Programmierung 2 (SS 2021)
Universität des Saarlandes
Fakultät MI
Compiler Design Lab

Musterlösung 15
Korrektheit & Verifikation

Prof. Dr. Sebastian Hack
Julian Rosemann, B. Sc.
Thorsten KlöSSner, M. Sc.
Julia Wichlacz, M. Sc.
Maximilian Fickert, M. Sc.

Im Vorlesungskalender finden Sie Informationen über die Kapitel des Skripts, die parallel zur Vorlesung bearbeitet werden sollen bzw. dort besprochen werden. Die Übungsaufgaben dienen der Vertiefung des Wissens, das in der Vorlesung vermittelt wird und als Vorbereitung auf Minitests und Klausur.
Weitere Aufgaben zu den Themen finden Sie jeweils am Ende der Skriptkapitel.
Die Schwierigkeitsgrade sind durch Steine des 2048-Spiels gekennzeichnet, von 512 „leicht“ bis 2048 „schwer“. 4096 steht für Knobelaufgaben.

Korrektheit

Aufgabe 15.0: Entscheidunsprobleme

Gegeben ist folgendes C0pb-Programm:

```
{
    a = A;
    b = B;
    while (b != 0) {
        if (a > b)
            a = a - b;
        else
            b = b - a;
    }
    r = a;
}
```

mit der Vorbedingung $V = A > 0 \land B \geq 0$.

1. Begründen oder widerlegen Sie, dass die folgenden Ausdrücke Invarianten der Schleife des Programms beschreiben.

   (a) $I_1 = a > 0 \land b \geq 0$

   (b) $I_2 = a > 0 \land b > 0$

   (c) $I_3 = A \mod a \neq 0 \land B \mod a \neq 0$

2. Begründen oder widerlegen Sie, dass die folgenden Funktionen Terminierungsfunktionen der Schleife des Programms sind. Es gilt dabei die Invariante $I = a > 0 \land b \geq 0$.

   (a) $t_1 = a$

   (b) $t_2 = b$

   (c) $t_3 = a + b$

   (d) $t_4 = A - a - b$

Lösung

1. Sei im folgenden `S = if (a > b) a = a - b; else b = b - a;`.

   (a) Ja, I_1 ist eine gültige Schleifeninvariante.

$$\begin{aligned} wp(S|I_1) &= wp(\text{if } (a > b) a = a - b; \text{ else } b = b - a; |\, a > 0 \land b \geq 0) \\ &= (a > b \land a - b > 0 \land b \geq 0) \lor (a \leq b \land a > 0 \land b - a \geq 0) \\ &\Leftarrow a > 0 \land b > 0 \Leftrightarrow I_1 \land b \neq 0 \end{aligned}$$

   (b) Nein, denn für alle $a = b$ mit $a, b > 0$ ist $b - a > 0$ bzw. $a - b > 0$ nicht erfüllt. Daher $I_2 \land b \neq 0 \not\Rightarrow wp(S \mid I_2)$. Wobei

$$wp(S|I_2) = (a > b \land a - b > 0 \land b > 0) \lor (a \leq b \land a > 0 \land b - a > 0) \not\Leftarrow I_2 \land b \neq 0$$

   (c) Nein, denn für z.B. $A = 7$, $B = 3$, $a = 4$ und $b = 3$ ist $I_3 \land b \neq 0$ erfüllt, aber $a \leq b$ bzw. $A \bmod a - b \neq 0 \Leftrightarrow A \bmod 1 \neq 0$ sind nicht erfüllt.
   Daher $I_3 \land b \neq 0 \not\Rightarrow wp(S \mid I_3)$. Wobei

$$\begin{aligned} wp(S|I_3) = &(a > b \land A \bmod a - b \neq 0 \land B \bmod a - b \neq 0) \\ &\lor (a \leq b \land A \bmod a \neq 0 \land B \bmod a \neq 0) \land b \neq 0 \end{aligned}$$

2. (a) Nein, z.B. für $a = 3$ und $b = 4$ ist a nach Ausführung des Schleifenrumpfs immernoch 3.

   (b) Nein, z.B. für $a = 4$ und $b = 3$ ist b nach Ausführung des Schleifenrumpfs immernoch 3.

   (c) Ja.

$$\begin{aligned} &wp(S \mid 0 \leq a + b \leq K \land \underbrace{a > 0 \land b \geq 0}_{\text{Invariante}}) \\ &= (a > b \land 0 \leq a - b + b \leq K \land a - b > 0 \land b \geq 0) \\ &\qquad \lor (a \leq b \land 0 \leq a + b - a \leq K \land a > 0 \land b - a \geq 0) \\ &\Leftrightarrow (a > b \land 0 \leq a \leq K \land b \geq 0) \lor (a \leq b \land 0 \leq b \leq K \land a > 0) \\ &\Leftarrow 0 \leq a + b \leq K + 1 \land a > 0 \land b > 0 \\ &\Leftrightarrow 0 \leq a + b \leq K + 1 \land a > 0 \land b \geq 0 \land \underbrace{b \neq 0}_{\text{Schleifenbedingung}} \end{aligned}$$

   (d) Nein, z.B. für $A = 4$ und $b = 1$ gilt $t_4 = -1 < 0$ vor der ersten Ausführung des Schleifenrumpfs, nach Definiton muss die Terminierungsfunktion jedoch nach $\mathbb{N}$ abbilden.

Aufgabe 15.1: Schleifeninvarianten und Terminierungsfunktionen

Betrachten Sie folgende Programme, die Invarianten `I` und die Funktionen `t`:

(1)

```
x = 10;
y = 5;
while (x <= y) {
    y = y - x;
}
```

mit `I` $:= \textit{true}$ und `t` $:= x$

(2)

```
x = 0;
b = B;
while (b > 0) {
    x = x + a;
    b = b - 1;
}
```

mit `I` $:= x = (B - b) * a$ und `t` $:= b$

(3)

```
a = 0;
x' = x;
while (x > 0) {
    t = x % 10;
    a += t;
    x -= t;
    x /= 10;
}
```

mit `I` $:= a = x + t$ und `t` $:= x$

(a) Handelt es sich bei den Angaben um gültige Schleifeninvarianten bzw. Terminierungsfunktionen? Argumentieren Sie jeweils kurz!

(b) Beweisen Sie Ihre Antworten nun formal mit Hilfe des wp-Kalküls!

(c) Falls es sich um keine gültigen Schleifeninvarianten bzw. Terminierungsfunktionen handelt, finden Sie eigene (möglichst starke) und beweisen Sie deren Gültigkeit!

Lösung

(a) (1) `I` ist trivialerweise eine Invariante, wohingegen `t` keine Terminierungsfunktion ist (`x` wird niemals geändert).

(2) `I` ist eine Invariante, da `B - b` gerade die Anzahl der Schleifeniterationen zählt und `x` in jeder solchen Iteration um `a` erhöht wird. Entsprechend ist `t` eine Terminierungsfunktion, weil `b` mit jeder Iteration um eins verringert wird.

