{=}\infty)$$

$$(x{\ge}1 \;\Rightarrow\; t' \le t + log\ x \;\;\Leftarrow\;\; x{=}1 \land x'{=}x \land t'{=}t)$$ context $x{=}1$ and $t'{=}t$

$$= \quad (1{\ge}1 \;\Rightarrow\; t \le t + log\ 1 \;\;\Leftarrow\;\; x{=}1 \land x'{=}x \land t'{=}t)$$ simplify

$$= \quad (\top \;\;\Leftarrow\;\; x{=}1 \land x'{=}x \land t'{=}t)$$ base law

$$= \quad \top$$

$$(\underline{x\geq 1} \;\Rightarrow\; \underline{t' \leq t + log\ x} \;\Leftarrow\; \underline{x\neq 1 \wedge (div\ x\ 2 \geq 1 \;\Rightarrow\; t' \leq t + 1 + log\ (div\ x\ 2))})$$

portation

$$= \quad x\neq 1 \wedge (div\ x\ 2 \geq 1 \;\Rightarrow\; t' \leq t + 1 + log\ (div\ x\ 2)) \wedge x\geq 1 \;\Rightarrow\; t' \leq t + log\ x$$

simplify

$$= \quad \underline{x>1} \wedge (\underline{x>1} \;\Rightarrow\; \underline{t' \leq t + 1 + log\ (div\ x\ 2)}) \;\Rightarrow\; t' \leq t + log\ x$$

discharge

$$= \quad x>1 \;\wedge\; t' \leq t + 1 + log\ (div\ x\ 2) \;\Rightarrow\; t' \leq t + log\ x$$

portation

$$= \quad x>1 \;\Rightarrow\; (t' \leq t + 1 + log\ (div\ x\ 2) \;\Rightarrow\; t' \leq t + log\ x)$$

Connection Law $t'\leq a \Rightarrow t'\leq b \;\Leftarrow\; a\leq b$

$$\Leftarrow \quad x>1 \;\Rightarrow\; t + 1 + log\ (div\ x\ 2) \;\leq\; t + log\ x$$

subtract $t+1$ from each side

$$= \quad x>1 \;\Rightarrow\; log\ (div\ x\ 2) \;\leq\; log\ x - 1$$

property of log

$$= \quad x>1 \;\Rightarrow\; log\ (div\ x\ 2) \;\leq\; log\ (x/2)$$

log is monotonic for $x>0$

$$\Leftarrow \quad div\ x\ 2 \leq x/2$$

$$= \quad \top$$

$$(x{<}1 \Rightarrow t'{=}\infty \;\;\Leftarrow\;\; x{=}1 \;\wedge\; x'{=}x \;\wedge\; t'{=}t)$$ portation

$$= \quad x{<}1 \wedge x{=}1 \;\wedge\; x'{=}x \;\wedge\; t'{=}t \;\;\Rightarrow\;\; t'{=}\infty$$ generic, base

$$= \quad \bot \;\;\Rightarrow\;\; t'{=}\infty$$ base

$$= \quad \top$$

$$(x{<}1 \Rightarrow t'{=}\infty \quad \Leftarrow \quad x{\neq}1 \ \land \ (div\ x\ 2 < 1 \ \Rightarrow \ t'{=}\infty)) \qquad \text{portation}$$

$$= \quad x{<}1 \land x{\neq}1 \land (div\ x\ 2 < 1 \ \Rightarrow \ t'{=}\infty) \ \ \Rightarrow \ \ t'{=}\infty \qquad \text{discharge}$$

$$= \quad x{<}1 \land t'{=}\infty \ \ \Rightarrow \ \ t'{=}\infty \qquad \text{specialization}$$

$$= \quad \top$$

Termination

$x'=2 \quad \Leftarrow \quad t:= t+1.\ x'=2$

complain only if $x' \neq 2$

$x'=2 \ \land \ t'<\infty$

unimplementable

$x'=2 \land (t<\infty \Rightarrow t'<\infty) \quad \Leftarrow \quad t:= t+1.\ x'=2 \land (t<\infty \Rightarrow t'<\infty)$

complain only if $x' \neq 2 \ \lor \ t<\infty \land t'=\infty$

$x'=2 \land t' \le t+1 \quad \Leftarrow \quad t:= t+1.\ x'=2 \land t' \le t+1$ X

$x'=2 \land t' \le t+1 \quad \Leftarrow \quad x:= 2$

Linear Search

Find the first occurrence of item x in list L . The execution time must be linear in $\#L$.

