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.

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.

$z'=x^y \quad \Leftarrow$

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.

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

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.

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

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

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.

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

Proof: $z:= 1.\; z' = z\times x^y$ Substitution Law

$=$ $z' = 1\times x^y$

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.

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

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

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.

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

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.

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

$z' = z\times x^y \quad \Leftarrow$

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** $y=0$

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*

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

Proof: $y=0 \wedge ok$

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.

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

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

Proof: $y=0 \wedge ok$ expand ok

$= \quad y=0 \wedge x'=x \wedge y'=y \wedge z'=z$

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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

Proof: $y=0 \wedge ok$ — expand ok

$=$ $y=0 \wedge x'=x \wedge y'=y \wedge z'=z$ — specialize, 1 is identity for ×

$\Rightarrow$ $y=0 \wedge z' = z \times 1$

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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** $y>0 \Rightarrow z' = z{\times}x^y$ **fi**

Proof: $y=0 \land ok$ — expand *ok*

$=\quad y=0 \land x'=x \land y'=y \land z'=z$ — specialize, 1 is identity for ×

$\Rightarrow\quad y=0 \land z' = z{\times}1$ — $x^0=1$

$=\quad y=0 \land z' = z{\times}x^0$ — context $y=0$ and specialize

$\Rightarrow\quad z' = z{\times}x^y$

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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

$y>0 \Rightarrow z' = z \times x^y \Leftarrow$

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

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

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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** $y{>}0 \Rightarrow z' = z\times x^y$ **fi**

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

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

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

Proof: $(y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad z:= z\times x.\ \ y:= y-1.\ \ z' = z\times x^y)$ portation

$=$ $z' = z\times x^y \ \Leftarrow\ y>0 \wedge (z:= z\times x.\ \ y:= y-1.\ \ z' = z\times x^y)$

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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

$=$ $z' = z\times x^y \;\Leftarrow\; y>0 \wedge z' = z\times x\times x^{y-1}$

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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

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

Proof: $(y>0 \Rightarrow z' = z \times x^y \Leftarrow z:= z \times x.\ y:= y-1.\ z' = z \times x^y)$ portation

$= \quad z' = z \times x^y \Leftarrow y>0 \wedge (z:= z \times x.\ y:= y-1.\ z' = z \times x^y)$ Substitution Law twice

$= \quad z' = z \times x^y \Leftarrow y>0 \wedge z' = z \times x \times x^{y-1}$ Law of Exponents

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

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

Proof: $(y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad z:= z\times x.\ y:= y-1.\ z' = z\times x^y)$ portation

$=$ $z' = z\times x^y \ \Leftarrow\ y>0 \land (z:= z\times x.\ y:= y-1.\ z' = z\times x^y)$ Substitution Law twice

$=$ $z' = z\times x^y \ \Leftarrow\ y>0 \land z' = z\times x\times x^{y-1}$ Law of Exponents

$=$ $z' = z\times x^y \ \Leftarrow\ y>0 \land z' = z\times x^y$ 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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

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

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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

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

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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

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

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

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

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

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.

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

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

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

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

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

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

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

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** $y>0 \Rightarrow z' = z{\times}x^y$ **fi**

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

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

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

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

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

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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

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

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

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

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.

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

$z' = z \times x^y \;\Longleftarrow\; \textbf{if } y=0 \textbf{ then } ok \textbf{ else } y>0 \Rightarrow z' = z \times x^y \textbf{ fi}$

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

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

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

Proof: $(even\ y \wedge y>0 \Rightarrow z' = z \times x^y \;\Longleftarrow\; x:= x \times x.\;\; y:= y/2.\;\; z' = z \times x^y)$ 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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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

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

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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

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

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

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

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

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** $y>0 \Rightarrow z' = z \times x^y$ **fi**

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

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

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

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

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** $y>0 \Rightarrow z' = z{\times}x^y$ **fi**

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

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

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

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

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.

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

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

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

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

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

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

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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

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

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

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.

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

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

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

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

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

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

even $y \Rightarrow z' = z\times x^y \quad \Leftarrow$

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

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

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

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

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

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

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** $y>0 \Rightarrow z' = z\times x^y$ **fi**

↑

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

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

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

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

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

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.