(3) `I` ist keine Invariante, da `I` $\wedge$ `x > 0` $\not\Rightarrow$ $wp($`s | I`$)$, wobei `S` der Schleifenrumpf ist. Da `x` in jeder Schleifeniteration mindestens um den Faktor 10 kleiner wird, ist `t` eine Terminierungsfunktion.

(b) Es gilt im Allgemeinen:

- `I` ist eine Schleifeninvariante, wenn gilt:
  Schleifenbedingung $\wedge$ `I` $\Rightarrow$ wp(Schleifenrumpf | `I`)
- `t` ist eine Terminierungsfunktion, wenn gilt:
  Schleifenbedingung $\wedge$ `I` $\wedge\ 0 \leq$ `t` $\leq \mathrm{k} + 1 \Rightarrow$ wp(Schleifenrumpf | `I` $\wedge\ 0 \leq$ `t` $\leq \mathrm{k}$)

(1) $\texttt{I} := \texttt{true}$ ist eine Schleifeninvariante:

$$\begin{aligned} & wp(\texttt{y = y - x;} \mid \texttt{true}) \\ = {} & \texttt{true} \end{aligned}$$

Weiterhin:

$$\begin{aligned} & \texttt{x} \leq \texttt{y} \wedge \texttt{true} \Rightarrow \texttt{true} \\ \Leftrightarrow {} & \neg(\texttt{x} \leq \texttt{y} \wedge \texttt{true}) \vee \texttt{true} \\ \Leftrightarrow {} & \texttt{true} \end{aligned}$$

Wäre $\texttt{t}$ eine Terminierungsfunktion, müsste

$$\texttt{x} \leq \texttt{y} \wedge \texttt{true} \wedge 0 \leq \texttt{x} \leq k+1 \Rightarrow wp(y = y - x; \mid \texttt{true} \wedge 0 \leq \texttt{x} \leq k)$$

gelten. Allerdings

$$\texttt{x} \leq \texttt{y} \wedge 0 \leq \texttt{x} \leq k+1 \not\Rightarrow 0 \leq \texttt{x} \leq k$$

Somit ist $\texttt{t}$ keine Terminierungsfunktion.

(2) $\texttt{I} := \texttt{x} = (\texttt{B - b}) * \texttt{a}$ ist eine Schleifeninvariante:

$$\begin{aligned} & wp(\texttt{x = x + a; b = b - 1;} \mid \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a}) \\ = {} & wp(\texttt{x = x + a;} \mid wp(\texttt{b = b - 1;} \mid \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a})) \\ = {} & wp(\texttt{x = x + a;} \mid \texttt{x} = (\texttt{B} - \texttt{b} + 1) * \texttt{a}) \\ = {} & \texttt{x} + \texttt{a} = (\texttt{B} - \texttt{b} + 1) * \texttt{a} \\ \Leftrightarrow {} & \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a} \end{aligned}$$

Weiterhin:

$$\texttt{b} > 0 \wedge \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a} \Rightarrow \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a}$$

$\texttt{t} := \texttt{b}$ ist eine Terminierungsfunktion:

$$\begin{aligned} & wp(\texttt{x = x + a; b = b - 1;} \mid \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a} \wedge 0 \leq \texttt{b} \leq k) \\ = {} & wp(\texttt{x = x + a;} \mid wp(\texttt{b = b - 1;} \mid \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a} \wedge 0 \leq \texttt{b} \leq k)) \\ = {} & wp(\texttt{x = x + a;} \mid \texttt{x} = (\texttt{B} - \texttt{b} + 1) * \texttt{a} \wedge 0 \leq \texttt{b} - 1 \leq k) \\ = {} & \texttt{x} + \texttt{a} = (\texttt{B} - \texttt{b} + 1) * \texttt{a} \wedge 0 \leq \texttt{b} - 1 \leq k \\ \Leftrightarrow {} & \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a} \wedge 1 \leq \texttt{b} \leq k+1 \end{aligned}$$

Weiterhin:

$$\texttt{b} > 0 \wedge \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a} \wedge 0 \leq \texttt{b} \leq k+1 \Rightarrow \texttt{x} = (\texttt{B} - \texttt{b}) * \texttt{a} \wedge 1 \leq \texttt{b} \leq k+1$$

(3) $\texttt{I} := \texttt{a} = \texttt{x} + \texttt{t}$ ist *keine* Schleifeninvariante:

$$\begin{aligned} & wp(\texttt{t = x \% 10; a = a + t; x = x - t; x = x / 10;} \mid \texttt{a = x + t}) \\ = {} & wp(\texttt{t = x \% 10;} \mid wp(\texttt{a = a + t;} \mid wp(\texttt{x = x - t;} \mid wp(\texttt{x = x / 10;} \mid \texttt{a = x + t})))) \\ = {} & wp(\texttt{t = x \% 10;} \mid wp(\texttt{a = a + t;} \mid wp(\texttt{x = x - t;} \mid \texttt{a = x / 10 + t}))) \\ = {} & wp(\texttt{t = x \% 10;} \mid wp(\texttt{a = a + t;} \mid \texttt{a = (x - t) / 10 + t})) \\ = {} & wp(\texttt{t = x \% 10;} \mid \texttt{a + t = (x - t) / 10 + t}) \\ \Leftrightarrow {} & wp(\texttt{t = x \% 10;} \mid \texttt{a = (x - t) / 10 }) \\ = {} & \texttt{a = (x - x \% 10) / 10} \\ \not\Leftarrow {} & \texttt{x > 0} \wedge \texttt{a = x + t} \quad (\text{z.B. } [\texttt{a} \mapsto \texttt{10, x} \mapsto \texttt{9, t} \mapsto \texttt{1}]) \end{aligned}$$

$\texttt{t} := \texttt{x}$ ist eine Terminierungsfunktion: Kann erst gezeigt werden, wenn wir eine gültige Schleifeninvariante $\texttt{I}$ gefunden haben. Siehe dazu Teil (c).

