Formale Spezifikation und Verifikation
Hoare-Logik, Schleifen-Invarianten

Wintersemester 2024
Übungsblatt 05

Prof. Dr. Gidon Ernst, Marian Lingsch-Rosenfeld, Simon Rossmair, Noah König

3. Dezember 2024

Einfache Exponentiation

```
y = 1;
while x > 0 do
    y = y * 2;
    x = x - 1;
end
z = y;
```

Einfache Exponentiation

$\{x \geq 0 \land x = x_{init}\}$ Vorbedingung

$y = 1;$

while $x > 0$ **do**

$\quad y = y * 2;$

$\quad x = x - 1;$

end

$z = y;$

$\{z = 2^{x_{init}}\}$ Nachbedingung soll hier gelten

Einfache Exponentiation

$\{x \geq 0 \land x = x_{init}\}$ Vorbedingung

$y = 1;$

$\{2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$ Invariante initial zu zeigen

while $x > 0$ **do**

$\quad y = y * 2;$

$\quad x = x - 1;$

end

$\{x \leq 0 \land 2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$ Annahme: negierter Test & Invariante

$z = y;$

$\{z = 2^{x_{init}}\}$ Nachbedingung soll hier gelten

Einfache Exponentiation

$\{x \geq 0 \wedge x = x_{\mathtt{init}}\}$ — Vorbedingung

$\{2^{x_{\mathtt{init}}} = 1 \cdot 2^{x} \wedge x \geq 0\}$

$y = 1;$

$\{2^{x_{\mathtt{init}}} = y \cdot 2^{x} \wedge x \geq 0\}$ — Invariante initial zu zeigen

while $x > 0$ **do**

$\quad y = y * 2;$

$\quad x = x - 1;$

end

$\{x \leq 0 \wedge 2^{x_{\mathtt{init}}} = y \cdot 2^{x} \wedge x \geq 0\}$ — Annahme: negierter Test & Invariante

$z = y;$

$\{x \leq 0 \wedge 2^{x_{\mathtt{init}}} = y \cdot 2^{x} \wedge x \geq 0 \wedge z = y\}$

$\{z = 2^{x_{\mathtt{init}}}\}$ — Nachbedingung soll hier gelten

Einfache Exponentiation

$\{x \geq 0 \land x = x_{init}\}$ Vorbedingung

$\{2^{x_{init}} = 1 \cdot 2^{x} \land x \geq 0\}$

$y = 1;$

$\{2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$ Invariante initial zu zeigen

while $x > 0$ **do**

$\{x > 0 \land 2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$ Annahme: Schleifentest & Invariante

$y = y * 2;$

$x = x - 1;$

$\{2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$ Invariante gilt wieder

end

$\{x \leq 0 \land 2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$ Annahme: negierter Test & Invariante

$z = y;$

$\{x \leq 0 \land 2^{x_{init}} = y \cdot 2^{x} \land x \geq 0 \land z = y\}$

$\{z = 2^{x_{init}}\}$ Nachbedingung soll hier gelten

Einfache Exponentiation

$\{\mathtt{x} \geq 0 \land \mathtt{x} = \mathtt{x}_{\mathtt{init}}\}$	Vorbedingung
$\{2^{\mathtt{x}_{\mathtt{init}}} = 1 \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$	
$\mathtt{y} = 1;$	
$\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$	Invariante initial zu zeigen
while $\mathtt{x} > 0$ **do**	
$\{\mathtt{x} > 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$	Annahme: Schleifentest & Invariante
$\mathtt{y} = \mathtt{y} * 2;$	
$\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}-1} \land \mathtt{x} - 1 \geq 0\}$	
$\mathtt{x} = \mathtt{x} - 1;$	
$\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$	Invariante gilt wieder
end	
$\{\mathtt{x} \leq 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$	Annahme: negierter Test & Invariante
$\mathtt{z} = \mathtt{y};$	
$\{\mathtt{x} \leq 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0 \land \mathtt{z} = \mathtt{y}\}$	
$\{\mathtt{z} = 2^{\mathtt{x}_{\mathtt{init}}}\}$	Nachbedingung soll hier gelten