$$\neg\, x{:}\ L\,(0,..h') \ \wedge\ (Lh'=x \vee h'=\#L)$$

$$[\ ?\ ;\ ?\ ;\ ?\ ;\ ?\ ;\ x\ ;\ ?\ ;\ ?\ ;\ ?\ ;\ ?\ ]$$

$0 \leftarrow$ x is not in this part $\rightarrow h'$ $\qquad\qquad$ $\#L$

Linear Search

Find the first occurrence of item x in list L. The execution time must be linear in $\#L$.

$$\neg\, x{:}\, L\,(0,..h') \;\wedge\; (Lh'{=}x \vee h'{=}\#L) \;\Longleftarrow\; h{:=}\,0.\; h{\le}\#L \Rightarrow \neg\, x{:}\, L\,(h,..h') \;\wedge\; (Lh'{=}x \vee h'{=}\#L)$$

$$h{\le}\#L \Rightarrow \neg\, x{:}\, L\,(h,..h') \;\wedge\; (Lh'{=}x \vee h'{=}\#L) \;\Longleftarrow$$

$$\textbf{if } h{=}\#L \textbf{ then } ok \textbf{ else } h{<}\#L \Rightarrow \neg\, x{:}\, L\,(h,..h') \;\wedge\; (Lh'{=}x \vee h'{=}\#L)$$

$$h{<}\#L \Rightarrow \neg\, x{:}\, L\,(h,..h') \;\wedge\; (Lh'{=}x \vee h'{=}\#L) \;\Longleftarrow$$

$$\textbf{if } Lh{=}x \textbf{ then } ok \textbf{ else } (h{:=}\,h{+}1.\; h{\le}\#L \Rightarrow \neg\, x{:}\, L\,(h,..h') \;\wedge\; (Lh'{=}x \vee h'{=}\#L))$$

Linear Search

timing

$$t' \le t+\#L \quad \Leftarrow \quad h:=0.\ \ h\le\#L \ \Rightarrow\ t' \le t+\#L-h$$

$$h\le\#L \ \Rightarrow\ t' \le t+\#L-h \quad \Leftarrow \quad \textbf{if}\ h=\#L\ \textbf{then}\ ok\ \textbf{else}\ h<\#L \ \Rightarrow\ t' \le t+\#L-h$$

$$h<\#L \ \Rightarrow\ t' \le t+\#L-h \quad \Leftarrow \quad \textbf{if}\ Lh=x\ \textbf{then}\ ok\ \textbf{else}\ (h:=h+1.\ \ t:=t+1.\ \ h\le\#L \ \Rightarrow\ t' \le t+\#L-h)$$

	$h:=h+1.\ \ t:=t+1.\ \ h\le\#L \ \Rightarrow\ t' \le t+\#L-h$	substitution law
$=$	$h:=h+1.\ \ h\le\#L \ \Rightarrow\ t' \le t+1+\#L-h$	substitution law
$=$	$h+1\le\#L \ \Rightarrow\ t' \le t+1+\#L-h-1$	simplify
$=$	$h<\#L \ \Rightarrow\ t' \le t+\#L-h$	

Linear Search

Find the first occurrence of item x in list L . The execution time must be linear in $\#L$.

nonempty

$$\neg\ x{:}\ L\,(0,..h')\ \wedge\ (Lh'{=}x \vee h'{=}\#L)\ \Leftarrow\ h{:=}\,0.\ \ h{\le}\#L \Rightarrow \neg\ x{:}\ L\,(h,..h')\ \wedge\ (Lh'{=}x \vee h'{=}\#L)$$

<

$$h{\le}\#L \Rightarrow \neg\ x{:}\ L\,(h,..h')\ \wedge\ (Lh'{=}x \vee h'{=}\#L)\ \Leftarrow$$

$$\textbf{if}\ h{=}\#L\ \textbf{then}\ ok\ \textbf{else}\ h{<}\#L \Rightarrow \neg\ x{:}\ L\,(h,..h')\ \wedge\ (Lh'{=}x \vee h'{=}\#L)$$

$$h{<}\#L \Rightarrow \neg\ x{:}\ L\,(h,..h')\ \wedge\ (Lh'{=}x \vee h'{=}\#L)\ \Leftarrow$$

$$\textbf{if}\ Lh{=}x\ \textbf{then}\ ok\ \textbf{else}\ (h{:=}\,h{+}1.\ \ h{\le}\#L \Rightarrow \neg\ x{:}\ L\,(h,..h')\ \wedge\ (Lh'{=}x \vee h'{=}\#L))$$

Binary Search

Find an occurrence of item x in nonempty sorted list L .

The execution time must be logarithmic in $\#L$.

