Lehrstuhl für Sprachen und Beschreibungsstrukturen WS 2008/09
Einführung in die Informatik 2 **Übungsblatt 3**
Prof. Dr. Helmut Seidl, T.M. Gawlitza, S. Pott 28.10.2008

Abgabe: 04.11.2008 (vor der Vorlesung)

Aufgabe 3.1 (H) Division mit Rest

Schreiben Sie ein MiniJava-Programm, das zwei ganze Zahlen `a` und `b` einliest und dann folgende Berechnung ausführt: Falls eine der beiden Zahlen negativ ist, dann soll 0 ausgegeben werden. Andernfalls soll sowohl `a` **div** `b` als auch `a` **mod** `b` ausgegeben werden. Werden beispielsweise 14 und 3 eingeben, so sollen 4 und 2 ausgegeben werden, da $14 = 4 \cdot 3 + 2$ gilt.

Bei der Implementierung dürfen jedoch Multiplikationen und Divisionen **nicht** verwendet werden. An arithmetischen Operationen sind lediglich Additionen und Subtraktionen erlaubt.

a) Schreiben Sie das MiniJava-Programm! (Dabei sind erklärende Kommentare selbstverständlich!)

b) Testen Sie Ihr MiniJava-Programm! Sie können das MiniJava-Programm auch dazu benutzen, um die Gültigkeit von Zusicherungen mithilfe von `assert`-Anweisungen zu testen.

c) Erstellen Sie das Kontrollfluß-Diagramm!

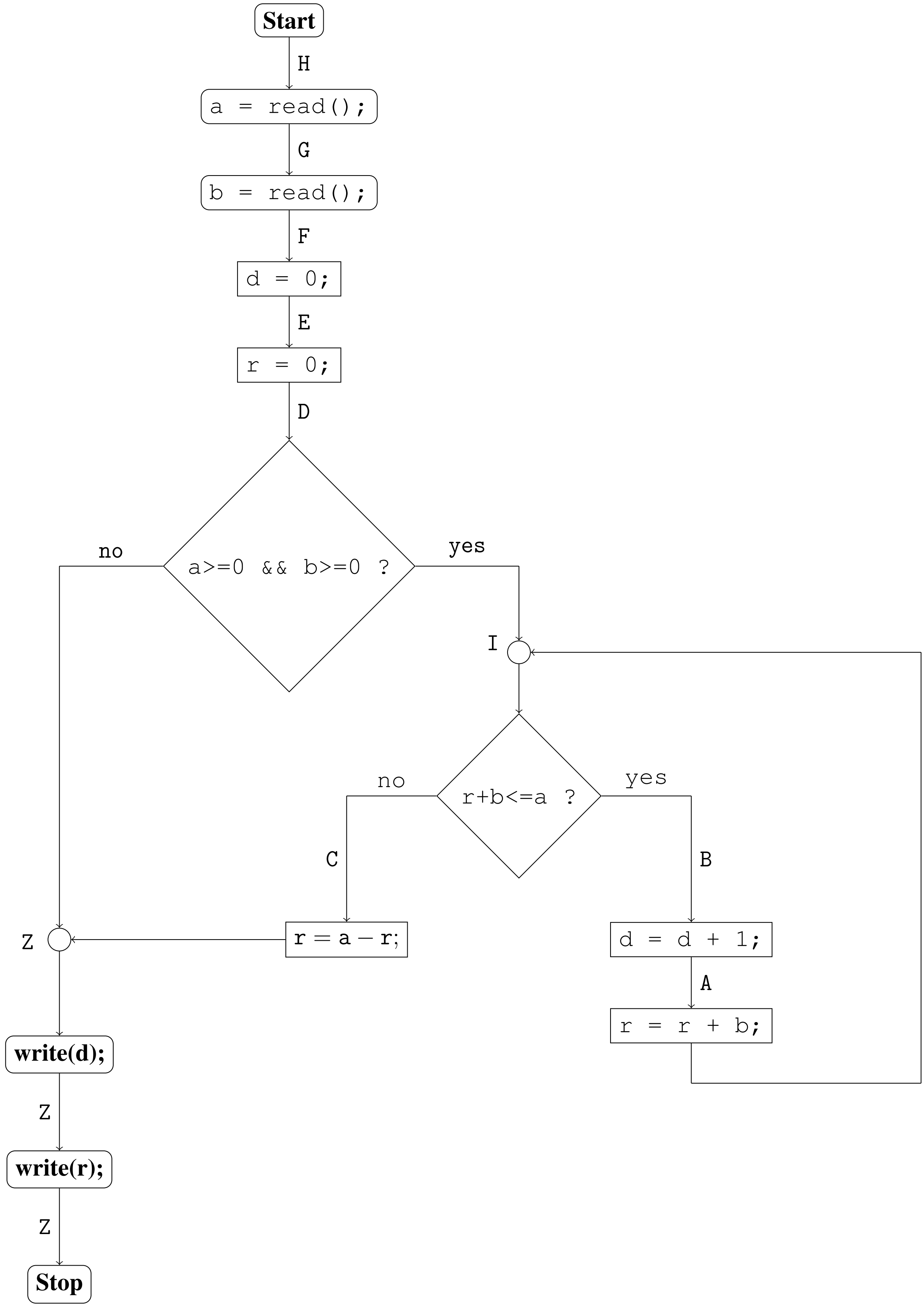
d) Zeigen Sie, dass Ihr Programm korrekt ist!