Einfache Exponentiation

$\{x \geq 0 \land x = x_{init}\}$	Vorbedingung
$\{2^{x_{init}} = 1 \cdot 2^{x} \land x \geq 0\}$	
$y = 1;$	
$\{2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$	Invariante initial zu zeigen
while $x > 0$ **do**	
$\quad \{x > 0 \land 2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$	Annahme: Schleifentest & Invariante
$\quad \{2^{x_{init}} = (y \cdot 2) \cdot 2^{x-1} \land x - 1 \geq 0\}$	
$\quad y = y * 2;$	
$\quad \{2^{x_{init}} = y \cdot 2^{x-1} \land x - 1 \geq 0\}$	
$\quad x = x - 1;$	
$\quad \{2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$	Invariante gilt wieder
end	
$\{x \leq 0 \land 2^{x_{init}} = y \cdot 2^{x} \land x \geq 0\}$	Annahme: negierter Test & Invariante
$z = y;$	
$\{x \leq 0 \land 2^{x_{init}} = y \cdot 2^{x} \land x \geq 0 \land z = y\}$	
$\{z = 2^{x_{init}}\}$	Nachbedingung soll hier gelten

Einfache Exponentiation

$\{\mathtt{x} \geq 0 \land \mathtt{x} = \mathtt{x}_{\mathtt{init}}\}$ — Vorbedingung

$\{2^{\mathtt{x}_{\mathtt{init}}} = 1 \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$

$\mathtt{y} = 1;$

$\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$ — Invariante initial zu zeigen

while $\mathtt{x} > 0$ **do**

  $\{\mathtt{x} > 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$ — Annahme: Schleifentest & Invariante

  $\{2^{\mathtt{x}_{\mathtt{init}}} = (\mathtt{y} \cdot 2) \cdot 2^{\mathtt{x}-1} \land \mathtt{x} - 1 \geq 0\}$

  $\mathtt{y} = \mathtt{y} * 2;$

  $\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}-1} \land \mathtt{x} - 1 \geq 0\}$

  $\mathtt{x} = \mathtt{x} - 1;$

  $\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$ — Invariante gilt wieder

end

$\{\mathtt{x} \leq 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$ — Annahme: negierter Test & Invariante

$\mathtt{z} = \mathtt{y};$

$\{\mathtt{x} \leq 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0 \land \mathtt{z} = \mathtt{y}\}$

$\{\mathtt{z} = 2^{\mathtt{x}_{\mathtt{init}}}\}$ — Nachbedingung soll hier gelten

Nebenrechnungen: alle direkt aufeinander folgenden Zusicherungen im Code sind Anwendungen der Regel Conseq und erfordern einen Beweis!

Einfache Exponentiation: Nebenrechnungen

Einfache Exponentiation: Nebenrechnungen

$\{\mathtt{x} \geq 0 \land \mathtt{x} = \mathtt{x}_{\mathtt{init}}\}$

$\{2^{\mathtt{x}_{\mathtt{init}}} = 1 \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$

Einfache Exponentiation: Nebenrechnungen

$\{\mathtt{x} \geq 0 \wedge \mathtt{x} = \mathtt{x}_{\mathtt{init}}\}$

Einsetzen und vereinfachen

$\{2^{\mathtt{x}_{\mathtt{init}}} = 1 \cdot 2^{\mathtt{x}} \wedge \mathtt{x} \geq 0\}$

Einfache Exponentiation: Nebenrechnungen

$\{\mathtt{x} \geq 0 \land \mathtt{x} = \mathtt{x}_{\mathtt{init}}\}$

Einsetzen und vereinfachen

$\{2^{\mathtt{x}_{\mathtt{init}}} = 1 \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$

$\{\mathtt{x} > 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$

$\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}} \land \mathtt{x} - 1 \geq 0\}$

Einfache Exponentiation: Nebenrechnungen

$\{\mathtt{x} \geq 0 \land \mathtt{x} = \mathtt{x_{init}}\}$

Einsetzen und vereinfachen

$\{2^{\mathtt{x_{init}}} = 1 \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$

$\{\mathtt{x} > 0 \land 2^{\mathtt{x_{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$