$(x{:}\ L\ (0,..\#L)\ =\ p' \ \ \Longrightarrow\ \ Lh' = x) \ \ \Longleftarrow\ \ h{:=}\ 0.\ \ j{:=}\ \#L.\ \ h{<}j \Rightarrow R$

$h{<}j \Rightarrow R \ \ \Longleftarrow\ \ \textbf{if}\ j{-}h = 1\ \textbf{then}\ p{:=}\ Lh{=}x\ \textbf{else}\ j{-}h{\ge}2 \Rightarrow R$

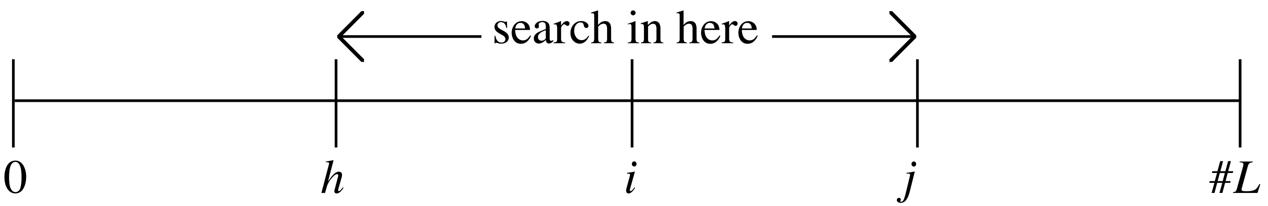
$j{-}h{\ge}2 \Rightarrow R \ \ \Longleftarrow\ \ \ j{-}h{\ge}2\ \ \Rightarrow\ \ h'{=}h{<}i'{<}j{=}j'.$

$\qquad\qquad \textbf{if}\ Li{\le}x\ \textbf{then}\ h{:=}\ i\ \textbf{else}\ j{:=}\ i.$

$\qquad\qquad h{<}j \Rightarrow R$

$j{-}h{\ge}2\ \ \Rightarrow\ \ h'{=}h{<}i'{<}j{=}j' \ \ \Longleftarrow\ \ \ i{:=}\ div\ (h{+}j)\ 2$

Define $R\ =\ (x{:}\ L\ (h,..j)\ =\ p' \ \ \Longrightarrow\ \ Lh' = x)$



$$T \Leftarrow h{:=}\,0.\;\; j{:=}\,\#L.\;\; U$$

$$U \Leftarrow \textbf{if } j{-}h = 1 \textbf{ then } p{:=}\, Lh{=}x \textbf{ else } V$$

$$V \Leftarrow i{:=}\, div\,(h{+}j)\,2.$$

$$\textbf{if } Li{\le}x \textbf{ then } h{:=}\,i \textbf{ else } j{:=}\,i.$$

$$t{:=}\,t{+}1.\;\; U$$

$\#L$	=	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$t'{-}t$	=	0	1	2	2	3	3	3	3	4	4	4	4	4	4	4	4	5	5

$$T = t' \le t + ceil\,(log\,(\#L))$$

$$U = h{<}j \Rightarrow t' \le t + ceil\,(log\,(j{-}h))$$

$$V = j{-}h{\ge}2 \Rightarrow t' \le t + ceil\,(log\,(j{-}h))$$

Three Levels of Care

highest write all specifications

prove all refinements (an automated theorem prover can help)

middle write all specifications

but don't prove the refinements (just argue them informally)

lowest don't bother with specifications

don't bother with refinements

just write code

Fast Exponentiation

Given rational variables x and z and natural variable y, write a program for $z' = x^y$ that runs fast without using exponentiation.

$z'=x^y \quad \Leftarrow \quad z:= 1.\ \ z' = z \times x^y$

Proof:	$z:= 1.\ \ z' = z \times x^y$	Substitution Law
$=$	$z' = 1 \times x^y$	1 is identity for $\times$
$=$	$z' = x^y$	

Fast Exponentiation

Given rational variables x and z and natural variable y, write a program for $z' = x^y$ that runs fast without using exponentiation.

$z'=x^y \quad \Leftarrow \quad z:= 1.\ z' = z\times x^y$

$z' = z\times x^y \quad \Leftarrow \quad$ **if** $y=0$ **then** ok **else** $y>0 \Rightarrow z' = z\times x^y$

Proof:	$y=0 \wedge ok$	expand ok
$=$	$y=0 \wedge x'=x \wedge y'=y \wedge z'=z$	specialize, 1 is identity for $\times$
$\Rightarrow$	$y=0 \wedge z' = z\times 1$	$x^0=1$
$=$	$y=0 \wedge z' = z\times x^0$	context $y=0$ and specialize
$\Rightarrow$	$z' = z\times x^y$	

Fast Exponentiation

Given rational variables x and z and natural variable y, write a program for $z' = x^y$ that runs fast without using exponentiation.