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

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

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

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

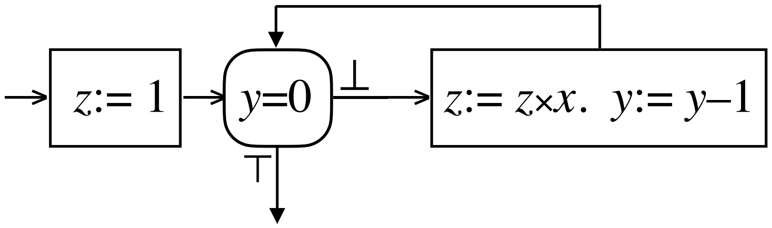
if *even* y **then** *even* $y \wedge y>0 \Rightarrow z' = z\times x^y$ **else** *odd* $y \Rightarrow z' = z\times x^y$ **fi**

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

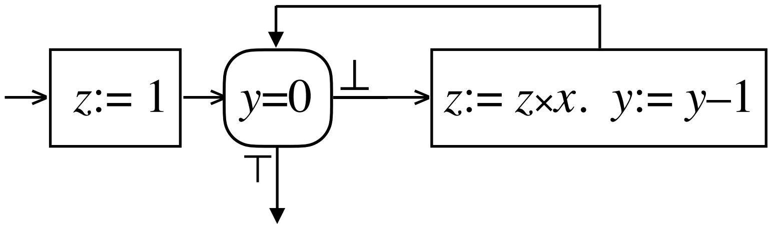
odd $y \Rightarrow z' = z\times x^y \quad \Leftarrow \quad z:= z\times x.\ \ y:= y-1.$ ~~$z' = z\times x^y$~~ *even* $y \Rightarrow z' = z\times x^y$

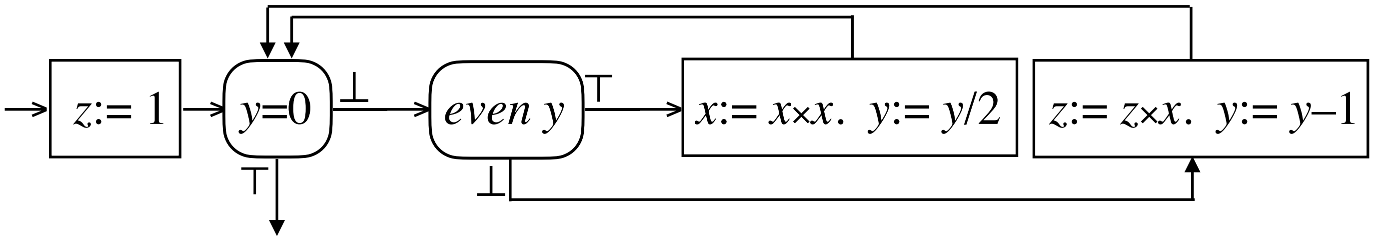
even $y \Rightarrow z' = z\times x^y \quad \Leftarrow$ **if** $y = 0$ **then** *ok* **else** *even* $y \wedge y>0 \Rightarrow z' = z\times x^y$ **fi**