$2^{\mathtt{x_{init}}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}}$
$\mathtt{x} > 0 \Rightarrow x - 1 \geq 0$

$\{2^{\mathtt{x_{init}}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}} \land \mathtt{x} - 1 \geq 0\}$

$2^{\mathtt{x_{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}}$
$\mathtt{x} \geq 0$ ist als Annahme nicht ausreichend

Einfache Exponentiation: Nebenrechnungen

$\{\mathtt{x} \geq 0 \land \mathtt{x} = \mathtt{x}_{\mathtt{init}}\}$

Einsetzen und vereinfachen

$\{2^{\mathtt{x}_{\mathtt{init}}} = 1 \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$

$\{\mathtt{x} > 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0\}$

$2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}}$
$\mathtt{x} > 0 \Rightarrow x - 1 \geq 0$

$2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}}$
$\mathtt{x} \geq 0$ ist als Annahme nicht ausreichend

$\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}} \land \mathtt{x} - 1 \geq 0\}$

$\{\mathtt{x} \leq 0 \land 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \land \mathtt{x} \geq 0 \land \mathtt{z} = \mathtt{y}\}$

$\{\mathtt{z} = 2^{\mathtt{x}_{\mathtt{init}}}\}$

Einfache Exponentiation: Nebenrechnungen

$\{\mathtt{x} \geq 0 \wedge \mathtt{x} = \mathtt{x}_{\mathtt{init}}\}$

Einsetzen und vereinfachen

$\{2^{\mathtt{x}_{\mathtt{init}}} = 1 \cdot 2^{\mathtt{x}} \wedge \mathtt{x} \geq 0\}$

$\{\mathtt{x} > 0 \wedge 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \wedge \mathtt{x} \geq 0\}$

$2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}}$
$\mathtt{x} > 0 \Rightarrow x - 1 \geq 0$

$2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}}$
$\mathtt{x} \geq 0$ ist als Annahme nicht ausreichend

$\{2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2 \cdot 2^{\mathtt{x-1}} \wedge \mathtt{x} - 1 \geq 0\}$

$\{\mathtt{x} \leq 0 \wedge 2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}} \wedge \mathtt{x} \geq 0 \wedge \mathtt{z} = \mathtt{y}\}$

$2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y} \cdot 2^{\mathtt{x}}$
$2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{y}$
$2^{\mathtt{x}_{\mathtt{init}}} = \mathtt{z}$

$\mathtt{x} \leq 0 \wedge \mathtt{x} \geq 0 \Rightarrow \mathtt{x} = 0 \wedge 2^0 = 1$
$\mathtt{z} = \mathtt{y}$

$\{\mathtt{z} = 2^{\mathtt{x}_{\mathtt{init}}}\}$

Binäre Exponentiation

$\mathtt{y} = 1; \mathtt{k} = 2; \mathtt{n} = 0;$ (Platz sparen, normalerweise 3 Zeilen)

while $\mathtt{x} > 0$ **do**

  if $!(\mathtt{x}\%2 = 0)$ **then**
    $\mathtt{y} = \mathtt{y} * \mathtt{k};$
  else
    `;//skip`

  $\mathtt{k} = \mathtt{k} * \mathtt{k}; \mathtt{x} = \mathtt{x}/2; \mathtt{n} = \mathtt{n} + 1;$ (Platz sparen, normalerweise 3 Zeilen)

end

$\mathtt{z} = \mathtt{y};$

Binäre Exponentiation

$\{x \geq 0 \wedge x = x_{init}\}$ Vorbedingung

$y = 1; k = 2; n = 0;$ (Platz sparen, normalerweise 3 Zeilen)

while $x > 0$ **do**

    if $!(x\%2 = 0)$ **then**

        $y = y * k;$

    else

        ;//skip

    $k = k * k; x = x/2; n = n + 1;$ (Platz sparen, normalerweise 3 Zeilen)