Lösungsvorschlag 3.1

a)
```
int a, b, d, r;

a = read();
b = read();
d = 0;
r = 0;
if (a >= 0 && b >= 0) {
  while(r + b <= a) {
    d = d + 1;
    r = r + b;
  }
  r = a - r;
}
write(d);
write(r);
```

b) Funktioniert!

c)



d) Wir setzen

$$\mathtt{Z} :\equiv (\mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}+\mathtt{r}=\mathtt{a} \land 0 \leq \mathtt{r} < \mathtt{b}) \lor (\neg(\mathtt{a},\mathtt{b}\geq 0) \land \mathtt{d}=0 \land \mathtt{r}=0).$$

Anmerkung: Es gilt

$$\mathtt{Z} \equiv (\mathtt{a},\mathtt{b} \geq 0 \Rightarrow (\mathtt{d}\cdot\mathtt{b}+\mathtt{r}=\mathtt{a} \land 0 \leq \mathtt{r} < \mathtt{b})) \land (\neg(\mathtt{a},\mathtt{b}\geq 0) \Rightarrow (\mathtt{d}=0 \land \mathtt{r}=0)).$$

Es ergibt sich

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{r = a - r;}]\!](\mathtt{Z}) &\equiv (\mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}+\mathtt{a}-\mathtt{r}=\mathtt{a} \land 0 \leq \mathtt{a}-\mathtt{r} < \mathtt{b}) \\
&\qquad \lor (\neg(\mathtt{a},\mathtt{b}\geq 0) \land \mathtt{d}=0 \land \mathtt{a}-\mathtt{r}=0) \\
&\Leftarrow (\mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}+\mathtt{a}-\mathtt{r}=\mathtt{a} \land 0 \leq \mathtt{a}-\mathtt{r} < \mathtt{b}) \\
&\equiv (\mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r} \land \mathtt{r}+\mathtt{b} > \mathtt{a} \geq \mathtt{r}) \\
&\equiv: \mathtt{C}.
\end{aligned}$$

Wir raten die Schleifen-Invariante

$$\mathtt{I} :\equiv \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{r} \leq \mathtt{a} \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r}.$$

Es ergibt sich

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{r = r + b;}]\!](\mathtt{I}) &\equiv \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{r}+\mathtt{b} \leq \mathtt{a} \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r}+\mathtt{b} \\
&\equiv: \mathtt{A}
\end{aligned}$$

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{d = d + 1;}]\!](\mathtt{A}) &\equiv \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{r}+\mathtt{b} \leq \mathtt{a} \land (\mathtt{d}+1)\cdot\mathtt{b}=\mathtt{r}+\mathtt{b} \\
&\equiv \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{r}+\mathtt{b} \leq \mathtt{a} \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r} \\
&\equiv: \mathtt{B}
\end{aligned}$$

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{r + b <= a}]\!](\mathtt{C},\mathtt{B}) &\equiv (\mathtt{r}+\mathtt{b} > \mathtt{a} \land \mathtt{r} \leq \mathtt{a} \land \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r}) \\
&\qquad \lor (\mathtt{r}+\mathtt{b} \leq \mathtt{a} \land \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r}) \\
&\Leftarrow (\mathtt{r}+\mathtt{b} > \mathtt{a} \land \mathtt{r} \leq \mathtt{a} \land \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r}) \\
&\qquad \lor (\mathtt{r}+\mathtt{b} \leq \mathtt{a} \land \mathtt{r} \leq \mathtt{a} \land \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r}) \\
&\equiv (\mathtt{r}+\mathtt{b} > \mathtt{a} \lor \mathtt{r}+\mathtt{b} \leq \mathtt{a}) \land \mathtt{r} \leq \mathtt{a} \land \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r} \\
&\equiv \mathtt{r} \leq \mathtt{a} \land \mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r} \\
&\equiv \mathtt{I}
\end{aligned}$$