Fast Exponentiation

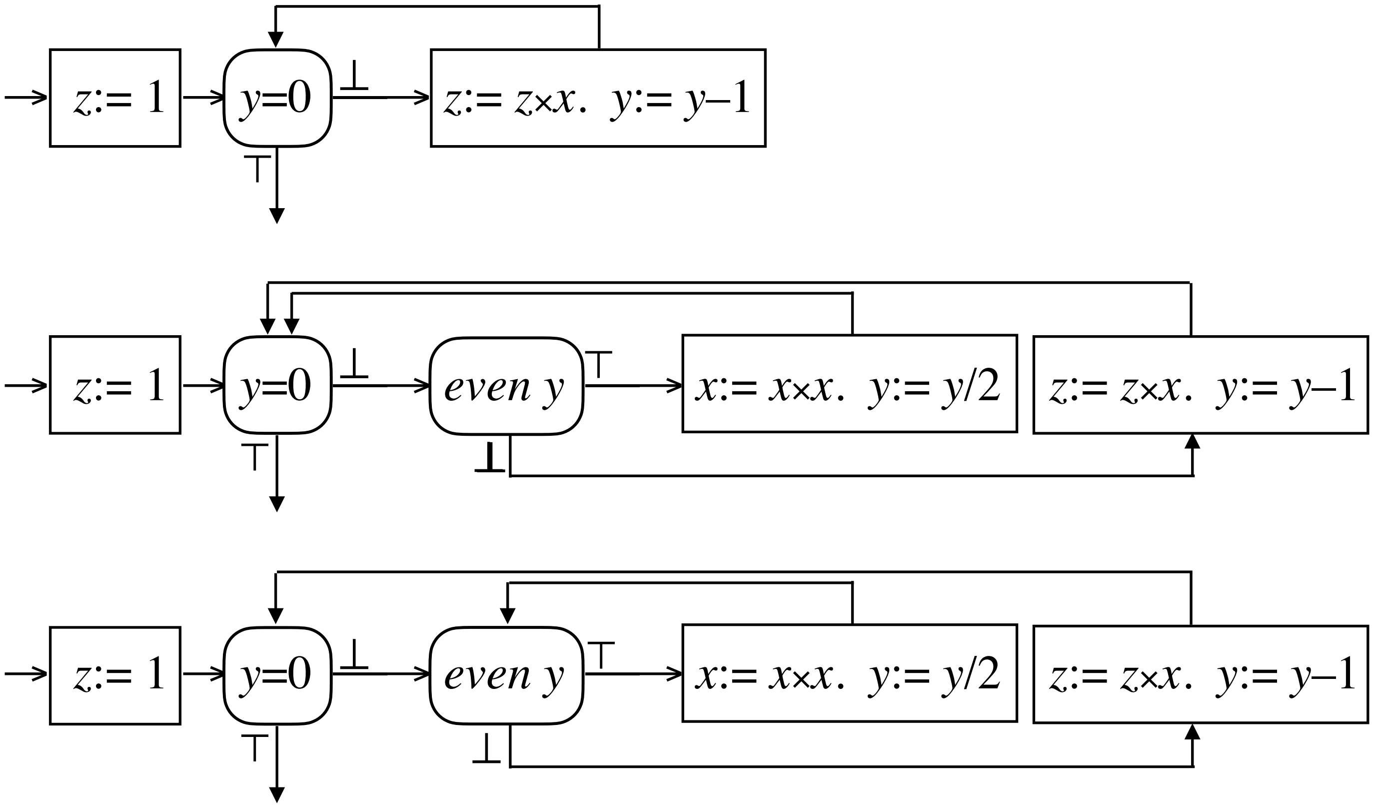


Fast Exponentiation

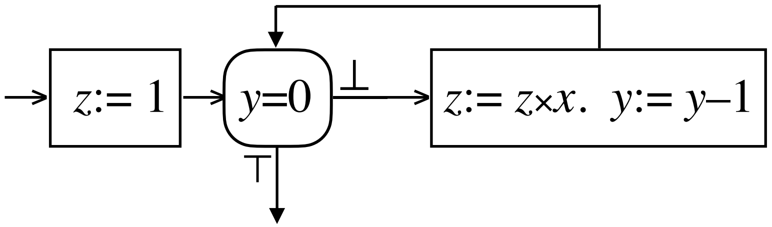


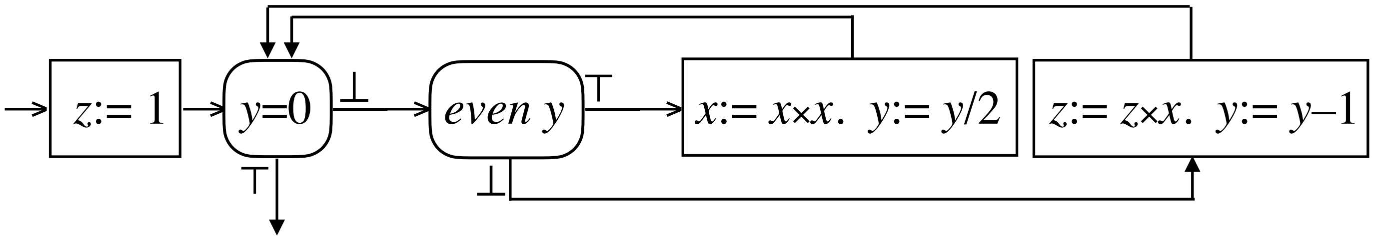


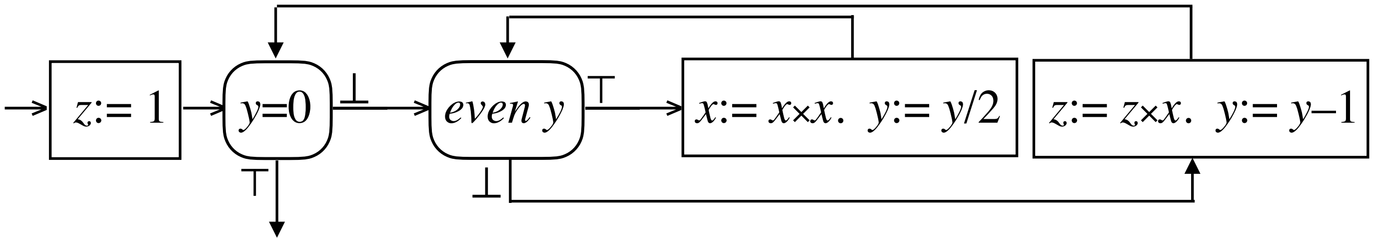
Fast Exponentiation

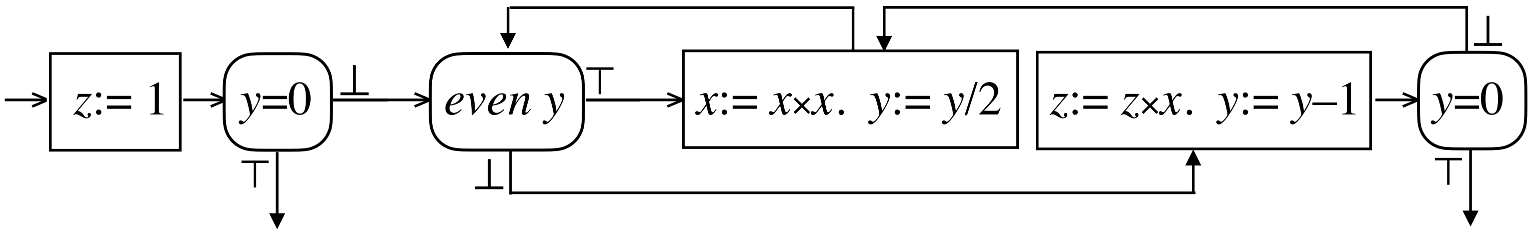


Fast Exponentiation

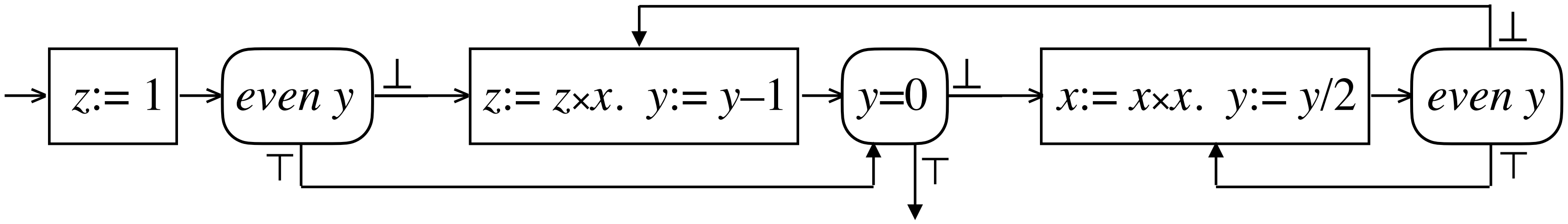




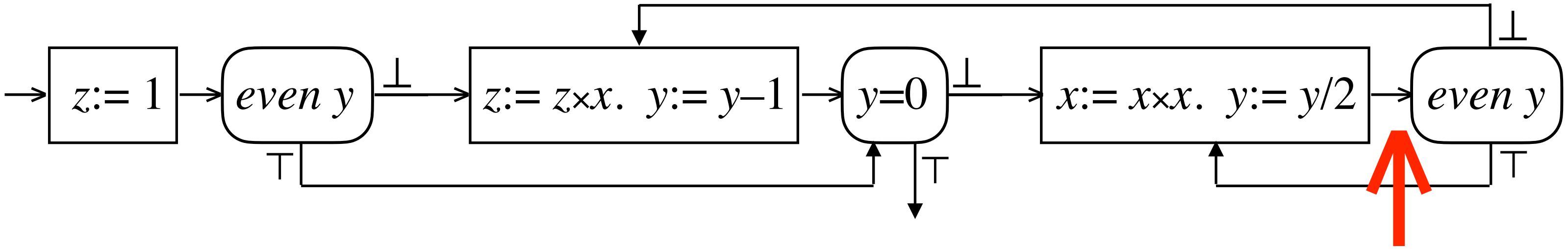




Fast Exponentiation

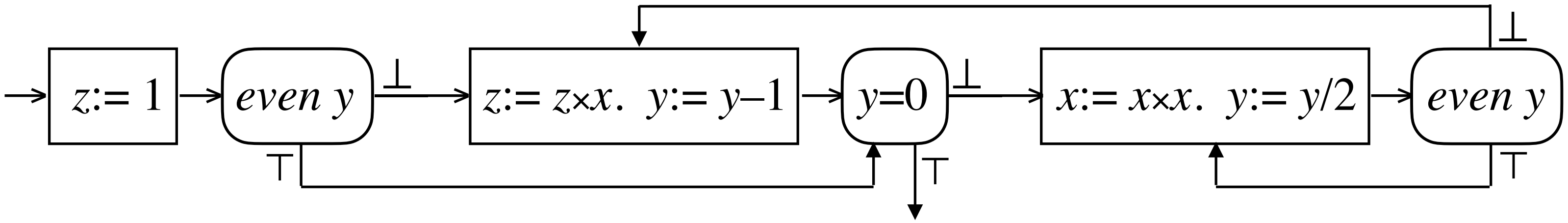


Fast Exponentiation



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

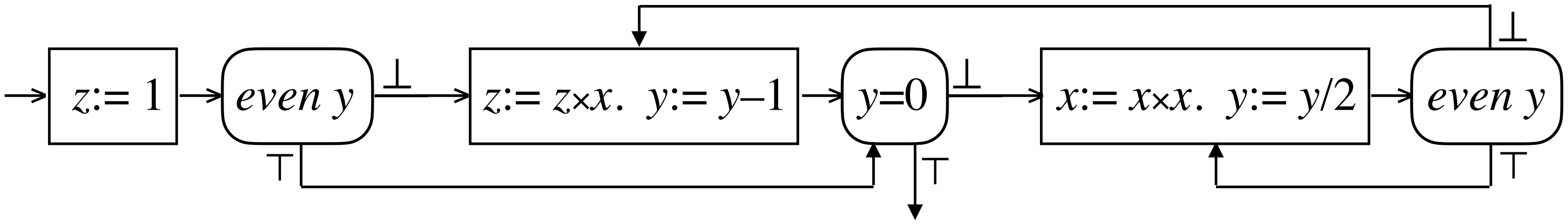
Fast Exponentiation



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