end

$z = y;$

$\{z = 2^{x_{init}}\}$ Nachbedingung soll hier gelten

Binäre Exponentiation

$\{x \geq 0 \land x = x_{\mathtt{init}}\}$	Vorbedingung
$y = 1; k = 2; n = 0;$	(Platz sparen, normalerweise 3 Zeilen)
$\{y \cdot k^{x} = 2^{x_{\mathtt{init}}} \land k = 2^{2^{n}} \land x \geq 0\}$	Invariante initial zu zeigen
while $x > 0$ **do**	
if $!(x\%2 = 0)$ **then**	
$y = y * k;$	
else	
;//skip	
$k = k * k; x = x/2; n = n + 1;$	(Platz sparen, normalerweise 3 Zeilen)
end	
$\{x \leq 0 \land y \cdot k^{x} = 2^{x_{\mathtt{init}}} \land k = 2^{2^{n}} \land x \geq 0\}$	negierter Test & Invariante
$z = y;$	
$\{z = 2^{x_{\mathtt{init}}}\}$	Nachbedingung soll hier gelten

Binäre Exponentiation

$\{\mathtt{x} \geq 0 \land \mathtt{x} = \mathtt{x_{init}}\}$ — Vorbedingung

$\{1 \cdot 2^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land 2 = 2^{2^0} \land \mathtt{x} \geq 0\}$

$\mathtt{y} = 1; \mathtt{k} = 2; \mathtt{n} = 0;$ — (Platz sparen, normalerweise 3 Zeilen)

$\{\mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$ — Invariante initial zu zeigen

while $\mathtt{x} > 0$ **do**

  if $!(\mathtt{x}\%2 = 0)$ **then**

    $\mathtt{y} = \mathtt{y} * \mathtt{k};$

  else

    `;//skip`

  $\mathtt{k} = \mathtt{k} * \mathtt{k}; \mathtt{x} = \mathtt{x}/2; \mathtt{n} = \mathtt{n} + 1;$ — (Platz sparen, normalerweise 3 Zeilen)

end

$\{\mathtt{x} \leq 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$ — negierter Test & Invariante

$\mathtt{z} = \mathtt{y};$

$\{\mathtt{x} \leq 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0 \land z = y\}$

$\{\mathtt{z} = 2^{\mathtt{x_{init}}}\}$ — Nachbedingung soll hier gelten

Binäre Exponentiation

$\{x \geq 0 \land x = x_{init}\}$	Vorbedingung
$\{1 \cdot 2^{x} = 2^{x_{init}} \land 2 = 2^{2^0} \land x \geq 0\}$	
$y = 1; k = 2; n = 0;$	(Platz sparen, normalerweise 3 Zeilen)
$\{y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^n} \land x \geq 0\}$	Invariante initial zu zeigen
while $x > 0$ **do**	
$\quad \{x > 0 \land y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^n} \land x \geq 0\}$	(Schleifentest & Invariante) $= P_{\text{if}}$
$\quad$ **if** $!(x\%2 = 0)$ **then**	
$\qquad y = y * k;$	
$\quad$ **else**	
$\qquad$ `;//skip`	
$\quad k = k * k; x = x/2; n = n + 1;$	(Platz sparen, normalerweise 3 Zeilen)
$\quad \{y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^n} \land x \geq 0\}$	Invariante gilt wieder
end	
$\{x \leq 0 \land y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^n} \land x \geq 0\}$	negierter Test & Invariante
$z = y;$	
$\{x \leq 0 \land y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^n} \land x \geq 0 \land z = y\}$	
$\{z = 2^{x_{init}}\}$	Nachbedingung soll hier gelten