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{a >= 0 \&\& b >= 0}]\!](\mathtt{Z},\mathtt{I}) &\equiv (\neg(\mathtt{a},\mathtt{b}\geq 0) \land \mathtt{Z}) \lor (\mathtt{a},\mathtt{b} \geq 0 \land \mathtt{I}) \\
&\Leftarrow (\neg(\mathtt{a},\mathtt{b}\geq 0) \land \mathtt{d}=0 \land \mathtt{r}=0) \lor (\mathtt{a},\mathtt{b} \geq 0 \land \mathtt{r} \leq \mathtt{a} \land \mathtt{d}\cdot\mathtt{b}=\mathtt{r}) \\
&\Leftarrow (\neg(\mathtt{a},\mathtt{b}\geq 0) \land \mathtt{d}=0 \land \mathtt{r}=0) \lor (\mathtt{a},\mathtt{b} \geq 0 \land \mathtt{d}=0 \land \mathtt{r}=0) \\
&\equiv \mathtt{d}=0 \land \mathtt{r}=0 \\
&\equiv: \mathtt{D}
\end{aligned}$$

$$\mathbf{WP}[\![\mathtt{r = 0;}]\!](\mathtt{D}) \equiv \mathtt{d}=0 \equiv: \mathtt{E}$$

$$\mathbf{WP}[\![\mathtt{d = 0;}]\!](\mathtt{E}) \equiv \mathbf{true} \equiv: \mathtt{F}$$

$$\mathbf{WP}[\![\mathtt{b = read();}]\!](\mathtt{F}) \equiv \mathbf{true} \equiv: \mathtt{G}$$

$$\mathbf{WP}[\![\mathtt{a = read();}]\!](\mathtt{G}) \equiv \mathbf{true} \equiv: \mathtt{H}$$

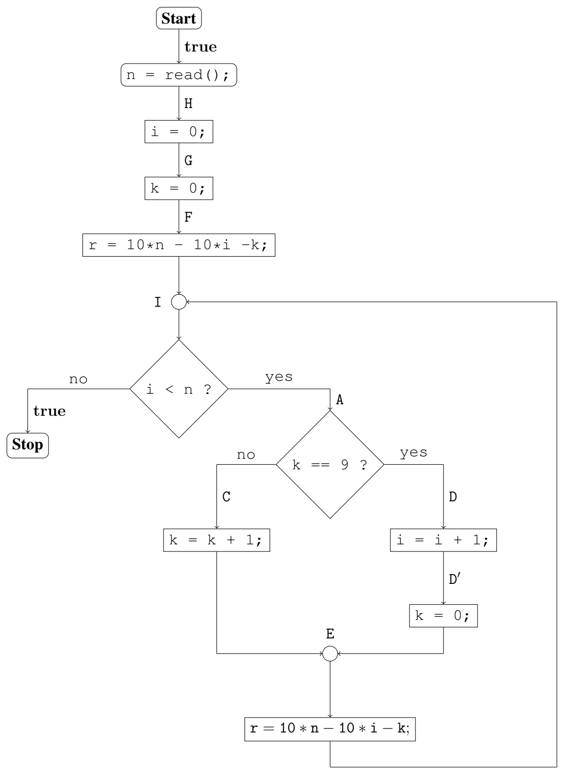
Aufgabe 3.2 (P) Terminierung

Zeigen Sie, dass jede Ausführung des folgenden Programms terminiert!

```
int i, k, n;
n = read();
i = 0;
k = 0;
while (i < n) {
  if (k == 9) {
    i = i + 1;
    k = 0;
  } else {
    k = k + 1;
  }
}
```

Lösungsvorschlag 3.2

Wir erstellen zunächst das *instrumentierte* Kontrollfluß-Diagramm.



Wir raten die Schleifen-Invariante

$$\mathtt{I} :\equiv \mathtt{r} = 10 \cdot \mathtt{n} - 10 \cdot \mathtt{i} - \mathtt{k} \wedge \mathtt{k} \leq 9.$$

Entsprechend setzen wir

$$\mathtt{A} :\equiv \mathtt{i} < \mathtt{n} \wedge \mathtt{I}.$$

Für die Terminierung ist wichtig, dass

$$\mathtt{A} \Rightarrow \mathtt{r} > 0 \tag{1}$$

gilt. Dies bedeutet, dass $\texttt{r} > 0$ immer dann gilt, wenn die Schleife betreten wird. Dies wird wie folgt bewiesen:

$$\begin{aligned}
\texttt{A} &\equiv \texttt{r} = 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k} \land \texttt{k} \leq 9 \land \texttt{i} < \texttt{n} \\
&\Rightarrow \texttt{r} > 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - 10 \land \texttt{i} < \texttt{n} \\
&\Rightarrow \texttt{r} > 10 \cdot (\texttt{n} - \texttt{i} - 1) \land \texttt{i} < \texttt{n} \\
&\Rightarrow \texttt{r} > 0
\end{aligned}$$