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

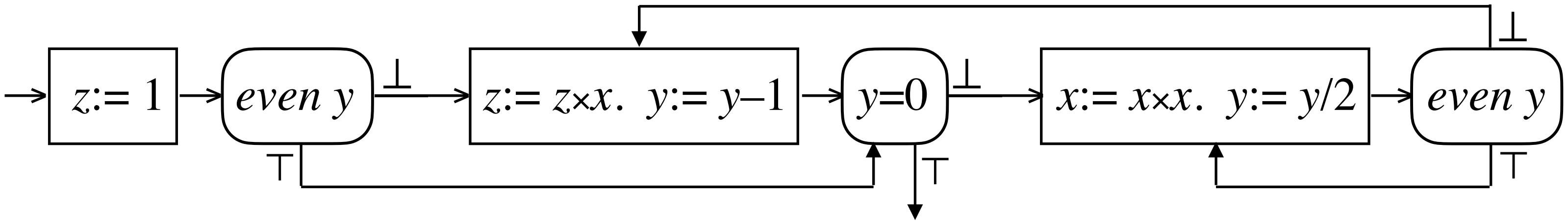
Fast Exponentiation



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

			↓	↓		↓				↓								↓		
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

Fast Exponentiation

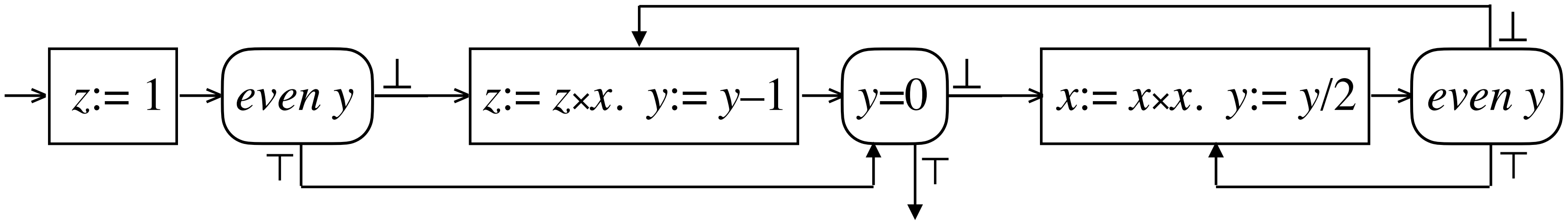


$$even\ y \wedge y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad x:= x\times x.\ \ y:= y/2.\ \ t:= t+1.\ \ y>0 \Rightarrow z' = z\times x^y$$

↓

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

Fast Exponentiation

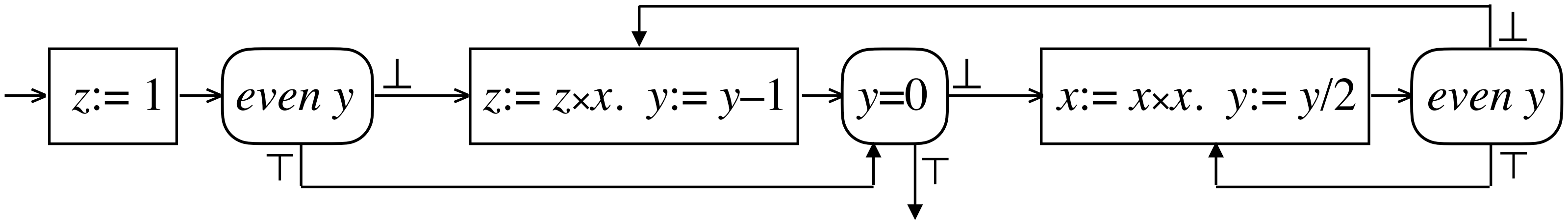


$$even\ y \land y>0 \Rightarrow z' = z\times x^y \quad \Leftarrow \quad x:= x\times x.\ \ y:= y/2.\ \ t:= t+1.\ \ y>0 \Rightarrow z' = z\times x^y$$