Binäre Exponentiation

$\{x \geq 0 \land x = x_{init}\}$	Vorbedingung
$\{1 \cdot 2^{x} = 2^{x_{init}} \land 2 = 2^{2^{0}} \land x \geq 0\}$	
$y = 1; k = 2; n = 0;$	(Platz sparen, normalerweise 3 Zeilen)
$\{y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^{n}} \land x \geq 0\}$	Invariante initial zu zeigen
while $x > 0$ **do**	
$\quad \{x > 0 \land y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^{n}} \land x \geq 0\}$	(Schleifentest & Invariante) $= P_{\text{if}}$
$\quad$ **if** $!(x\%2 = 0)$ **then**	
$\qquad y = y * k;$	
$\quad$ **else**	
$\qquad ; //skip$	
$\quad \{y \cdot (k \cdot k)^{\lfloor x/2 \rfloor} = 2^{x_{init}} \land k \cdot k = 2^{2^{n+1}} \land x \geq 0\}$	Nachbedingung Q_{if} ("/“ $\widehat{=}$ Ganzzahldiv.)
$\quad k = k * k; x = x/2; n = n + 1;$	(Platz sparen, normalerweise 3 Zeilen)
$\quad \{y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^{n}} \land x \geq 0\}$	Invariante gilt wieder
end	
$\{x \leq 0 \land y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^{n}} \land x \geq 0\}$	negierter Test & Invariante
$z = y;$	
$\{x \leq 0 \land y \cdot k^{x} = 2^{x_{init}} \land k = 2^{2^{n}} \land x \geq 0 \land z = y\}$	
$\{z = 2^{x_{init}}\}$	Nachbedingung soll hier gelten

Binäre Exponentiation

$\{\mathtt{x} \geq 0 \wedge \mathtt{x} = \mathtt{x}_{\mathtt{init}}\}$ Vorbedingung

$\{1 \cdot 2^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \wedge 2 = 2^{2^0} \wedge \mathtt{x} \geq 0\}$

$\mathtt{y} = 1; \mathtt{k} = 2; \mathtt{n} = 0;$ (Platz sparen, normalerweise 3 Zeilen)

$\{\mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \wedge k = 2^{2^{\mathtt{n}}} \wedge \mathtt{x} \geq 0\}$ Invariante initial zu zeigen

while $\mathtt{x} > 0$ **do**

$\quad\{\mathtt{x} > 0 \wedge \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \wedge k = 2^{2^{\mathtt{n}}} \wedge \mathtt{x} \geq 0\}$ (Schleifentest & Invariante) $= P_{\text{if}}$

$\quad$ **if** $!(\mathtt{x}\%2 = 0)$ **then**

$\quad\quad \mathtt{y} = \mathtt{y} * \mathtt{k};$

$\quad$ **else**

$\quad\quad \mathtt{;//skip}$

$\quad\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \mathtt{x}/2 \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \wedge \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \wedge \mathtt{x} \geq 0\}$ Nachbedingung Q_{if} ("/" $\widehat{=}$ Ganzzahldiv.)

$\quad \mathtt{k} = \mathtt{k} * \mathtt{k}; \mathtt{x} = \mathtt{x}/2; \mathtt{n} = \mathtt{n} + 1;$ (Platz sparen, normalerweise 3 Zeilen)

$\quad\{\mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \wedge k = 2^{2^{\mathtt{n}}} \wedge \mathtt{x} \geq 0\}$ Invariante gilt wieder

end

$\{\mathtt{x} \leq 0 \wedge \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \wedge k = 2^{2^{\mathtt{n}}} \wedge \mathtt{x} \geq 0\}$ negierter Test & Invariante

$\mathtt{z} = \mathtt{y};$

$\{\mathtt{x} \leq 0 \wedge \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \wedge k = 2^{2^{\mathtt{n}}} \wedge \mathtt{x} \geq 0 \wedge z = y\}$

$\{\mathtt{z} = 2^{\mathtt{x}_{\mathtt{init}}}\}$ Nachbedingung soll hier gelten

Binäre Exponentiation

$\{\mathtt{x} \geq 0 \land \mathtt{x} = \mathtt{x_{init}}\}$	Vorbedingung
$\{1 \cdot 2^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land 2 = 2^{2^0} \land \mathtt{x} \geq 0\}$	
$\mathtt{y} = 1; \mathtt{k} = 2; \mathtt{n} = 0;$	(Platz sparen, normalerweise 3 Zeilen)
$\{\mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	Invariante initial zu zeigen
while $\mathtt{x} > 0$ **do**	
$\quad\{\mathtt{x} > 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	(Schleifentest & Invariante) $= P_{\text{if}}$
$\quad$ **if** $!(\mathtt{x}\%2 = 0)$ **then**	
$\qquad \mathtt{y} = \mathtt{y} * \mathtt{k};$	
$\quad$ **else**	
$\qquad$ `;//skip`	
$\quad\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \mathtt{x}/2 \rfloor} = 2^{\mathtt{x_{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	Nachbedingung Q_{if} ("/" $\widehat{=}$ Ganzzahldiv.)
$\quad\mathtt{k} = \mathtt{k} * \mathtt{k}; \mathtt{x} = \mathtt{x}/2; \mathtt{n} = \mathtt{n} + 1;$	(Platz sparen, normalerweise 3 Zeilen)
$\quad\{\mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	Invariante gilt wieder
end	
$\{\mathtt{x} \leq 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	negierter Test & Invariante
$\mathtt{z} = \mathtt{y};$	
$\{\mathtt{x} \leq 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0 \land z = y\}$	
$\{\mathtt{z} = 2^{\mathtt{x_{init}}}\}$	Nachbedingung soll hier gelten