Die lokale Konsistenz am ersten Bedingungsknoten gilt, denn es gilt

$$\begin{aligned}
\mathbf{WP}[\![\texttt{i} < \texttt{n}]\!](\mathbf{true}, \texttt{A}) &\equiv (\texttt{i} \geq \texttt{n} \land \mathbf{true}) \lor (\texttt{i} < \texttt{n} \land \texttt{A}) \\
&\equiv \texttt{i} \geq \texttt{n} \lor (\texttt{i} < \texttt{n} \land \texttt{I}) \\
&\Leftarrow (\texttt{i} \geq \texttt{n} \land \texttt{I}) \lor (\texttt{i} < \texttt{n} \land \texttt{I}) \\
&\equiv (\texttt{i} \geq \texttt{n} \lor \texttt{i} < \texttt{n}) \land \texttt{I} \\
&\equiv \mathbf{true} \land \texttt{I} \\
&\equiv \texttt{I}.
\end{aligned}$$

Weiterhin gilt

$$\mathbf{WP}[\![\texttt{r} = 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k}]\!](\texttt{I}) \equiv \texttt{k} \leq 9.$$

Wir setzen

$$\texttt{E} :\equiv \texttt{r} > 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k} \land \texttt{k} \leq 9.$$

Für die Terminierung ist wichtig, dass offensichtlich

$$\texttt{E} \Rightarrow \texttt{r} > 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k} \tag{2}$$

gilt. Dies bedeutet, dass die Variable $\texttt{r}$ in jedem Schleifen-Durchlauf kleiner wird.

Entsprechend setzen wir:

$$\mathbf{WP}[\![\texttt{k} = 0;]\!](\texttt{E}) \equiv \texttt{r} > 10 \cdot \texttt{n} - 10 \cdot \texttt{i} \land 0 \leq 9 \equiv \texttt{r} > 10 \cdot \texttt{n} - 10 \cdot \texttt{i} \equiv: \texttt{D}'$$

$$\mathbf{WP}[\![\texttt{i} = \texttt{i} + 1;]\!](\texttt{D}') \equiv \texttt{r} > 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - 10 \equiv: \texttt{D}$$

$$\mathbf{WP}[\![\texttt{k} = \texttt{k} + 1;]\!](\texttt{E}) \equiv \texttt{r} \geq 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k} \land \texttt{k} < 9 \equiv: \texttt{C}$$

Als nächstes zeigen wir die lokale Konsistenz am zweiten Bedingungsknoten.

$$\begin{aligned}
\mathbf{WP}[\![\texttt{k} == 9]\!](\texttt{C}, \texttt{D}) &\equiv (\texttt{k} \neq 9 \land \texttt{C}) \lor (\texttt{k} = 9 \land \texttt{D}) \\
&\equiv (\texttt{k} \neq 9 \land \texttt{r} \geq 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k} \land \texttt{k} < 9) \lor (\texttt{k} = 9 \land \texttt{r} > 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - 10) \\
&\equiv (\texttt{k} < 9 \land \texttt{r} \geq 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k}) \lor (\texttt{k} = 9 \land \texttt{r} > 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - 10) \\
&\equiv (\texttt{k} < 9 \land \texttt{r} \geq 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k}) \lor (\texttt{k} = 9 \land \texttt{r} \geq 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k}) \\
&\equiv (\texttt{k} < 9 \lor \texttt{k} = 9) \land \texttt{r} \geq 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k} \\
&\equiv \texttt{k} \leq 9 \land \texttt{r} \geq 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k} \\
&\Leftarrow \texttt{k} \leq 9 \land \texttt{r} \geq 10 \cdot \texttt{n} - 10 \cdot \texttt{i} - \texttt{k} \land \texttt{i} < \texttt{n} \\
&\equiv \texttt{A}
\end{aligned}$$

Weiter geht's wie folgt:

$$\mathbf{WP}[\![\texttt{r} = 10 * \texttt{n} - 10 * \texttt{i} - \texttt{k};]\!](\texttt{I}) \equiv \texttt{k} \leq 9 \equiv: \texttt{F}$$

$$\mathbf{WP}[\![\texttt{k} = \texttt{0;}]\!](\texttt{F}) \equiv \texttt{0} \leq \texttt{9} \equiv \mathbf{true} \equiv: \texttt{G}$$

$$\mathbf{WP}[\![\texttt{i} = \texttt{0;}]\!](\texttt{G}) \equiv \mathbf{true} \equiv: \texttt{H}$$

$$\mathbf{WP}[\![\texttt{n} = \texttt{read();}]\!](\texttt{H}) \equiv \forall \texttt{n}.\mathbf{true} \equiv \mathbf{true}$$

Zusammenfassend sind folgende Aussagen gezeigt:

a) Die so gewählten Zusicherungen sind lokal konsistent.
b) Der Start-Knoten ist mit $\mathbf{true}$ annotiert.
c) Beim Betreten der Schleife gilt stets $\texttt{r} > \texttt{0}$ (siehe (1)).
d) Mit jedem Schleifen-Durchlauf wird $\texttt{r}$ kleiner (siehe (2)).