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

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

Fast Exponentiation



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

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

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

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

Fibonacci Numbers

$$\begin{aligned} \mathit{fib}\ 0 &= 0 \\ \mathit{fib}\ 1 &= 1 \\ \mathit{fib}\ (n{+}2) &= \mathit{fib}\ n + \mathit{fib}\ (n{+}1) \end{aligned}$$

Fibonacci Numbers

$$fib\ 0 \ = \ 0$$

$$fib\ 1 \ = \ 1$$

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

$$fib \ = \ 0 \rightarrow 0 \ \mid \ 1 \rightarrow 1 \ \mid \ \langle n\text{: } nat{+}2\cdot \ fib(n{-}2) + fib(n{-}1)\rangle$$

Fibonacci Numbers

$fib\ 0 = 0$

$fib\ 1 = 1$

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

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

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

Fibonacci Numbers

Fibonacci Numbers

$x' = \mathit{fib}\ n$

Fibonacci Numbers

$$x' = \mathit{fib}\ n \quad \Leftarrow \quad x' = \mathit{fib}\ n \ \land\ y' = \mathit{fib}\ (n+1)$$

Fibonacci Numbers

$$x' = \mathit{fib}\ n \quad \Leftarrow \quad x' = \mathit{fib}\ n \ \land \ y' = \mathit{fib}\ (n+1) \quad = \quad P$$