(c) (1) Wähle $\texttt{t'} := \texttt{y / x}$ und zeige, dass es sich um eine Terminierungsfunktion handelt:

$$\begin{aligned}
& wp(\texttt{y = y - x;} \mid \texttt{x > 0} \wedge 0 \leq \texttt{y / x} \leq k) \\
= \; & \texttt{x > 0} \wedge 0 \leq \texttt{(y - x) / x} \leq k \\
\Leftrightarrow \; & \texttt{x > 0} \wedge 0 \leq \texttt{y - x} \leq \texttt{x} * k \\
\Leftarrow \; & \texttt{x > 0} \wedge \texttt{-x} \leq \texttt{y - x} \leq \texttt{x} * k \wedge \texttt{x} \leq \texttt{y} \\
\Leftrightarrow \; & \texttt{x > 0} \wedge 0 \leq \texttt{y} \leq \texttt{x} * k + \texttt{x} \wedge \texttt{x} \leq \texttt{y} \\
\Leftrightarrow \; & \texttt{x > 0} \wedge 0 \leq \texttt{y / x} \leq k + 1 \wedge \texttt{x} \leq \texttt{y} \quad \checkmark
\end{aligned}$$

Es fällt auf, dass wir eine stärkere Invariante benutzt haben. Dies war nötig, um `t'` als Terminierungsfunktion zu beweisen. Nachfolgend noch der Beweis, dass $\texttt{I'} := \texttt{x > 0}$ eine Schleifeninvariante ist:

$$\begin{aligned}
& wp(\texttt{y = y - x;} \mid \texttt{x > 0}) \\
= \; & \texttt{x > 0} \\
\Leftarrow \; & \texttt{x > 0} \wedge \texttt{x} \leq \texttt{y} \quad \checkmark
\end{aligned}$$

Bereits in Teil (b) vollständig. Aber es fällt auf, dass wir eine stärkere Invariante benutzt haben. Dies war nötig, um `t'` als Terminierungsfunktion zu beweisen. Nachfolgend noch der Beweis, dass $\texttt{I'} := \texttt{x > 0}$ eine Schleifeninvariante ist:

$$\begin{aligned}
& wp(\texttt{y = y - x;} \mid \texttt{x > 0}) \\
= \; & \texttt{x > 0} \\
\Leftarrow \; & \texttt{x > 0} \wedge \texttt{x} \leq \texttt{y} \quad \checkmark
\end{aligned}$$

(2) Bereits in Teil (b) vollständig.

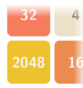
(3) Wähle $\texttt{I'} := \texttt{x} \geq \texttt{0}$ und zeige, dass es sich um eine Schleifeninvariante handelt:

$$\begin{aligned}
& wp(\texttt{t = x \% 10; a = a + t; x = x - t; x = x / 10;} \mid \texttt{x} \geq 0) \\
= \; & wp(\texttt{t = x \% 10;} \mid wp(\texttt{a = a + t;} \mid wp(\texttt{x = x - t;} \mid wp(\texttt{x = x / 10;} \mid \texttt{x} \geq 0)))) \\
= \; & wp(\texttt{t = x \% 10;} \mid wp(\texttt{a = a + t;} \mid wp(\texttt{x = x - t;} \mid \texttt{x / 10} \geq 0))) \\
= \; & wp(\texttt{t = x \% 10;} \mid wp(\texttt{a = a + t;} \mid \texttt{(x - t) / 10} \geq 0)) \\
= \; & wp(\texttt{t = x \% 10;} \mid \texttt{(x - t) / 10} \geq 0) \\
= \; & \texttt{(x - x \% 10) / 10} \geq 0 \\
\Leftrightarrow \; & \texttt{x - x \% 10} \geq 0 \\
\Leftrightarrow \; & \texttt{x} \geq \texttt{x \% 10} \\
\Leftarrow \; & \texttt{x} > 0 \\
\Leftrightarrow \; & \texttt{x} > 0 \wedge \texttt{x} \geq 0
\end{aligned}$$

Zeige nun noch, dass `t` eine Terminierungsfunktion ist:

$$\begin{aligned}
& wp(\texttt{t = x \% 10; a = a + t; x = x - t; x = x / 10;} \mid \texttt{x} \geq 0 \wedge 0 \leq \texttt{x} \leq k) \\
\Leftrightarrow \; & wp(\texttt{t = x \% 10; a = a + t; x = x - t; x = x / 10;} \mid 0 \leq \texttt{x} \leq k) \\
= \; & 0 \leq \texttt{(x - x \% 10) / 10} \leq k \\
\Leftrightarrow \; & 0 \leq \texttt{x - x \% 10} \leq 10 * k \\
\Leftrightarrow \; & \texttt{x \% 10} \leq \texttt{x} \leq 10 * k + \texttt{x \% 10} \\
\Leftarrow \; & 0 < \texttt{x} \leq k + 1 \\
\Leftrightarrow \; & \texttt{x} > 0 \wedge \texttt{x} \geq 0 \wedge 0 \leq \texttt{x} \leq k + 1
\end{aligned}$$

Aufgabe 15.2: Schon wieder Schleifen ...



Im Folgendenden sollen Sie die totale Korrektheit von kleinen Programmen `P` zeigen. Finden Sie dazu zu jeder While-Schleife eine ausreichend starke Invariante `I` und eine Terminierungsfunktion `t`. Beweisen Sie danach die Gültigkeit der Invariante `I` und der Terminierungsfunktion `t`. Nutzen Sie dann beides, um die totale Korrektheit von `P` zu zeigen.
(Hinweis: Vergessen Sie nicht zu zeigen, dass die Vorbedingung eine Teilmenge der Menge `Wp` darstellt, welche wir mit Hilfe des wp-Kalküls erhalten.)

1. Multiplikation

```
[ x ≥ 0 ∧ y ≥ 0 ∧ res = 0 ]

y' = y;
while (y > 0) {
    res = res + x;
    y = y - 1;
}

[ res = x * y' ]
```

2. Fakultät

```
[ x ≥ 0 ∧ res = 1 ]

if (x == 0) ;
else
    while (x > 0) {
        res = res * x;
        x = x - 1;
    }

[ res = X! ∧ x = 0 ]
```

3. Quadratwurzel

```
[ x ≥ 0 ∧ y = 0 ∧ res = 0 ]

while (y * y <= x ) {
    y = y + 1;
}
res = y - 1;

[ res² ≤ x ]
```

Lösung

Zunächst eine kurze Übersicht, wie wir die totale Korrektheit eines Programms `P` mit Vorbedingung `V`, Nachbedingung `N` und Schleife `S'` mit Schleifenrumpf `s` und Bedingung `b` beweisen:

- Suche eine Schleifeninvariante `I` für `S'` und beweise, dass es sich dabei um eine gültige Schleifeninvariante handelt (Zeige, dass $\mathtt{B} \cap \mathtt{I} \subseteq \mathtt{Wp}(\mathtt{s} \mid \mathtt{I})$ hält).
- Finde eine Terminierungsfunktion `t` für `S'` und beweise, dass es sich dabei um eine gültige Terminierungsfunktion für `S'` handelt (Zeige, dass $\forall \mathtt{k} \in \mathbb{N}.[\mathtt{b} \wedge \mathtt{I} \wedge 0 \leq \mathtt{t} \leq k+1]\ \ \mathtt{s}\ \ [\mathtt{I} \wedge 0 \leq \mathtt{t} \leq k]$ hält).
- Beweise, dass das Programm nach der Schleife, mit Vorbedingung $\mathtt{I} \wedge \neg\mathtt{b}$, in der Nachbedingung `N` terminiert (Zeige, dass $[\mathtt{I} \wedge \neg\mathtt{b}]\ \ \mathtt{s}_{\mathtt{nach\_der\_Schleife}}\ \ [\mathtt{N}]$ hält).
- Beweise, dass das Programm vor der Schleife, mit Vorbedingung `V`, in der Nachbedingung $\mathtt{I} \wedge \mathtt{t} \geq 0$ terminiert (Zeige, dass $[\mathtt{V}]\ \ \mathtt{s}_{\mathtt{vor\_der\_Schleife}}\ \ [\mathtt{I} \wedge \mathtt{t} \geq 0]$ hält).