Aufgabe 3.3 (P) Stellenweise Multiplikation

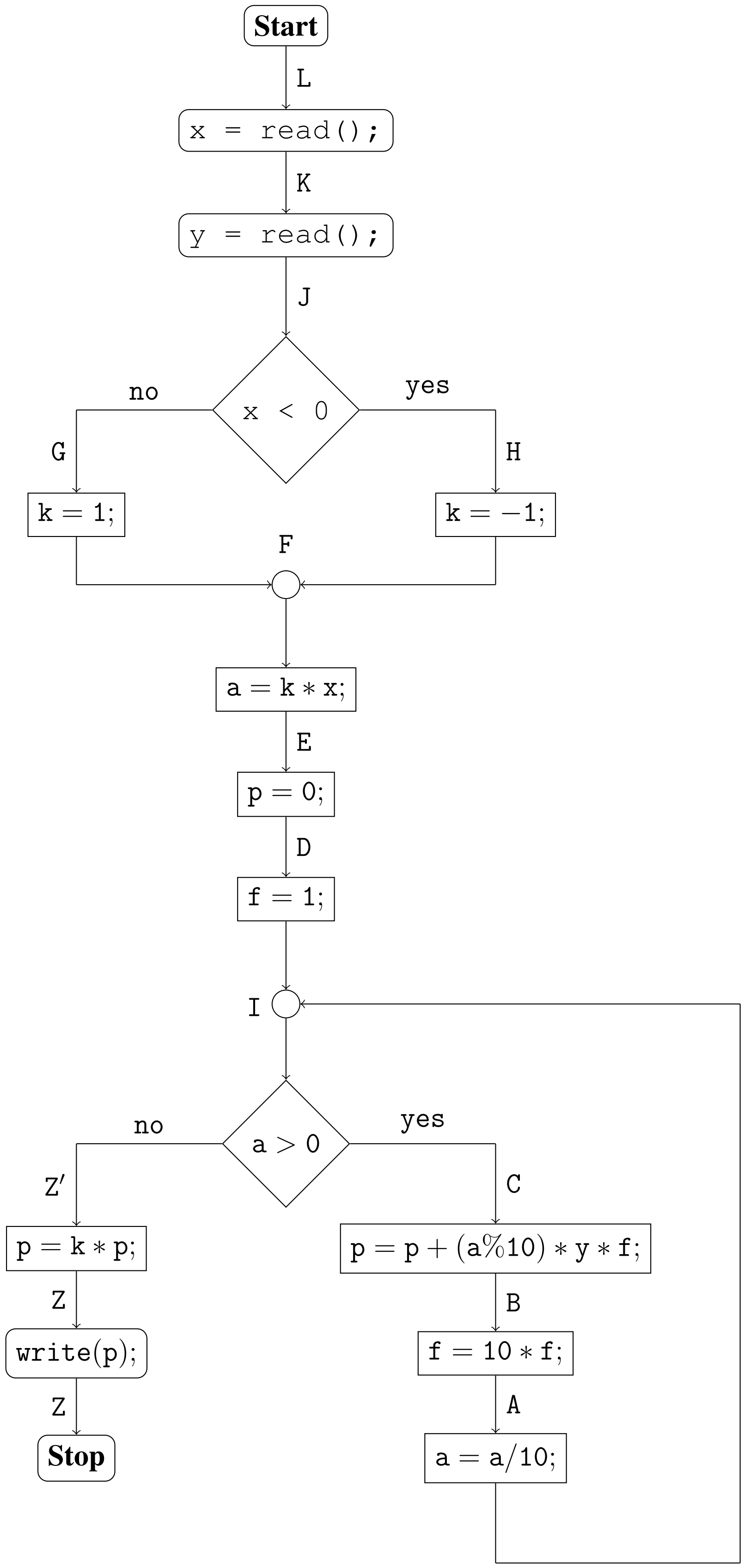
Gegeben sei das folgende MiniJava-Programm:

```
int a, x, y, f, p, k;

x = read();
y = read();
if (x < 0)
  k = -1;
else
  k = 1;
a = k * x;
p = 0;
f = 1;

while (a > 0) {
  p = p + (a % 10) * y * f;
  f = 10 * f;
  a = a / 10;
}
p = k * p;
write(p);
```

Zeigen Sie, dass das Produkt der beiden eingelesenen Zahlen ausgegeben wird!

Hinweis: Für alle $a, b, c \in \mathbb{Z}$ gilt $a \textbf{ mod } bc = b\,((a \textbf{ div } b) \textbf{ mod } c) + a \textbf{ mod } b$.

Lösungsvorschlag 3.3
Wir erstellen zunächst das Kontrollfluß-Diagramm.