Nebenrechnungen: alle direkt aufeinander folgenden Zusicherungen im Code sind Anwendungen der Regel CONSEQ und erfordern einen Beweis! Für die if-Anweisung muss das Hoare-Tripel noch zusätzlich bewiesen werden (nächste Seite).

Binäre Exponentiation: Nebenrechnungen

$\{y > 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$ Vorbedingung P_{if}

if $!(\mathtt{x}\%2 = 0)$ **then** if-Bedingung ϕ

$\quad \mathtt{y} = \mathtt{y} * \mathtt{k};$

else

$\quad$ `;//skip`

$\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$ Nachbedingung Q_{if}

Binäre Exponentiation: Nebenrechnungen

$\{y > 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	Vorbedingung P_{if}
if $!(\mathtt{x}\%2 = 0)$ **then**	if-Bedingung ϕ
$\quad\{\mathtt{x} \bmod 2 \neq 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	$\phi \land P_{\text{if}}$
$\quad\mathtt{y} = \mathtt{y} * \mathtt{k};$	
$\quad\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x_{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	Q_{if}
else	
$\quad\{\mathtt{x} \bmod 2 = 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x_{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	$\neg\phi \land P_{\text{if}}$
$\quad$`;//skip`	
$\quad\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x_{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	Q_{if}
$\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x_{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	Nachbedingung Q_{if}

Binäre Exponentiation: Nebenrechnungen

$\{y > 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	Vorbedingung P_{if}
if $!(\mathtt{x}\%2 = 0)$ **then**	if-Bedingung ϕ
$\quad\{\mathtt{x} \bmod 2 \neq 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	$\phi \land P_{\text{if}}$
$\quad\{\mathtt{y} \cdot \mathtt{k} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	
$\quad\mathtt{y} = \mathtt{y} * \mathtt{k};$	
$\quad\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	Q_{if}
else	
$\quad\{\mathtt{x} \bmod 2 = 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\}$	$\neg\phi \land P_{\text{if}}$
$\quad\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	
$\quad$`;//skip`	
$\quad\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	Q_{if}
$\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\}$	Nachbedingung Q_{if}

Binäre Exponentiation: Nebenrechnungen

$$
\begin{array}{ll}
\{y > 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\} & \text{Vorbedingung } P_{\text{if}} \\
\textbf{if } !(\mathtt{x}\%2 = 0) \textbf{ then} & \text{if-Bedingung } \phi \\
\quad \{\mathtt{x} \bmod 2 \neq 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\} & \phi \land P_{\text{if}} \\
\quad \{\mathtt{y} \cdot \mathtt{k} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\} & \\
\quad \mathtt{y} = \mathtt{y} * \mathtt{k}; & \\
\quad \{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\} & Q_{\text{if}} \\
\textbf{else} & \\
\quad \{\mathtt{x} \bmod 2 = 0 \land \mathtt{y} \cdot \mathtt{k}^{\mathtt{x}} = 2^{\mathtt{x}_{\mathtt{init}}} \land k = 2^{2^{\mathtt{n}}} \land \mathtt{x} \geq 0\} & \neg\phi \land P_{\text{if}} \\
\quad \{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\} & \\
\quad ;\mathtt{//skip} & \\
\quad \{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\} & Q_{\text{if}} \\
\{\mathtt{y} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = 2^{\mathtt{x}_{\mathtt{init}}} \land \mathtt{k} \cdot \mathtt{k} = 2^{2^{\mathtt{n}+1}} \land \mathtt{x} \geq 0\} & \text{Nachbedingung } Q_{\text{if}}
\end{array}
$$