Fibonacci Numbers

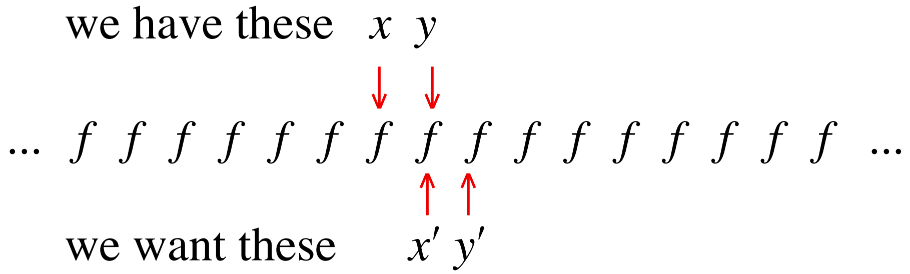
$x' = fib\ n \quad \Leftarrow \quad x' = fib\ n \ \wedge\ y' = fib\ (n+1) \quad = \quad P$

$P \quad \Leftarrow \quad$ **if** $n{=}0$ **then** $x{:=}\ 0.\ \ y{:=}\ 1$ **else** $n{:=}\ n{-}1.\ \ P.\ \ x'{=}y\ \wedge\ y'{=}x{+}y$ **fi**

Fibonacci Numbers

$$x' = \mathit{fib}\ n \quad \Leftarrow \quad x' = \mathit{fib}\ n \ \land \ y' = \mathit{fib}\ (n+1) \quad = \quad P$$

$P \quad \Leftarrow \quad$ **if** $n=0$ **then** $x:= 0.\ \ y:= 1$ **else** $n:= n-1.\ \ P.\ \ x'=y \ \land \ y'=x+y$ **fi**



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

$$x' = \mathit{fib}\ n \ \Leftarrow\ x' = \mathit{fib}\ n \ \land\ y' = \mathit{fib}\ (n+1) \ = \ P$$

$$P \ \Leftarrow\ \textbf{if } n=0 \textbf{ then } x:= 0.\ y:= 1 \textbf{ else } n:= n-1.\ P.\ x'=y \ \land\ y'=x+y \textbf{ fi}$$

Fibonacci Numbers

$x' = \mathit{fib}\ n \quad \Leftarrow \quad x' = \mathit{fib}\ n \ \wedge\ y' = \mathit{fib}\ (n+1) \quad = \quad P$

$P \quad \Leftarrow \quad$ **if** $n=0$ **then** $x:= 0.\ \ y:= 1$ **else** $n:= n-1.\ \ P.\ \ x'=y \ \wedge\ y'=x+y$ **fi**

$x'=y \ \wedge\ y'=x+y \quad \Leftarrow$

Fibonacci Numbers

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

$P \quad \Leftarrow \quad$ **if** $n=0$ **then** $x{:=}\ 0.\ \ y{:=}\ 1$ **else** $n{:=}\ n{-}1.\ \ P.\ \ x'{=}y\ \wedge\ y'{=}x{+}y$ **fi**

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

Fibonacci Numbers

$x' = \mathit{fib}\ n \ \Leftarrow\ x' = \mathit{fib}\ n \wedge y' = \mathit{fib}\ (n+1) \ = \ P$

$P \ \Leftarrow\ $ **if** $n{=}0$ **then** $x{:=}\ 0.\ \ y{:=}\ 1$ **else** $n{:=}\ n{-}1.\ \ P.\ \ x'{=}y \wedge y'{=}x{+}y$ **fi**

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

$t'{=}t{+}n \ \Leftarrow\ $ **if** $n{=}0$ **then** $x{:=}\ 0.\ \ y{:=}\ 1$ **else** $n{:=}\ n{-}1.\ \ t{:=}\ t{+}1.\ \ t'{=}t{+}n.\ \ t'{=}t$ **fi**

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

Fibonacci Numbers

Fibonacci Numbers

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

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

Fibonacci Numbers

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

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

```
$P$   $\Leftarrow$   if $n=0$ then $x{:=}\ 0.\ \ y{:=}\ 1$
                 else if $\mathit{even}\ n$ then $\mathit{even}\ n \land n>0 \Rightarrow P$
                      else $\mathit{odd}\ n \Rightarrow P$ fi fi
```