Lösung 1

Wir setzen

$$\mathtt{Z} :\equiv \mathtt{p} = \mathtt{xy}.$$

Dann folgt

$$\mathbf{WP}[\![\mathtt{p} = \mathtt{k} * \mathtt{p};]\!](\mathtt{Z}) \equiv \mathtt{kp} = \mathtt{xy} \equiv: \mathtt{Z}'$$

Wir setzen

$$\mathtt{P}(\mathtt{x}, \mathtt{k}) :\equiv \mathtt{k}^2 = \mathtt{1} \wedge \mathtt{kx} \geq \mathtt{0}$$

und raten die Schleifen-Invariante

$$\mathtt{I} :\equiv \mathtt{0} \leq \mathtt{a} = \mathtt{kx}\ \mathbf{div}\ \mathtt{f} \wedge \mathtt{p} = \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{f}) \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}).$$

Es folgt:

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{a} = \mathtt{a}/\mathtt{10};]\!](\mathtt{I}) &\equiv \mathtt{0} \leq \mathtt{a}\ \mathbf{div}\ \mathtt{10} = \mathtt{kx}\ \mathbf{div}\ \mathtt{f} \wedge \mathtt{p} = \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{f}) \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv: \mathtt{A}.
\end{aligned}$$

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{f} = \mathtt{10} * \mathtt{f};]\!](\mathtt{A}) &\equiv \mathtt{0} \leq \mathtt{a}\ \mathbf{div}\ \mathtt{10} = \mathtt{kx}\ \mathbf{div}\ \mathtt{10f} \wedge \mathtt{p} = \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{10f}) \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\Leftarrow \mathtt{0} \leq \mathtt{a} = \mathtt{kx}\ \mathbf{div}\ \mathtt{f} \wedge \mathtt{p} = \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{10f}) \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{B}.
\end{aligned}$$

$$\begin{aligned}
&\mathbf{WP}[\![\mathtt{p} = \mathtt{p} + (\mathtt{a\%10}) * \mathtt{y} * \mathtt{f};]\!](\mathtt{B}) \\
&\equiv \mathtt{0} \leq \mathtt{a} = \mathtt{kx}\ \mathbf{div}\ \mathtt{f} \wedge \mathtt{p} + (\mathtt{a}\ \mathbf{mod}\ \mathtt{10})\mathtt{yf} = \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{10f}) \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{0} \leq \mathtt{a} = \mathtt{kx}\ \mathbf{div}\ \mathtt{f} \wedge \mathtt{p} + (\mathtt{a}\ \mathbf{mod}\ \mathtt{10})\mathtt{yf} = \mathtt{y}(((\mathtt{kx}\ \mathbf{div}\ \mathtt{f})\ \mathbf{mod}\ \mathtt{10})\mathtt{f} + \mathtt{kx}\ \mathbf{mod}\ \mathtt{f}) \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{0} \leq \mathtt{a} = \mathtt{kx}\ \mathbf{div}\ \mathtt{f} \wedge \mathtt{p} + (\mathtt{a}\ \mathbf{mod}\ \mathtt{10})\mathtt{yf} = (\mathtt{a}\ \mathbf{mod}\ \mathtt{10})\mathtt{yf} + \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{f}) \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{0} \leq \mathtt{a} = \mathtt{kx}\ \mathbf{div}\ \mathtt{f} \wedge \mathtt{p} = \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{f}) \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{I} \\
&\equiv: \mathtt{C}.
\end{aligned}$$

Wir müssen noch folgendes zeigen

$$\mathtt{I} \Rightarrow \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C}).$$

Dazu nehmen wir an, dass $\sigma \models \mathtt{I}$ gilt. Wir müssen zeigen, dass $\sigma \models \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$ gilt. Wir unterscheiden zwei Fälle.

Fall 1: Es gilt $\sigma \models \mathtt{a} > \mathtt{0}$. Da $\sigma \models \mathtt{I}$ gilt, gilt auch $\sigma \models \mathtt{a} > \mathtt{0} \wedge \mathtt{I}$. Damit gilt auch $\sigma \models (\mathtt{a} \leq \mathtt{0} \wedge \mathtt{Z}') \vee (\mathtt{a} > \mathtt{0} \wedge \mathtt{I})$. Da $(\mathtt{a} \leq \mathtt{0} \wedge \mathtt{Z}') \vee (\mathtt{a} > \mathtt{0} \wedge \mathtt{I}) \equiv \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$ gilt, gilt auch $\sigma \models \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$.

Fall 2: Es gilt $\sigma \models \mathtt{a} \leq \mathtt{0}$. Da $\sigma \models \mathtt{I}$ gilt, folgt $\sigma \models \mathtt{0} = \mathtt{a} = \mathtt{kx}\ \mathbf{div}\ \mathtt{f}$. Damit gilt $\sigma \models \mathtt{p} = \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{f}) = \mathtt{ykx}$. Durch Multiplizieren der Gleichung mit k erhält man, dass $\sigma \models \mathtt{kp} = \mathtt{k}^2\mathtt{xy}$ gilt. Da zusätzlich $\sigma \models \mathtt{k}^2 = \mathtt{1}$ gilt, gilt $\sigma \models \mathtt{kp} = \mathtt{xy}$. Damit gilt $\sigma \models (\mathtt{a} \leq \mathtt{0} \wedge \mathtt{kp} = \mathtt{xy}) \vee (\mathtt{a} > \mathtt{0} \wedge \mathtt{C})$. Da $(\mathtt{a} \leq \mathtt{0} \wedge \mathtt{kp} = \mathtt{xy}) \vee (\mathtt{a} > \mathtt{0} \wedge \mathtt{C}) \equiv \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$ gilt, folgt $\sigma \models \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$.