$z'=x^y \;\Leftarrow\; z:= 1.\; z' = z\times x^y$

$z' = z\times x^y \;\Leftarrow\;$ **if** $y=0$ **then** ok **else** $y>0 \Rightarrow z' = z\times x^y$

$y>0 \Rightarrow z' = z\times x^y \;\Leftarrow\; z:= z\times x.\; y:= y-1.\; z' = z\times x^y$

Proof:	$(y>0 \Rightarrow z' = z\times x^y \;\Leftarrow\; z:= z\times x.\; y:= y-1.\; z' = z\times x^y)$	portation
$=$	$z' = z\times x^y \Leftarrow y>0 \wedge (z:= z\times x.\; y:= y-1.\; z' = z\times x^y)$	Substitution Law twice
$=$	$z' = z\times x^y \Leftarrow y>0 \wedge z' = z\times x\times x^{y-1}$	Law of Exponents
$=$	$z' = z\times x^y \Leftarrow y>0 \wedge z' = z\times x^y$	specialize
$=$	$\top$	

Fast Exponentiation

Given rational variables x and z and natural variable y, write a program for $z' = x^y$ that runs fast without using exponentiation.

$z'=x^y \quad \Leftarrow \quad z:= 1.\ \ z' = z\times x^y$

$z' = z\times x^y \quad \Leftarrow \quad$ **if** $y=0$ **then** ok **else** $y>0 \Rightarrow z' = z\times x^y$

$y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad \cancel{z:= z\times x.\ \ y:= y-1.\ \ z' = z\times x^y}$

if $even\ y$ **then** $even\ y \wedge y>0 \Rightarrow z' = z\times x^y$ **else** $odd\ y \Rightarrow z' = z\times x^y$

$even\ y \wedge y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad x:= x\times x.\ \ y:= y/2.\ \ z' = z\times x^y$

Proof: $(even\ y \wedge y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad x:= x\times x.\ \ y:= y/2.\ \ z' = z\times x^y)$ portation

$=$ $z' = z\times x^y \ \Leftarrow\ even\ y \wedge y>0 \wedge (x:= x\times x.\ \ y:= y/2.\ \ z' = z\times x^y)$ Substitution Law twice

$=$ $z' = z\times x^y \ \Leftarrow\ even\ y \wedge y>0 \wedge z' = z\times (x\times x)^{y/2}$ Law of Exponents

$=$ $z' = z\times x^y \ \Leftarrow\ even\ y \wedge y>0 \wedge z' = z\times x^y$ specialize

$=$ $\top$

Fast Exponentiation

Given rational variables x and z and natural variable y, write a program for $z' = x^y$ that runs fast without using exponentiation.

$z'=x^y \quad \Leftarrow \quad z:= 1.\ \ z' = z\times x^y$

$z' = z\times x^y \quad \Leftarrow \quad$ **if** $y=0$ **then** ok **else** $y>0 \Rightarrow z' = z\times x^y$

$y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad \cancel{z:= z\times x.\ \ y:= y-1.\ \ z' = z\times x^y}$

if $even\ y$ **then** $even\ y \wedge y>0 \Rightarrow z' = z\times x^y$ **else** $odd\ y \Rightarrow z' = z\times x^y$

$even\ y \wedge y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad x:= x\times x.\ \ y:= y/2.\ \ z' = z\times x^y$

$odd\ y \Rightarrow z' = z\times x^y \quad \Leftarrow \quad z:= z\times x.\ \ y:= y-1.\ \ z' = z\times x^y$

Fast Exponentiation

Given rational variables x and z and natural variable y, write a program for $z' = x^y$ that runs fast without using exponentiation.

$z'=x^y \quad \Leftarrow \quad z:= 1.\ \ z' = z \times x^y$

$z' = z \times x^y \quad \Leftarrow \quad$ **if** $y=0$ **then** ok **else** $y>0 \Rightarrow z' = z \times x^y$

$y>0 \Rightarrow z' = z \times x^y \quad \Leftarrow \quad \cancel{z:= z \times x.\ \ y:= y-1.\ \ z' = z \times x^y}$

if $even\ y$ **then** $even\ y \wedge y>0 \Rightarrow z' = z \times x^y$ **else** $odd\ y \Rightarrow z' = z \times x^y$

$even\ y \wedge y>0 \Rightarrow z' = z \times x^y \quad \Leftarrow \quad x:= x \times x.\ \ y:= y/2.\ \ \cancel{z' = z \times x^y}\ \ y>0 \Rightarrow z' = z \times x^y$

$odd\ y \Rightarrow z' = z \times x^y \quad \Leftarrow \quad z:= z \times x.\ \ y:= y-1.\ \ z' = z \times x^y$

Fast Exponentiation

Given rational variables x and z and natural variable y, write a program for $z' = x^y$ that runs fast without using exponentiation.