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  ⇐   if n=0 then x:= 0.  y:= 1
       else if even n then even n ∧ n>0 ⇒ P
            else odd n ⇒ P fi fi
```

$odd\ n \Rightarrow P \ \Leftarrow \ n:= (n–1)/2.\ \ P.\ \ x' = x^2 + y^2 \ \land \ y' = 2\times x\times y + y^2$

Fibonacci Numbers

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

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

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

else if $even\;n$ **then** $even\;n \wedge n{>}0 \Rightarrow P$

else $odd\;n \Rightarrow P$ **fi fi**

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

$\uparrow$

$n{=}2\times k+1$

Fibonacci Numbers

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

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

```
$P$  ⇐  **if** $n=0$ **then** $x:= 0.\; y:= 1$
        **else if** $\mathit{even}\; n$ **then** $\mathit{even}\; n \wedge n>0 \Rightarrow P$
            **else** $\mathit{odd}\; n \Rightarrow P$ **fi fi**
```

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

Fibonacci Numbers

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

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

```
$P \;\Leftarrow\;$  if $n=0$ then $x:= 0.\; y:= 1$
                    else if $even\;n$ then $even\;n \wedge n>0 \Rightarrow P$
                        else $odd\;n \Rightarrow P$ fi fi
```

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

$$\uparrow$$

$$x' = fib\;k \wedge y' = fib(k+1)$$

Fibonacci Numbers

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

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

```
$P$   $\Leftarrow$   if $n{=}0$ then $x{:=}\,0.\ \ y{:=}\,1$
                     else if $\mathit{even}\ n$ then $\mathit{even}\ n \land n{>}0 \Rightarrow P$
                          else $\mathit{odd}\ n \Rightarrow P$ fi fi
```

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

$\uparrow$

$$x = \mathit{fib}\ k \land y = \mathit{fib}(k{+}1)$$

Fibonacci Numbers

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

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

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

else if *even n* **then** $even\;n \wedge n{>}0 \Rightarrow P$

else $odd\;n \Rightarrow P$ **fi fi**

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

$\uparrow$ $\uparrow$

$x = fib\;k \wedge y = fib(k+1)$ $\qquad$ $x' = fib(2\times k+1) \wedge y' = fib(2\times k+2)$

Fibonacci Numbers

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

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

```
$P$  $\Leftarrow$   if $n=0$ then $x:= 0.\ \ y:= 1$
                    else if $even\ n$ then $even\ n \land n>0 \Rightarrow P$
                         else $odd\ n \Rightarrow P$ fi fi
```

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

Fibonacci Numbers

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

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

```
$P \Leftarrow$    if $n=0$ then $x:= 0.\ y:= 1$
                  else if $even\ n$ then $even\ n \wedge n>0 \Rightarrow P$
                       else $odd\ n \Rightarrow P$ fi fi
```

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

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

Fibonacci Numbers

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

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

$$\begin{aligned}P \;\Leftarrow\;\; & \textbf{if } n{=}0 \textbf{ then } x{:=}\,0.\;\; y{:=}\,1\\ & \textbf{else if } even\ n \textbf{ then } even\ n \wedge n{>}0 \Rightarrow P\\ & \qquad \textbf{else } odd\ n \Rightarrow P \textbf{ fi fi}\end{aligned}$$

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

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

Fibonacci Numbers

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

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

```
$P \;\Leftarrow\;$ if $n=0$ then $x:=0.\ y:=1$
    else if $even\ n$ then $even\ n \land n>0 \Rightarrow P$
        else $odd\ n \Rightarrow P$ fi fi
```

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

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

↑

$$x = fib\ k \land y = fib(k+1)$$

Fibonacci Numbers

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

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

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

else if $even\ n$ **then** $even\ n \wedge n{>}0 \Rightarrow P$

else $odd\ n \Rightarrow P$ **fi fi**

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

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

$\uparrow$ $\qquad\qquad\qquad\qquad\qquad\qquad$ $\uparrow$

$x = fib\,k \wedge y = fib(k+1)$ $\qquad\qquad$ $x' = fib(2\times k+2) \wedge y' = fib(2\times k+3)$

Fibonacci Numbers

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

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

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

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

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

Fibonacci Numbers

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

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

```
$P \Leftarrow$    if $n=0$ then $x:= 0.\; y:= 1$
                  else if $even\ n$ then $even\ n \wedge n>0 \Rightarrow P$
                       else $odd\ n \Rightarrow P$ fi fi
```

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

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

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

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

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 $odd\ n \Rightarrow T$ fi fi
```

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

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

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

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

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;}
}
```