Weiter geht's:

$$\begin{aligned}\mathbf{WP}[\![\mathtt{f = 1;}]\!](\mathtt{I}) &\equiv \mathtt{0} \le \mathtt{a} = \mathtt{kx}\ \mathbf{div}\ \mathtt{1} \wedge \mathtt{p} = \mathtt{y}(\mathtt{kx}\ \mathbf{mod}\ \mathtt{1}) \wedge \mathtt{P}(\mathtt{x},\mathtt{k})\\ &\equiv \mathtt{0} \le \mathtt{a} = \mathtt{kx} \wedge \mathtt{p} = \mathtt{0} \wedge \mathtt{P}(\mathtt{x},\mathtt{k})\\ &\equiv: \mathtt{D}\end{aligned}$$

$$\begin{aligned}\mathbf{WP}[\![\mathtt{p = 0;}]\!](\mathtt{D}) &\equiv \mathtt{0} \le \mathtt{a} = \mathtt{kx} \wedge \mathtt{0} = \mathtt{0} \wedge \mathtt{P}(\mathtt{x},\mathtt{k})\\ &\equiv \mathtt{0} \le \mathtt{a} = \mathtt{kx} \wedge \mathtt{P}(\mathtt{x},\mathtt{k})\\ &\equiv: \mathtt{E}\end{aligned}$$

$$\begin{aligned}\mathbf{WP}[\![\mathtt{a = k * x;}]\!](\mathtt{E}) &\equiv \mathtt{0} \le \mathtt{kx} = \mathtt{kx} \wedge \mathtt{P}(\mathtt{x},\mathtt{k})\\ &\equiv \mathtt{P}(\mathtt{x},\mathtt{k})\\ &\equiv: \mathtt{F}\end{aligned}$$

$$\begin{aligned}\mathbf{WP}[\![\mathtt{k = 1;}]\!](\mathtt{F}) &\equiv \mathtt{P}(\mathtt{x},\mathtt{1})\\ &\equiv \mathtt{x} \ge \mathtt{0}\\ &\equiv: \mathtt{G}\end{aligned}$$

$$\begin{aligned}\mathbf{WP}[\![\mathtt{k = -1;}]\!](\mathtt{F}) &\equiv \mathtt{P}(\mathtt{x},-\mathtt{1})\\ &\equiv \mathtt{x} \le \mathtt{0}\\ &\equiv: \mathtt{H}\end{aligned}$$

$$\begin{aligned}\mathbf{WP}[\![\mathtt{x < 0}]\!](\mathtt{G},\mathtt{H}) &\equiv (\mathtt{x} \ge \mathtt{0} \wedge \mathtt{x} \ge \mathtt{0}) \vee (\mathtt{x} < \mathtt{0} \wedge \mathtt{x} \le \mathtt{0})\\ &\equiv \mathtt{x} \ge \mathtt{0} \vee \mathtt{x} < \mathtt{0}\\ &\equiv \mathbf{true} \equiv: \mathtt{J} \equiv: \mathtt{K} \equiv: \mathtt{L}\end{aligned}$$

Lösung 2

Wir setzen

$$\mathtt{Z} :\equiv \mathtt{p} = \mathtt{xy}.$$

Dann folgt

$$\mathbf{WP}[\![\mathtt{p} = \mathtt{k} * \mathtt{p};]\!](\mathtt{Z}) \equiv \mathtt{kp} = \mathtt{xy} \equiv: \mathtt{Z}'$$

Wir setzen

$$\mathtt{P}(\mathtt{x}, \mathtt{k}) :\equiv \mathtt{k}^2 = \mathtt{1} \wedge \mathtt{kx} \geq \mathtt{0}$$

und raten die Schleifen-Invariante

$$\mathtt{I} :\equiv \mathtt{kxy} = \mathtt{ayf} + \mathtt{p} \wedge \mathtt{a} \geq \mathtt{0} \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}).$$

Es folgt:

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{f} = \mathtt{10} * \mathtt{f}; \mathtt{a} = \mathtt{a}/\mathtt{10};]\!](\mathtt{I}) &\equiv \mathtt{kxy} = \mathtt{10y}(\mathtt{a}\,\mathbf{div}\,\mathtt{10})\mathtt{f} + \mathtt{p} \wedge \mathtt{a}\,\mathbf{div}\,\mathtt{10} \geq \mathtt{0} \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\Leftarrow \mathtt{kxy} = (\mathtt{10}(\mathtt{a}\,\mathbf{div}\,\mathtt{10}))\mathtt{yf} + \mathtt{p} \wedge \mathtt{a} \geq \mathtt{0} \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{kxy} = (\mathtt{a} - \mathtt{a}\,\mathbf{mod}\,\mathtt{10})\mathtt{yf} + \mathtt{p} \wedge \mathtt{a} \geq \mathtt{0} \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv: \mathtt{B}.
\end{aligned}$$