Nach Konvention des Skripts beschreiben GroSSbuchstaben Zustandsmengen und Kleinbuchstaben Prädikate ($[\![\mathtt{b}]\!] = \mathtt{B}$).

1. Wähle $\texttt{I} := \texttt{res = (y' - y) * x} \land \texttt{y} \geq \texttt{0}$ und $\texttt{t} := \texttt{y}$.

   - Zeige $\texttt{I}$ ist eine Schleifeninvariante, dazu muss $\texttt{B} \cap \texttt{I} \subseteq \texttt{Wp(s | I)}$ gelten:

$$
\begin{aligned}
& \texttt{wp(res = res + x; y = y - 1;} \mid \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0) \\
= & \texttt{wp(res = res + x;} \mid \texttt{wp(y = y - 1;} \mid \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0)) \\
= & \texttt{wp(res = res + x;} \mid \texttt{res = (y' - (y - 1)) * x} \land \texttt{y - 1} \geq 0) \\
= & \texttt{res + x = (y' - (y - 1)) * x} \land \texttt{y - 1} \geq 0 \\
\Leftrightarrow & \texttt{res + x = (y' - y + 1) * x} \land \texttt{y} \geq 1 \\
\Leftrightarrow & \texttt{res + x = (y' - y) * x + x} \land \texttt{y} \geq 1 \\
\Leftrightarrow & \texttt{res = (y' - y) * x} \land \texttt{y} \geq 1 \\
\Leftarrow & \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0 \land \texttt{y > 0}
\end{aligned}
$$

   - Zeige $\texttt{t}$ ist eine Terminierungsfunktion, dazu muss gelten: $[\texttt{b} \land \texttt{I} \land 0 \leq \texttt{t} \leq k+1]\ \texttt{s}\ [\texttt{I} \land 0 \leq \texttt{t} \leq k]$

$$
\begin{aligned}
& \texttt{wp(res = res + x; y = y - 1;} \mid \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0 \land 0 \leq \texttt{y} \leq k) \\
= & \texttt{wp(res = res + x;} \mid \texttt{wp(y = y - 1;} \mid \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0 \land 0 \leq \texttt{y} \leq k)) \\
= & \texttt{wp(res = res + x;} \mid \texttt{res = (y' - (y - 1)) * x} \land \texttt{y - 1} \geq 0 \land 0 \leq \texttt{y - 1} \leq k) \\
= & \texttt{res + x = (y' - (y - 1)) * x} \land \texttt{y - 1} \geq 0 \land 0 \leq \texttt{y - 1} \leq k \\
\Leftrightarrow & \texttt{res = (y' - y) * x} \land 1 \leq \texttt{y} \leq k+1 \\
\Leftarrow & \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0 \land \texttt{y > 0} \land 0 \leq \texttt{y} \leq k+1
\end{aligned}
$$

   - Zeige wir nun, dass nach der letzten Schleifendurchführung die Schleifeninvariante die Nachbedingung impliziert, also $\texttt{I} \land \neg\texttt{b} \Rightarrow \texttt{res = x * y'}$:

$$
\begin{aligned}
& \texttt{I} \land \neg(\texttt{y > 0}) \\
\Leftrightarrow & \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0 \land \texttt{y} \leq 0 \\
\Leftrightarrow & \texttt{res = (y' - y) * x} \land \texttt{y} = 0 \\
\Leftrightarrow & \texttt{res = (y' - 0) * x} \\
\Leftrightarrow & \texttt{res = x * y'}
\end{aligned}
$$

   - Zeige zuletzt, dass $\texttt{V} \Rightarrow \texttt{wp}(\texttt{s}_{\texttt{vor\_der\_Schleife}} \mid \texttt{I} \land \texttt{t} \geq 0)$, also:
     $\texttt{x} \geq \texttt{0} \land \texttt{y} \geq \texttt{0} \land \texttt{res = 0} \Rightarrow \texttt{wp(y' = y;} \mid \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0 \land \texttt{y} \geq 0)$ gilt:

$$
\begin{aligned}
& \texttt{wp(y' = y;} \mid \texttt{res = (y' - y) * x} \land \texttt{y} \geq 0 \land \texttt{y} \geq 0) \\
= & \texttt{res = (y - y) * x} \land \texttt{y} \geq 0 \\
\Leftrightarrow & \texttt{res = 0} \land \texttt{y} \geq 0 \\
\Leftarrow & \texttt{x} \geq 0 \land \texttt{y} \geq 0 \land \texttt{res = 0}
\end{aligned}
$$

Damit haben wir die totale Korrektheit von $\texttt{P}$ bezüglich $\texttt{V}$ und $\texttt{N}$ bewiesen.

2. Wähle $\texttt{I} := \texttt{res} = \texttt{X}!/\texttt{x}! \land \texttt{x} \geq 0$ und $\texttt{t} := \texttt{x}$.

- Zeige $\texttt{I}$ ist eine Schleifeninvariante , dazu muss $\texttt{B} \cap \texttt{I} \subseteq \texttt{Wp}(\texttt{s} \mid \texttt{I})$ gelten:

$$
\begin{aligned}
&\texttt{wp(res = res * x; x = x - 1;} \mid \texttt{res} = \texttt{X}!/\texttt{x}! \land \texttt{x} \geq 0)\\
= &\texttt{res * x} = \texttt{X}!/(\texttt{x - 1})! \land \texttt{x - 1} \geq 0\\
\Leftrightarrow &\texttt{res * x} = \texttt{X}!/(\texttt{x - 1})! \land \texttt{x} \geq 1\\
\Leftarrow &\texttt{res} = \texttt{X}!/((\texttt{x - 1})! * \texttt{x}) \land \texttt{x} > 0\\
\Leftrightarrow &\texttt{res} = \texttt{X}!/\texttt{x}! \land \texttt{x} \geq 0 \land \texttt{x} > 0
\end{aligned}
$$