Nebenrechnungen: alle direkt aufeinander folgenden Zusicherungen im Code sind Anwendungen der Regel CONSEQ und erfordern einen Beweis! Für die zwei Fälle grobe Skizze:

Binäre Exponentiation: Noch mehr Nebenrechnungen

`if`-Fall:

- $x \bmod 2 \neq 0 \Rightarrow x \bmod 2 = 1 \Rightarrow \lfloor \frac{\mathtt{x}}{2} \rfloor = \frac{\mathtt{x}}{2} - \frac{1}{2}$
- $2 \cdot \lfloor \frac{\mathtt{x}}{2} \rfloor = \mathtt{x} - 1 \Rightarrow \mathtt{k} \cdot (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = \mathtt{k} \cdot (\mathtt{k}^2)^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = \mathtt{k} \cdot \mathtt{k}^{2 \cdot \lfloor \frac{\mathtt{x}}{2} \rfloor} = \mathtt{k} \cdot \mathtt{k}^{\mathtt{x}-1} = \mathtt{k}^{\mathtt{x}}$

`else`-Fall:

- $x \bmod 2 = 0 \Rightarrow \lfloor \frac{\mathtt{x}}{2} \rfloor = \frac{\mathtt{x}}{2}$
- $2 \cdot \lfloor \frac{\mathtt{x}}{2} \rfloor = \mathtt{x} \Rightarrow (\mathtt{k} \cdot \mathtt{k})^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = (\mathtt{k}^2)^{\lfloor \frac{\mathtt{x}}{2} \rfloor} = \mathtt{k}^{2 \cdot \lfloor \frac{\mathtt{x}}{2} \rfloor} = \mathtt{k}^{\mathtt{x}}$

Binäre Exponentiation: Einfachere Invariante?

Binäre Exponentiation: Einfachere Invariante?

- Der Teil mit $k = 2^{2^n}$ in der Invariante wird für den Beweis nicht benötigt und kann weggelassen werden.

Binäre Exponentiation: Einfachere Invariante?

- Der Teil mit $k = 2^{2^n}$ in der Invariante wird für den Beweis nicht benötigt und kann weggelassen werden.
- Tieferer Zusammenhang: Der Algorithmus kann für Exponentieren mit beliebiger (positiver) Basis benutzt werden, sofern `k` am Anfang auf diesen Wert gesetzt wird statt auf 2

Binäre Exponentiation: Einfachere Invariante?

- Der Teil mit $k = 2^{2^n}$ in der Invariante wird für den Beweis nicht benötigt und kann weggelassen werden.
- Tieferer Zusammenhang: Der Algorithmus kann für Exponentieren mit beliebiger (positiver) Basis benutzt werden, sofern `k` am Anfang auf diesen Wert gesetzt wird statt auf 2
- Der Beweis für allgemeine Startwerte von `k` geht dann weitestgehend analog

Binäre Exponentiation: Einfachere Invariante?

- Der Teil mit $k = 2^{2^n}$ in der Invariante wird für den Beweis nicht benötigt und kann weggelassen werden.
- Tieferer Zusammenhang: Der Algorithmus kann für Exponentieren mit beliebiger (positiver) Basis benutzt werden, sofern `k` am Anfang auf diesen Wert gesetzt wird statt auf 2
- Der Beweis für allgemeine Startwerte von `k` geht dann weitestgehend analog
- Die Hilfsvariable `n` im Programm kann deshalb auch entfernt werden

Laufzeitkomplexitäten

- Einfache Exponentiation:
- Binäre Exponentiation:

Laufzeitkomplexitäten

- Einfache Exponentiation:
- Binäre Exponentiation:

Laufzeitkomplexitäten

- Einfache Exponentiation: $\mathcal{O}(x)$
- Binäre Exponentiation:

Laufzeitkomplexitäten

- Einfache Exponentiation: $\mathcal{O}(x)$
- Binäre Exponentiation: $\mathcal{O}(\log x)$