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{p} = \mathtt{p} + (\mathtt{a}\%\mathtt{10}) * \mathtt{y} * \mathtt{f};]\!](\mathtt{B}) &\equiv \mathtt{kxy} = (\mathtt{a} - \mathtt{a}\,\mathbf{mod}\,\mathtt{10})\mathtt{yf} + \mathtt{p} + (\mathtt{a}\,\mathbf{mod}\,\mathtt{10})\mathtt{yf} \wedge \mathtt{a} \geq \mathtt{0} \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{kxy} = \mathtt{ayf} + \mathtt{p} \wedge \mathtt{a} \geq \mathtt{0} \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{I} \\
&\equiv: \mathtt{C}.
\end{aligned}$$

Wir müssen noch zeigen, dass

$$\mathtt{I} \Rightarrow \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$$

gilt. Dazu nehmen wir an, dass $\sigma \models \mathtt{I}$ gilt. Wir müssen zeigen, dass $\sigma \models \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$ gilt. Wir unterscheiden zwei Fälle.

Fall 1: Es gilt $\sigma \models \mathtt{a} > \mathtt{0}$. Da $\sigma \models \mathtt{I}$ gilt, gilt auch $\sigma \models \mathtt{a} > \mathtt{0} \wedge \mathtt{I}$. Damit gilt auch $\sigma \models (\mathtt{a} \leq \mathtt{0} \wedge \mathtt{Z}') \vee (\mathtt{a} > \mathtt{0} \wedge \mathtt{I})$. Da $(\mathtt{a} \leq \mathtt{0} \wedge \mathtt{Z}') \vee (\mathtt{a} > \mathtt{0} \wedge \mathtt{I}) \equiv \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$ gilt, gilt auch $\sigma \models \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$.

Fall 2: Es gilt $\sigma \models \mathtt{a} \leq \mathtt{0}$. Da $\sigma \models \mathtt{I}$ gilt, folgt $\sigma \models \mathtt{0} = \mathtt{a}$. Damit gilt $\sigma \models \mathtt{kxy} = \mathtt{p}$. Durch Multiplizieren der Gleichung mit k erhält man, dass $\sigma \models \mathtt{k}^2\mathtt{xy} = \mathtt{kp}$ gilt. Da zusätzlich $\sigma \models \mathtt{k}^2 = \mathtt{1}$ gilt, gilt $\sigma \models \mathtt{kp} = \mathtt{xy}$. Damit gilt $\sigma \models (\mathtt{a} \leq \mathtt{0} \wedge \mathtt{kp} = \mathtt{xy}) \vee (\mathtt{a} > \mathtt{0} \wedge \mathtt{C})$. Da $(\mathtt{a} \leq \mathtt{0} \wedge \mathtt{kp} = \mathtt{xy}) \vee (\mathtt{a} > \mathtt{0} \wedge \mathtt{C}) \equiv \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$ gilt, folgt $\sigma \models \mathbf{WP}[\![\mathtt{a} > \mathtt{0}]\!](\mathtt{Z}', \mathtt{C})$.

Weiter geht's:

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{a} = \mathtt{k} * \mathtt{x}; \mathtt{p} = \mathtt{0}; \mathtt{f} = \mathtt{1};]\!](\mathtt{I}) &\equiv \mathtt{kxy} = \mathtt{kxy} + \mathtt{0} \wedge \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv \mathtt{P}(\mathtt{x}, \mathtt{k}) \\
&\equiv: \mathtt{F}
\end{aligned}$$

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{k = 1;}]\!](\mathtt{F}) &\equiv \mathtt{P(x, 1)} \\
&\equiv \mathtt{x} \geq \mathtt{0} \\
&\equiv: \mathtt{G}
\end{aligned}$$

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{k = -1;}]\!](\mathtt{F}) &\equiv \mathtt{P(x, -1)} \\
&\equiv \mathtt{x} \leq \mathtt{0} \\
&\equiv: \mathtt{H}
\end{aligned}$$

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{x} < \mathtt{0}]\!](\mathtt{G}, \mathtt{H}) &\equiv (\mathtt{x} \geq \mathtt{0} \wedge \mathtt{x} \geq \mathtt{0}) \vee (\mathtt{x} < \mathtt{0} \wedge \mathtt{x} \leq \mathtt{0}) \\
&\equiv \mathtt{x} \geq \mathtt{0} \vee \mathtt{x} < \mathtt{0} \\
&\equiv \mathbf{true} \equiv: \mathtt{J} \equiv: \mathtt{K} \equiv: \mathtt{L}
\end{aligned}$$