- Zeige $\texttt{t}$ ist eine Terminierungsfunktion: $[\texttt{b} \land \texttt{I} \land 0 \leq \texttt{t} \leq k+1]\ \texttt{s}\ [\texttt{I} \land 0 \leq \texttt{t} \leq k]$

$$
\begin{aligned}
&\texttt{wp(res = res * x; x = x - 1;} \mid \texttt{res} = \texttt{X}!/\texttt{x}! \land \texttt{x} \geq 0 \land 0 \leq \texttt{x} \leq k)\\
\Leftrightarrow &\texttt{wp(res = res * x; x = x - 1;} \mid \texttt{res} = \texttt{X}!/\texttt{x}! \land 0 \leq \texttt{x} \leq k)\\
= &\texttt{res * x} = \texttt{X}!/(\texttt{x - 1})! \land 0 \leq \texttt{x - 1} \leq k\\
\Leftrightarrow &\texttt{res * x} = \texttt{X}!/(\texttt{x - 1})! \land 1 \leq \texttt{x} \leq k+1\\
\Leftarrow &\texttt{res} = \texttt{X}!/((\texttt{x - 1})! * \texttt{x}) \land 1 \leq \texttt{x} \leq k+1\\
\Leftrightarrow &\texttt{res} = \texttt{X}!/\texttt{x}! \land \texttt{x} > 0 \land 0 \leq \texttt{x} \leq k+1
\end{aligned}
$$

- Zeige $\texttt{I} \land \neg(\texttt{x} > 0) \Rightarrow \texttt{res = X!} \land \texttt{x = 0}$:

$$
\begin{aligned}
&\texttt{I} \land \neg(\texttt{x} > 0)\\
\Leftrightarrow &\texttt{res = X! / x!} \land \texttt{x} \geq 0 \land \texttt{x} \leq 0\\
\Leftrightarrow &\texttt{res = X! / x!} \land \texttt{x} = 0\\
\Leftrightarrow &\texttt{res = X! / 1} \land \texttt{x} = 0\\
\Leftrightarrow &\texttt{res = X!} \land \texttt{x} = 0
\end{aligned}
$$

- Zeige $\texttt{x} \geq \texttt{0} \land \texttt{res = 1} \Rightarrow$ $\texttt{wp(if (x == 0) ; else while (x > 0) \{ res = res * x; x = x - 1; \}} \mid \texttt{res = X!} \land \texttt{x = 0})$:

$$
\begin{aligned}
&\texttt{wp(if (x == 0) ; else while (x > 0) \{ res = res * x; x = x - 1; \}} \mid \texttt{res = X!} \land \texttt{x = 0})\\
= &(\texttt{x} = 0 \land \texttt{wp(;} \mid \texttt{res = X!} \land \texttt{x = 0})) \lor\\
&(\texttt{x} \neq 0 \land \texttt{wp(while (x > 0) \{ res = res * x; x = x - 1; \}} \mid \texttt{res = X!} \land \texttt{x = 0}))\\
= &(\texttt{x} = 0 \land \texttt{res = X!} \land \texttt{x = 0}) \lor (\texttt{x} \neq 0 \land \texttt{res = X! / x!} \land \texttt{x} \geq 0 \land \texttt{x} \geq 0)\\
\Leftrightarrow &(\texttt{x} = 0 \land \texttt{res = X!}) \lor (\texttt{x} > 0 \land \texttt{res = X! / x!})\\
\overset{\texttt{X = x}}{\Leftrightarrow} &(\texttt{x} = 0 \land \texttt{res = 1}) \lor (\texttt{x} > 0 \land \texttt{res = 1})\\
\Leftrightarrow &(\texttt{x} = 0 \lor \texttt{x} > 0) \land \texttt{res = 1}\\
\Leftrightarrow &\texttt{x} \geq 0 \land \texttt{res = 1}
\end{aligned}
$$

3. Wähle $\texttt{I} := ((\texttt{y}-1)^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}=0)) \land \texttt{y} \ge 0$ und $\texttt{t} := \texttt{x - y + 1}$.

- Zeige $\texttt{I}$ ist eine Schleifeninvariante und $\texttt{t}$ ist eine Terminierungsfunktion:

$$
\begin{aligned}
&\texttt{wp(y = y + 1;} \mid ((\texttt{y}-1)^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}=0)) \land \texttt{y} \ge 0 \land 0 \le \texttt{x}-\texttt{y}+1 \le k)\\
=\ &(\texttt{y}^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}+1=0)) \land \texttt{y} \ge -1 \land 0 \le \texttt{x}-(\texttt{y}+1)+1 \le k\\
\Leftrightarrow\ &(\texttt{y}^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}=-1)) \land \texttt{y} \ge -1 \land 0 \le \texttt{x}-\texttt{y} \le k\\
\Leftrightarrow\ &(\texttt{y}^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}=-1)) \land \texttt{y} \ge -1 \land 1 \le \texttt{x}-\texttt{y}+1 \le k+1\\
\Leftarrow\ &\texttt{y}^2 \le \texttt{x} \land \texttt{y} \ge 0 \land 1 \le \texttt{x}-\texttt{y}+1 \le k+1\\
\Leftarrow\ &((\texttt{y}-1)^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}=0)) \land \texttt{y} \ge 0 \land \texttt{y}^2 \le \texttt{x} \land 0 \le \texttt{x}-\texttt{y}+1 \le k+1
\end{aligned}
$$

  Dabei gilt die letzte Implikation, da:

$$
\begin{aligned}
&((\texttt{y}-1)^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}=0)) \land \texttt{y} \ge 0 \land \texttt{y}^2 \le \texttt{x} \land 0 \le \texttt{x}-\texttt{y}+1 \le k+1\\
\Rightarrow\ &0 \le \texttt{y} \le \texttt{y}^2 \le \texttt{x}\\
\Rightarrow\ &1 \le \texttt{y}+1 \le \texttt{y}^2+1 \le \texttt{x}+1\\
\Rightarrow\ &\texttt{y}+1 \le \texttt{x}+1\\
\Rightarrow\ &1 \le \texttt{x}-\texttt{y}+1
\end{aligned}
$$

- Zeige $\texttt{I} \land \neg(\texttt{y}^2 \le \texttt{x}) \Rightarrow \texttt{wp(res = y - 1;} \mid \texttt{res}^2 \le \texttt{x})$:

$$
\begin{aligned}
&\texttt{I} \land \neg(\texttt{y}^2 \le \texttt{x})\\
\Leftrightarrow\ &((\texttt{y}-1)^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}=0)) \land \texttt{y} \ge 0 \land \texttt{y}^2 > \texttt{x}\\
\Rightarrow\ &(\texttt{y}-1)^2 \le \texttt{x}\\
=\ &\texttt{wp(res = y - 1;} \mid \texttt{res}^2 \le \texttt{x})
\end{aligned}
$$

- Zeige $\texttt{x} \ge 0 \land \texttt{y}=0 \land \texttt{res}=0 \Rightarrow ((\texttt{y}-1)^2 \le \texttt{x} \lor (\texttt{x}=0 \land \texttt{y}=0)) \land \texttt{y} \ge 0 \land \texttt{x}-\texttt{y}+1 \ge 0$:
  - Fall $\texttt{x = 0}$:

    $(0-1)^2 \le 0 \lor (0=0 \land y=0)$ ✓Linker Fall

    $0 \ge 0$ ✓

    $0-0+1 \ge 0$ ✓
  - Fall $\texttt{x > 0}$:

    $(0-1)^2 = 1 \le x \lor (x=0 \land y=0)$ ✓Rechter Fall

    $0 \ge 0$ ✓

    $x-0+1 \ge 0$ ✓

Verifikation

Aufgabe 15.3: Automatisierte Verifikation

Verifizieren Sie das folgende Programm analog zu Beispiel 6.17 aus dem Skript.

```
[ x ≥ 0 ∧ y ≥ 0 ∧ res = 0 ]

y' = y;
while (y > 0)
  _Inv(res = (y' - y) * x && y >= 0)
  _Term(y)
{
    res = res + x;
    y = y - 1;
}

[ res = x * y' ]
```

Lösung

Gegeben sind:

$$
\begin{aligned}
V &:= x \geq 0 \land y \geq 0 \land res = 0 \\
N &:= res = x \cdot y' \\
i &:= res = (y - y') \cdot x \land y \geq 0 \\
e &:= y > 0 \\
t &:= y \\
s &:= res = res + x; y = y - 1;
\end{aligned}
$$

Wir wollen die Allgemeingültigkeit der folgenden Formel (Pämisse für Korrolar 6.7) zeigen:

$$\text{vc}(P \mid N) \land (V \Rightarrow \text{pc}(P \mid N))$$

Wir beginnen mit der rechten Seite der Verundung:

$$
\begin{aligned}
\text{pc}(P \mid N) &= \text{pc}(y' = y; \textbf{while}(y > 0)\ \_\textbf{Inv}(i)\ \_\textbf{Term}(t)\{s\} \mid N) \\
&= \text{pc}(y' = y; | \text{ pc}(\textbf{while}(e)\{s\} \mid N)) \\
&= \text{pc}(y' = y; | \ y \geq 0 \land res = (y' - y) \cdot x \land y \geq 0) \\
&= \text{wp}(y' = y; | \ y \geq 0 \land res = (y' - y) \cdot x \land y \geq 0) \\
&= y \geq 0 \land res = 0 \land y \geq 0
\end{aligned}
$$

$$
\begin{aligned}
&V && \Rightarrow \text{pc}(P \mid N) \\
\Leftrightarrow\ & x \geq 0 \land y \geq 0 \land res = 0 && \Rightarrow y \geq 0 \land res = 0 \land y \geq 0 \\
\Leftrightarrow\ & \text{true}
\end{aligned}
$$

Wir berechnen erst einige Zwischenergebnisse und betrachten dann die die linke Seite der Verundung:

$$
\begin{aligned}
\mathrm{pc}(s \mid N) &= \mathrm{pc}(res = res + x; y = y - 1; \mid res = (y' - y) \cdot x \wedge y \geq 0 \wedge 0 \leq y \leq k) \\
&= \mathrm{pc}(res = res + x; \mid \mathrm{pc}(y = y - 1 \mid res = (y' - y) \cdot x \wedge y \geq 0 \wedge 0 \leq y \leq k)) \\
&= \mathrm{wp}(res = res + x; \mid \mathrm{wp}(y = y - 1 \mid res = (y' - y) \cdot x \wedge y \geq 0 \wedge 0 \leq y \leq k)) \\
&= \mathrm{wp}(res = res + x; \mid res = (y' - (y - 1)) \cdot x \wedge y - 1 \geq 0 \wedge 0 \leq y - 1 \leq k) \\
&= res + x = (y' - (y - 1)) \cdot x \wedge y - 1 \geq 0 \wedge 0 \leq y - 1 \leq k) \\
&\equiv res + x = (y' - (y - 1)) \cdot x \wedge y > 0 \wedge 0 \leq y - 1 \leq k)
\end{aligned}
$$

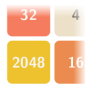
$$
\begin{aligned}
\mathrm{vc}(P \mid N) &\equiv \mathrm{vc}(y' = y; \textbf{while}(e)\ \textbf{\_Inv}(i)\ \textbf{\_Term}(t)\{s\} \mid N) \\
&\equiv \mathrm{vc}(y' = y \mid \mathrm{pc}(\textbf{while}(e)\ \textbf{\_Inv}(i)\ \textbf{\_Term}(t)\{s\} \mid N)) \wedge \mathrm{vc}(\textbf{while}(e)\ \textbf{\_Inv}(i)\ \textbf{\_Term}(t)\{s\} \mid N) \\
&\equiv \mathrm{true} \wedge \mathrm{vc}(\textbf{while}(e)\ \textbf{\_Inv}(i)\ \textbf{\_Term}(t)\{s\} \mid N) \\
&\equiv \mathrm{vc}(\textbf{while}(e)\ \textbf{\_Inv}(i)\ \textbf{\_Term}(t)\{s\} \mid N) \\
&\equiv \mathrm{vc}(s \mid i \wedge 0 \leq y \leq k) \wedge (i \wedge \neg e \Rightarrow N) \\
&\quad \wedge (e \wedge i \wedge 0 \leq y \leq k + 1 \\
&\qquad \Rightarrow \mathrm{pc}(s \mid i \wedge 0 \leq y \leq k)) \\
&\equiv \mathrm{true} \wedge (y \leq 0 \wedge res = (y' - y) \cdot x \wedge y \geq 0 \Rightarrow res = x \cdot y') \\
&\quad \wedge (y > 0 \wedge res = (y' - y) \cdot x \wedge y \geq 0 \wedge 0 \leq y \leq k + 1 \\
&\qquad \Rightarrow \mathrm{pc}(s \mid i \wedge 0 \leq y \leq k)) \\
&\equiv (y = 0 \wedge res = (y' - y) \cdot x \Rightarrow res = x \cdot y') \\
&\quad \wedge (res = (y' - y) \cdot x \wedge 0 < y \leq k + 1 \\
&\qquad \Rightarrow \mathrm{pc}(s \mid i \wedge 0 \leq y \leq k)) \\
&\equiv \mathrm{true} \\
&\quad \wedge (0 < y \leq k + 1 \wedge res = (y' - y) \cdot x) \\
&\quad \Rightarrow (y - 1 \geq 0 \wedge 0 \leq y - 1 \leq k \wedge res + x = (y' - (y - 1)) \cdot x) \\
&\equiv (0 < y \leq k + 1 \wedge res = (y' - y) \cdot x) \\
&\quad \Rightarrow (0 < y \leq k + 1 \wedge res + x = (y' - (y - 1)) \cdot x) \\
&\equiv (0 < y \leq k + 1 \wedge res = y' \cdot x - y \cdot x) \\
&\quad \Rightarrow (0 < y \leq k + 1 \wedge res + x = y' \cdot x - y \cdot x + x) \\
&\equiv \mathrm{true}
\end{aligned}
$$

Daraus ergibt sich:

$$\mathrm{vc}(P \mid N) \wedge (V \Rightarrow \mathrm{pc}(P \mid N)) \equiv \mathrm{true}$$

woraus aus Korollar 6.7 folgt, dass $[V]P[N]$.