$z'=x^y \;\Leftarrow\; z:= 1.\; z' = z\times x^y$

$z' = z\times x^y \;\Leftarrow\;$ **if** $y=0$ **then** ok **else** $y>0 \Rightarrow z' = z\times x^y$

$y>0 \Rightarrow z' = z\times x^y \;\Leftarrow\; \cancel{z:= z\times x.\; y:= y-1.\; z' = z\times x^y}$

if $even\ y$ **then** $even\ y \wedge y>0 \Rightarrow z' = z\times x^y$ **else** $odd\ y \Rightarrow z' = z\times x^y$

$even\ y \wedge y>0 \Rightarrow z' = z\times x^y \;\Leftarrow\; x:= x\times x.\; y:= y/2.\; \cancel{z' = z\times x^y}\; y>0 \Rightarrow z' = z\times x^y$

$odd\ y \Rightarrow z' = z\times x^y \;\Leftarrow\; z:= z\times x.\; y:= y-1.\; \cancel{z' = z\times x^y}\; even\ y \Rightarrow z' = z\times x^y$

$even\ y \Rightarrow z' = z\times x^y \;\Leftarrow\;$ **if** $y = 0$ **then** ok **else** $even\ y \wedge y>0 \Rightarrow z' = z\times x^y$

Fast Exponentiation

Given rational variables x and z and natural variable y, write a program for $z' = x^y$ that runs fast without using exponentiation.

$z'=x^y \quad \Leftarrow \quad z:= 1.\ z' = z\times x^y$

$z' = z\times x^y \quad \Leftarrow \quad \cancel{\textbf{if } y=0 \textbf{ then } ok \textbf{ else } y>0 \Rightarrow z' = z\times x^y}$

$\qquad\qquad \textbf{if } even\ y \textbf{ then } even\ y \Rightarrow z' = z\times x^y \textbf{ else } odd\ y \Rightarrow z' = z\times x^y$

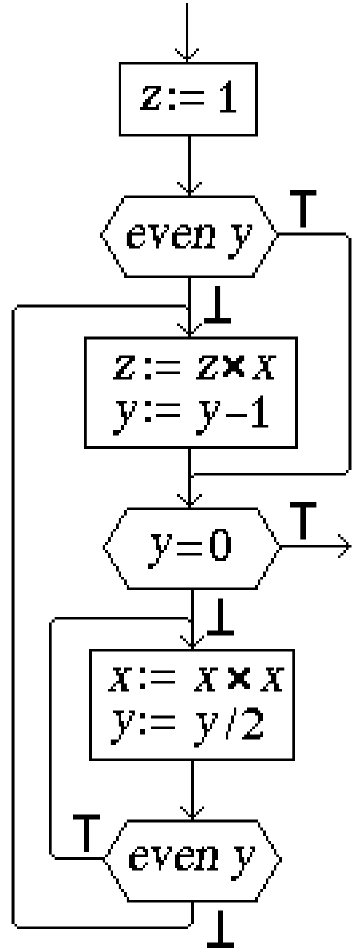
$y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad \cancel{z:= z\times x.\ y:= y-1.\ z' = z\times x^y}$

$\qquad\qquad \textbf{if } even\ y \textbf{ then } even\ y \land y>0 \Rightarrow z' = z\times x^y \textbf{ else } odd\ y \Rightarrow z' = z\times x^y$

$even\ y \land y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad x:= x\times x.\ y:= y/2.\ \cancel{z' = z\times x^y}\ y>0 \Rightarrow z' = z\times x^y$

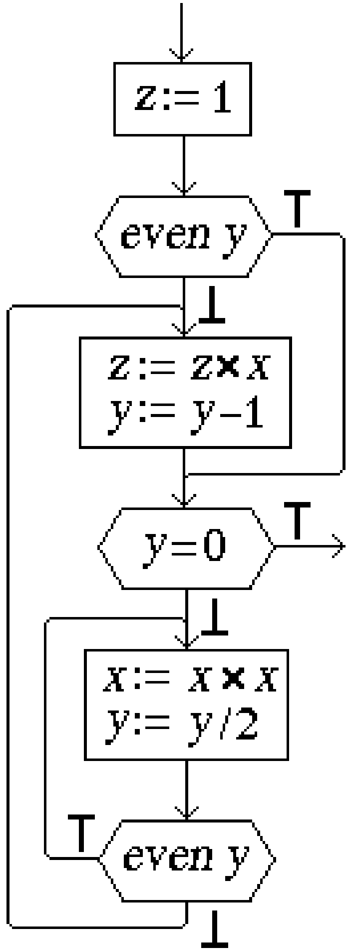
$odd\ y \Rightarrow z' = z\times x^y \quad \Leftarrow \quad z:= z\times x.\ y:= y-1.\ \cancel{z' = z\times x^y}\ even\ y \Rightarrow z' = z\times x^y$

$even\ y \Rightarrow z' = z\times x^y \quad \Leftarrow \quad \textbf{if } y = 0 \textbf{ then } ok \textbf{ else } even\ y \land y>0 \Rightarrow z' = z\times x^y$



$$even\ y \land y{>}0 \Rightarrow z' = z{\times}x^y \quad \Longleftarrow \quad x{:=}\ x{\times}x.\ \ y{:=}\ y/2.\ \ t{:=}\ t{+}1.\ \ y{>}0 \Rightarrow z' = z{\times}x^y$$

y	=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$t'–t$	=	0	0	1	1	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4



$$even\ y \land y>0 \Rightarrow z' = z \times x^y \quad \Leftarrow \quad x := x \times x.\ \ y := y/2.\ \ t := t+1.\ \ y>0 \Rightarrow z' = z \times x^y$$

if $y=0$ **then** $t'=t$ **else** $t' = t + floor\ (log\ y)$

if $y=0$ **then** $t'=t$ **else** $t' \le t + log\ y$

Fibonacci Numbers

$$fib\ 0 \ = \ 0$$

$$fib\ 1 \ = \ 1$$

$$fib\ (n+2) \ = \ fib\ n + fib\ (n+1)$$

$$fib \ = \ 0 \to 0 \ \mid \ 1 \to 1 \ \mid \ \langle n\colon nat+2 \to fib(n-2) + fib(n-1)\rangle$$

$$fib \ = \ \langle n\colon nat \to \mathbf{if}\ n<2\ \mathbf{then}\ n\ \mathbf{else}\ fib(n-2) + fib(n-1)\rangle$$

Fibonacci Numbers

$$x' = fib\ n \ \Longleftarrow\ x' = fib\ n \ \wedge\ y' = fib\ (n+1) \ = \ P$$

$$P \ \Longleftarrow\ \textbf{if } n=0 \textbf{ then } (x{:=}\ 0.\ \ y{:=}\ 1) \textbf{ else } (n{:=}\ n{-}1.\ \ P.\ \ x'{=}y\ \wedge\ y'{=}x{+}y)$$

we have these x y

… f f f f f f f f f f f f f f f f …

we want these x' y'

Fibonacci Numbers

$$x' = fib\ n \;\; \Leftarrow \;\; x' = fib\ n \;\wedge\; y' = fib\ (n+1) \;\; = \;\; P$$

$$P \;\; \Leftarrow \;\; \textbf{if}\ n{=}0\ \textbf{then}\ (x{:=}\ 0.\ \ y{:=}\ 1)\ \textbf{else}\ (n{:=}\ n{-}1.\ \ P.\ \ x'{=}y \;\wedge\; y'{=}x{+}y)$$

$$x'{=}y \;\wedge\; y'{=}x{+}y \;\; \Leftarrow \;\; n{:=}\ x.\ \ x{:=}\ y.\ \ y{:=}\ n{+}y$$

$$t'{=}t{+}n \;\; \Leftarrow \;\; \textbf{if}\ n{=}0\ \textbf{then}\ (x{:=}\ 0.\ \ y{:=}\ 1)\ \textbf{else}\ (n{:=}\ n{-}1.\ \ t{:=}\ t{+}1.\ \ t'{=}t{+}n.\ \ t'{=}t)$$

$$t'{=}t \;\; \Leftarrow \;\; n{:=}\ x.\ \ x{:=}\ y.\ \ y{:=}\ n{+}y$$

Fibonacci Numbers

$$fib(2\times k+1) \;=\; fib\ k^{\,2} + fib(k+1)^{\,2}$$

$$fib(2\times k+2) \;=\; 2 \times fib\ k \times fib(k+1) \;+\; fib(k+1)^{\,2}$$

$$P \;\Leftarrow\; \textbf{if } n{=}0 \textbf{ then } (x{:=}\ 0.\ \ y{:=}\ 1)$$
$$\textbf{else if } even\ n \textbf{ then } even\ n \wedge n{>}0 \Rightarrow P$$
$$\textbf{else } odd\ n \Rightarrow P$$

$$odd\ n \Rightarrow P \;\Leftarrow\; n{:=}\ (n-1)/2.\ \ P.\ \ x' = x^2 + y^2 \;\wedge\; y' = 2\times x\times y + y^2$$