Aufgabe 15.4:



Zeigen Sie, dass das folgende Hoare-Tripel gültig ist, indem Sie gültige Invarianten und Terminierungsfunktionen finden, und die Allgemeingültigkeit von $vc(s|N) \wedge V \Rightarrow pc(s|N)$ zeigen.
$[\mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0]$

```
res = 1;
i = 0;
while (i < y) {
  acc = 0;
  j = 0;
  while (j < x) {
    acc = acc + res;
    j = j + 1;
  }
  res = acc;
  i = i + 1;
}
```

$[\ \mathtt{res} = \mathtt{x}^{\mathtt{y}}\ ]$
Was fällt Ihnen auf?

Lösung

Wir definieren

$$\begin{aligned}
i_1 &:= \mathtt{res} = \mathtt{x}^{\mathtt{i}} \wedge \mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \wedge 0 \leq \mathtt{i} \leq \mathtt{y} \\
t_1 &:= \mathtt{y} - \mathtt{i} \\
i_2' &:= \mathtt{acc} = \mathtt{j} * \mathtt{res} \wedge \mathtt{y} > 0 \wedge \mathtt{j} \leq \mathtt{x} \\
i_1' &:= \mathtt{i} < \mathtt{y} \wedge i_1 \wedge 0 \leq t_1 \leq k_1 + 1 \\
i_2 &:= i_2' \wedge i_1' \\
t_2 &:= \mathtt{x} - \mathtt{j}
\end{aligned}$$

wobei i_1 die Invariante, t_1 die Terminierungsfunktion der äußeren Schleife ist und i_2 die Invariante, t_2 die Terminierungsfunktion der Inneren. Dabei ist k_2 die Obergrenze, die notwendig ist, um zu zeigen, dass t_2 eine Terminierungsfunktion ist. Wir müssen insgesamt zeigen, dass $vc(s|N) \wedge V \Rightarrow pc(s|N)$, was zur Konjunktion der folgenden Punkte auswertet, die wir auch gleich beweisen:

- $V \Rightarrow pc(\mathtt{res\ =\ 1;\ i\ =\ 0;}|i_1 \wedge t_1 \geq 0)$:

$$\begin{aligned}
& pc(\mathtt{res\ =\ 1;\ i\ =\ 0;}|i_1 \wedge t_1 \geq 0) \\
=\ & pc(\mathtt{res\ =\ 1;}|pc(\mathtt{i\ =\ 0;}|i_1 \wedge t_1 \geq 0)) \\
=\ & pc(\mathtt{res\ =\ 1;}|\mathtt{res} = \mathtt{x}^0 \wedge \mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \wedge 0 \leq 0 \leq \mathtt{y} \wedge \mathtt{y} - 0 \geq 0) \\
\Leftrightarrow\ & pc(\mathtt{res\ =\ 1;}|\mathtt{res} = 1 \wedge \mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0) \\
=\ & 1 = 1 \wedge \mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \\
\Leftrightarrow\ & \mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \\
\Leftarrow\ & \mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \\
=\ & V
\end{aligned}$$

- $\mathtt{i} < \mathtt{y} \land i_1 \land 0 \leq t_1 \leq k_1 + 1 \Rightarrow pc(\texttt{acc = 0; j = 0;} | i_2 \land t_2 \geq 0)$:

$$\begin{aligned}
& pc(\texttt{acc = 0; j = 0;} | i_2 \land t_2 \geq 0) \\
&= pc(\texttt{acc = 0;} | pc(\texttt{j = 0;} | i_2' \land i_1' \land t_2 \geq 0)) \\
&= pc(\texttt{acc = 0;} | pc(\texttt{j = 0;} | \mathtt{acc} = \mathtt{j} * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{j} \leq \mathtt{x} \land i_1' \land \mathtt{x} - \mathtt{j} \geq 0)) \\
&= pc(\texttt{acc = 0;} | \mathtt{acc} = 0 * \mathtt{res} \land \mathtt{y} > 0 \land 0 \leq \mathtt{x} \land i_1' \land \mathtt{x} - 0 \geq 0) && |\mathtt{j} \text{ nicht in } i_1' \\
&\Leftrightarrow pc(\texttt{acc = 0;} | \mathtt{acc} = 0 \land \mathtt{y} > 0 \land i_1') && |0 \leq \mathtt{x} \text{ bereits in } i_1' \\
&= 0 = 0 \land \mathtt{y} > 0 \land i_1' && |\mathtt{acc} \text{ nicht in } i_1' \\
&\Leftrightarrow \mathtt{y} > 0 \land \mathtt{i} < \mathtt{y} \land i_1 \land 0 \leq t_1 \leq k_1 + 1 \\
&\Leftarrow \mathtt{i} < \mathtt{y} \land i_1 \land 0 \leq t_1 \leq k_1 + 1
\end{aligned}$$

  Die Implikation am Ende ist gültig, da insbesondere:

$$\begin{aligned}
& \mathtt{i} < \mathtt{y} \land i_1 \land 0 \leq t_1 \leq k_1 + 1 \\
&\Rightarrow \mathtt{i} < \mathtt{y} \land \mathtt{res} = \mathtt{x}^{\mathtt{i}} \land \mathtt{x} \geq 0 \land \mathtt{y} \geq 0 \land 0 \leq \mathtt{i} \leq \mathtt{y} \\
&\Rightarrow \mathtt{i} < \mathtt{y} \land 0 \leq \mathtt{i} \\
&\Rightarrow 0 < \mathtt{y}
\end{aligned}$$

- $\mathtt{j} < \mathtt{x} \land i_2 \land 0 \leq t_2 \leq k_2 + 1 \Rightarrow pc(\texttt{acc = acc + res; j = j + 1;} | i_2 \land 0 \leq t_2 \leq k_2)$:

$$\begin{aligned}
& pc(\texttt{acc = acc + res; j = j + 1;} | i_2' \land i_1' \land 0 \leq t_2 \leq k_2) \\
&= pc(\texttt{acc = acc + res;} | pc(\texttt{j = j + 1;} | \mathtt{acc} = \mathtt{j} * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{j} \leq \mathtt{x} \land i_1' \land 0 \leq \mathtt{x} - \mathtt{j} \leq k_2)) \\
&= pc(\texttt{acc = acc + res;} | \mathtt{acc} = (\mathtt{j} + 1) * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{j} + 1 \leq \mathtt{x} \land i_1' \land 0 \leq \mathtt{x} - (\mathtt{j} + 1) \leq k_2) && |\mathtt{j} \text{ nicht in } i_1' \\
&= \mathtt{acc} + \mathtt{res} = (\mathtt{j} + 1) * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{j} + 1 \leq \mathtt{x} \land i_1' \land 0 \leq \mathtt{x} - (\mathtt{j} + 1) \leq k_2 && |\mathtt{acc} \text{ nicht in } i_1' \\
&\Leftrightarrow \mathtt{acc} = \mathtt{j} * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{j} + 1 \leq \mathtt{x} \land i_1' \land 0 \leq \mathtt{x} - \mathtt{j} - 1 \leq k_2 \\
&\Leftrightarrow \mathtt{acc} = \mathtt{j} * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{j} + 1 \leq \mathtt{x} \land i_1' \land 1 \leq \mathtt{x} - \mathtt{j} \leq k_2 + 1 \\
&\Leftarrow \mathtt{j} < \mathtt{x} \land \mathtt{acc} = \mathtt{j} * \mathtt{res} \land \mathtt{y} > 0 \land i_1' \land 0 \leq \mathtt{x} - \mathtt{j} \leq k_2 + 1 \\
&\Leftrightarrow \mathtt{j} < \mathtt{x} \land i_2 \land 0 \leq t_2 \leq k_2 + 1
\end{aligned}$$

  Die Implikation am Ende ist gültig, da insbesondere:

$$\begin{aligned}
& \mathtt{j} < \mathtt{x} \land \mathtt{acc} = \mathtt{j} * \mathtt{res} \land \mathtt{y} > 0 \land i_1' \land 0 \leq \mathtt{x} - \mathtt{j} \leq k_2 + 1 \\
&\Rightarrow \mathtt{j} < \mathtt{x} \\
&\Rightarrow 0 < \mathtt{x} - \mathtt{j} \land \mathtt{j} + 1 \leq \mathtt{x} \\
&\Rightarrow 1 \leq \mathtt{x} - \mathtt{j} \land \mathtt{j} + 1 \leq \mathtt{x}
\end{aligned}$$

- $\neg(\mathtt{j} < \mathtt{x}) \land i_2 \Rightarrow pc(\texttt{res = acc; i = i + 1;} | i_1 \land 0 \leq t_1 \leq k_1)$:

$$\begin{aligned}
& pc(\texttt{res = acc; i = i + 1;} | \mathtt{res} = \mathtt{x}^{\mathtt{i}} \land \mathtt{x} \geq 0 \land \mathtt{y} \geq 0 \land 0 \leq \mathtt{i} \leq \mathtt{y} \land 0 \leq \mathtt{y} - \mathtt{i} \leq k_1) \\
&= pc(\texttt{res = acc;} | pc(\texttt{i = i + 1;} | \mathtt{res} = \mathtt{x}^{\mathtt{i}} \land \mathtt{x} \geq 0 \land \mathtt{y} \geq 0 \land 0 \leq \mathtt{i} \leq \mathtt{y} \land 0 \leq \mathtt{y} - \mathtt{i} \leq k_1)) \\
&= pc(\texttt{res = acc;} | \mathtt{res} = \mathtt{x}^{\mathtt{i}+1} \land \mathtt{x} \geq 0 \land \mathtt{y} \geq 0 \land 0 \leq \mathtt{i} + 1 \leq \mathtt{y} \land 0 \leq \mathtt{y} - (\mathtt{i} + 1) \leq k_1) \\
&= \mathtt{acc} = \mathtt{x}^{\mathtt{i}+1} \land \mathtt{x} \geq 0 \land \mathtt{y} \geq 0 \land 0 \leq \mathtt{i} + 1 \leq \mathtt{y} \land 0 \leq \mathtt{y} - (\mathtt{i} + 1) \leq k_1 \\
&\Leftrightarrow \mathtt{acc} = \mathtt{x} * \mathtt{x}^{\mathtt{i}} \land \mathtt{x} \geq 0 \land \mathtt{y} \geq 0 \land 0 \leq \mathtt{i} + 1 \leq \mathtt{y} \land 1 \leq \mathtt{y} - \mathtt{i} \leq k_1 + 1 \\
&\Leftarrow \mathtt{acc} = \mathtt{x} * \mathtt{x}^{\mathtt{i}} \land 0 < \mathtt{i} < \mathtt{y} \land \mathtt{x} \geq 0 \land 0 \leq \mathtt{y} - \mathtt{i} \leq k_1 + 1 \\
&\Leftarrow \mathtt{acc} = \mathtt{x} * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{i} < \mathtt{y} \land \mathtt{res} = \mathtt{x}^{\mathtt{i}} \land \mathtt{x} \geq 0 \land \mathtt{y} \geq 0 \land 0 \leq \mathtt{i} \leq \mathtt{y} \land 0 \leq \mathtt{y} - \mathtt{i} \leq k_1 + 1 \\
&\Leftarrow \mathtt{j} = \mathtt{x} \land \mathtt{acc} = \mathtt{j} * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{i} < \mathtt{y} \land i_1 \land 0 \leq \mathtt{y} - \mathtt{i} \leq k_1 + 1 \\
&\Leftarrow \mathtt{j} \geq \mathtt{x} \land \mathtt{acc} = \mathtt{j} * \mathtt{res} \land \mathtt{y} > 0 \land \mathtt{j} \leq \mathtt{x} \land \mathtt{i} < \mathtt{y} \land i_1 \land 0 \leq \mathtt{y} - \mathtt{i} \leq k_1 + 1 \\
&\Leftrightarrow \neg(\mathtt{j} < \mathtt{x}) \land i_2
\end{aligned}$$

- $\neg(\mathtt{i} < \mathtt{y}) \wedge i_1 \Rightarrow N$:

$$\begin{aligned}
&\neg(\mathtt{i} < \mathtt{y}) \wedge i_1 \\
\Rightarrow\ &\mathtt{i} \geq \mathtt{y} \wedge \mathtt{res} = \mathtt{x}^{\mathtt{i}} \wedge \mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \wedge 0 \leq \mathtt{i} \leq \mathtt{y} \\
\Rightarrow\ &\mathtt{i} = \mathtt{y} \wedge \mathtt{res} = \mathtt{x}^{\mathtt{i}} \wedge \mathtt{x} \geq 0 \wedge \mathtt{y} \geq 0 \\
\Rightarrow\ &\mathtt{res} = \mathtt{x}^{\mathtt{y}} \\
=\ &V
\end{aligned}$$

Damit ist gezeigt, dass all diese Formeln allgemeingültig sind. Das Programm ist also korrekt.

Interessanterweise ist es hier notwendig, dass die Invariante i_2 Aussagen über die Terminierung der äußeren Schleife trefft, also insbesondere das k_1 enthält. Laut Skript darf das k im Programm nicht vorkommen. Die Art der Verwendung, die wir hier erlauben (nur in Schleifeninvarianten) ist jedoch zulässig, da das k insgesamt seinen Wert nicht über den Verlauf ändert, da ihm nichts zugewiesen werden kann, denn Auftreten im eigentlichen Programm (und nicht nur in den virtuellen Teilen wie Invariante) ist weiterhin verboten.