$$even\ n \wedge n{>}0 \Rightarrow P \;\Leftarrow\; n{:=}\ n/2 - 1.\ \ P.\ \ x' = 2\times x\times y + y^2 \;\wedge\; y' = x^2 + y^2 + x'$$

$$x' = x^2 + y^2 \;\wedge\; y' = 2\times x\times y + y^2 \;\Leftarrow\; n{:=}\ x.\ \ x{:=}\ x^2 + y^2.\ \ y{:=}\ 2\times n\times y + y^2$$

$$x' = 2\times x\times y + y^2 \wedge\; y' = x^2 + y^2 + x' \;\Leftarrow\; n{:=}\ x.\ \ x{:=}\ 2\times x\times y + y^2.\ \ y{:=}\ n^2 + y^2 + x$$

Fibonacci Numbers

$T \;=\; t' \le t + log\,(n+1)$

$T \;\Leftarrow\;$ **if** $n=0$ **then** $(x{:=}\,0.\;\; y{:=}\,1)$

else if $even\ n$ **then** $even\ n \land n>0 \Rightarrow T$

else $odd\ n \Rightarrow T$

$odd\ n \Rightarrow T \;\Leftarrow\; n{:=}\,(n-1)/2.\;\; t{:=}\,t+1.\;\; T.\;\; t'=t$

$even\ n \land n>0 \Rightarrow T \;\Leftarrow\; n{:=}\,n/2-1.\;\; t{:=}\,t+1.\;\; T.\;\; t'=t$

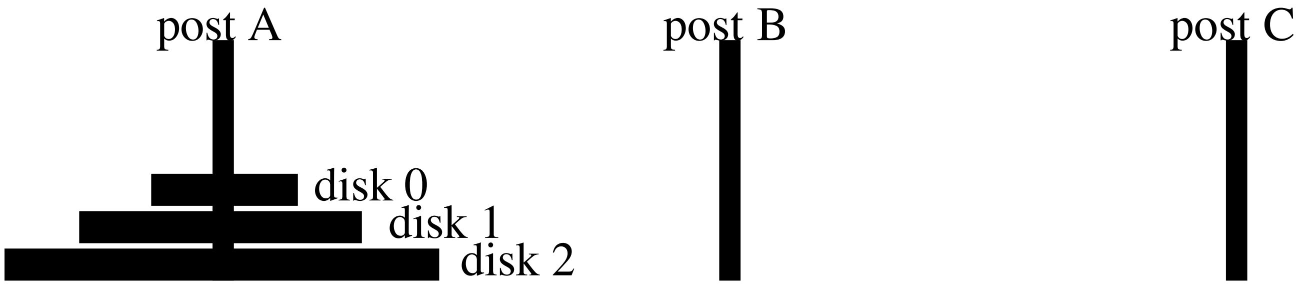
$t'=t \;\Leftarrow\; n{:=}\,x.\;\; x{:=}\,x^2+y^2.\;\; y{:=}\,2\times n\times y+y^2$

$t'=t \;\Leftarrow\; n{:=}\,x.\;\; x{:=}\,2\times x\times y+y^2.\;\; y{:=}\,n^2+y^2+x$

Fibonacci Numbers

```
void P (void)
{	if (n==0) {x = 0;  y = 1;}
	else if (n%2==0) {n = n / 2 – 1;  P();  n = x;  x = 2*x*y + y*y;  y = n*n + y*y + x;}
	else {n = (n–1) / 2;  P();  n = x;  x = x*x + y*y;  y = 2*n*y + y*y;}
}
```

Towers of Hanoi



Towers of Hanoi

MovePile from to using $\Leftarrow$

if n=0 **then** *ok*

else (n:= n–1.

MovePile from using to.

MoveDisk from to.

MovePile using to from.

n:= n+1)

Towers of Hanoi — time

$t := t + 2^n - 1 \;\Leftarrow$

if $n=0$ **then** ok

else ($n := n-1$.

$t := t + 2^n - 1$.

$t := t+1$.

$t := t + 2^n - 1$.

$n := n+1$)

Towers of Hanoi — space

$s'=s \Leftarrow$

if $n=0$ **then** ok

else ($n:= n-1$.

$s:= s+1$. $s'=s$. $s:= s-1$.

ok.

$s:= s+1$. $s'=s$. $s:= s-1$.

$n:= n+1$)

Towers of Hanoi — maximum space

$m{\ge}s \Rightarrow (m{:=}\ max\ m\ (s{+}n)) \ \Leftarrow$

if $n{=}0$ **then** ok

else ($n{:=}\ n{-}1.$

$s{:=}\ s{+}1.\ \ m{:=}\ max\ m\ s.\ \ m{\ge}s \Rightarrow (m{:=}\ max\ m\ (s{+}n)).\ \ s{:=}\ s{-}1.$

$ok.$

$s{:=}\ s{+}1.\ \ m{:=}\ max\ m\ s.\ \ m{\ge}s \Rightarrow (m{:=}\ max\ m\ (s{+}n)).\ \ s{:=}\ s{-}1.$

$n{:=}\ n{+}1$)

Towers of Hanoi — average space

$p:= p + s\times(2^n - 1) + (n-2)\times 2^n + 2 \;\Longleftarrow$

if $n=0$ **then** ok

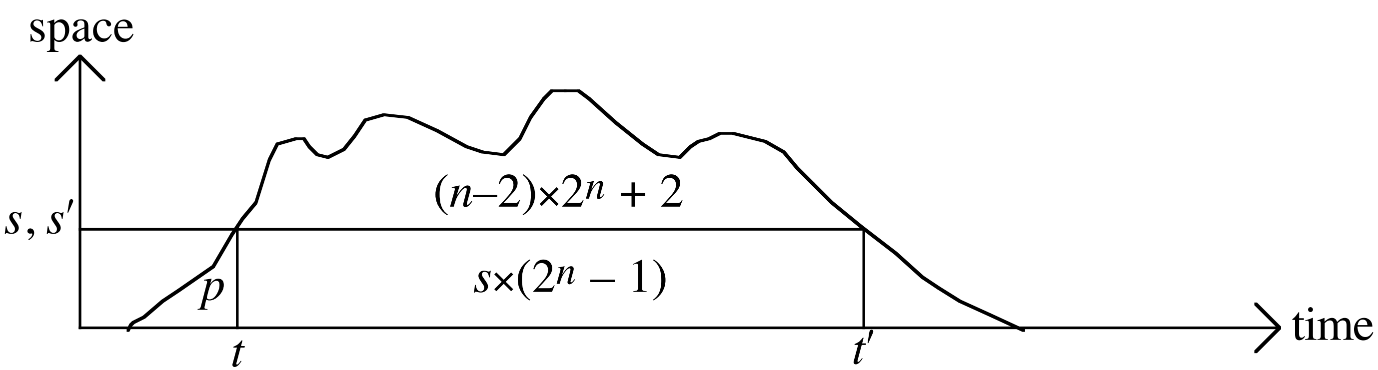
else ($n:= n-1$.

$s:= s+1$. $p:= p + s\times(2^n - 1) + (n-2)\times 2^n + 2$. $s:= s-1$.

$p:= p+s$.

$s:= s+1$. $p:= p + s\times(2^n - 1) + (n-2)\times 2^n + 2$. $s:= s-1$.

$n:= n+1$)



Towers of Hanoi — average space

$p:= p + s×(2^n – 1) + (n–2)×2^n + 2 \Longleftarrow$

if $n=0$ **then** ok

else ($n:= n–1$.

$s:= s+1$. $p:= p + s×(2^n – 1) + (n–2)×2^n + 2$. $s:= s–1$.

$p:= p+s$.

$s:= s+1$. $p:= p + s×(2^n – 1) + (n–2)×2^n + 2$. $s:= s–1$.

$n:= n+1$)

average space $= ((n–2)×2^n + 2) / (2^n – 1)$

$= n + n/(2^n – 1) – 2$

Easier: $p' \le p + (s+n)×(2^n–1)$

average space $\le n$

Towers of Hanoi

$$
\begin{array}{l}
\textit{MovePile} \Leftarrow \\
\quad \textbf{if } n{=}0 \textbf{ then } ok \\
\quad \textbf{else } (\ n{:=}\ n{-}1.\\
\qquad s{:=}\ s{+}1.\ \ m{:=}\ \mathit{max}\ m\ s.\ \ \textit{MovePile}.\ \ s{:=}\ s{-}1.\\
\qquad t{:=}\ t{+}1.\ \ p{:=}\ p{+}s.\ \ ok.\\
\qquad s{:=}\ s{+}1.\ \ m{:=}\ \mathit{max}\ m\ s.\ \ \textit{MovePile}.\ \ s{:=}\ s{-}1.\\
\qquad n{:=}\ n{+}1\ )
\end{array}
$$

$$
\begin{array}{lll}
\textit{MovePile} = & & n'{=}n \\
& \land & t' = t + 2^n - 1 \\
& \land & s'{=}s \\
& \land & (m{\ge}s \Rightarrow m' = \mathit{max}\ m\ (s{+}n)) \\
& \land & p' = p + s{\times}(2^n - 1) + (n{-}2){\times}2^n + 2
\end{array}
$$