Übung "Grundbegriffe der Informatik"

Karlsruher Institut für Technologie

Matthias Schulz, Gebäude 50.34, Raum 034

email: schulz@ira.uka.de

Schleifeninvarianten

Am besten in while Schleifen:

$while\ B\ do$

$\vdots$

od

.

Schleifeninvarianten

Am besten in while Schleifen:

Schleifeninvariante gilt
$while\ B\ do$
  Schleifeninvariante gilt
  $\vdots$
  Schleifeninvariante gilt
od
Schleifeninvariante gilt

.

Schleifeninvarianten

Am besten in while Schleifen:

Schleifeninvariante gilt
$while\ B\ do$
  Schleifeninvariante gilt
  $\vdots$
  Schleifeninvariante gilt
od
Schleifeninvariante gilt

Programmstück bildet Belegung B_1 auf Belegung B_2 ab.

.

Schleifeninvarianten

Am besten in while Schleifen:

Schleifeninvariante gilt
$while\ B\ do$
  Schleifeninvariante gilt
  $\vdots$
  Schleifeninvariante gilt
od
Schleifeninvariante gilt

Programmstück bildet Belegung B_1 auf Belegung B_2 ab.
Jede Belegung B' am Schleifenende wird auf B_2 abgebildet.

.

Schleifeninvarianten

Nicht so gut bei for Schleifen:

Schleifeninvariante gilt
$for\ i \leftarrow x\ to\ y\ do$
  Schleifeninvariante gilt I
  $\vdots$
  Schleifeninvariante gilt II
od
Schleifeninvariante gilt

.

Schleifeninvarianten

Nicht so gut bei for Schleifen:

Schleifeninvariante gilt
$for\ i \leftarrow x\ to\ y\ do$
  Schleifeninvariante gilt I
  $\vdots$
  Schleifeninvariante gilt II
od
Schleifeninvariante gilt

Problem: Änderung von i zwischen II und I.

.

Schleifeninvarianten

Nicht so gut bei for Schleifen:

Schleifeninvariante gilt
$for\ i \leftarrow x\ to\ y\ do$
  Schleifeninvariante gilt I
  $\vdots$
  Schleifeninvariante gilt II
od
Schleifeninvariante gilt

Lösung: Verwende in SI Variable j, die im Schleifenrumpf den Wert von i annimmt.

.

Schleifeninvarianten

Nicht so gut bei for Schleifen:

$j \leftarrow x$
Schleifeninvariante gilt
$for\ i \leftarrow x\ to\ y\ do$
  Schleifeninvariante gilt I
  $j \leftarrow j + 1$
  $\vdots$
  Schleifeninvariante gilt II
od
Schleifeninvariante gilt

.

Schleifeninvarianten

Beispiel:

$$
\begin{array}{l}
x \leftarrow a,\ y \leftarrow b \\
s_1 \leftarrow 1,\ s_2 \leftarrow 0,\ t_1 \leftarrow 0,\ t_2 \leftarrow 1 \\
while\ y > 0\ do \\
\quad q \leftarrow x \ \mathtt{div}\ y \\
\quad v \leftarrow y, \quad y \leftarrow x - qy, \quad x \leftarrow v, \\
\quad v \leftarrow s_2, \quad s_2 \leftarrow s_1 - qs_2, \quad s_1 \leftarrow v \\
\quad v \leftarrow t_2, \quad t_2 \leftarrow t_1 - qt_2, \quad t_1 \leftarrow v \\
od
\end{array}
$$

.

Schleifeninvarianten

Anfang:

$$\begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \to \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Schleife:

$$\begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \to \begin{pmatrix} y & x - qy \\ s_2 & s_1 - qs_2 \\ t_2 & t_1 - qt_2 \end{pmatrix}$$

.

Schleifeninvarianten

Anfang:

$$\begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \to \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Schleife:

$$\begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \to \begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$$

.

Schleifeninvarianten

Falls vor Schleife $A \cdot \begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} = 0$ gilt,

gilt das auch nach der Schleife.

.

Schleifeninvarianten

Falls vor Schleife $A \cdot \begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} = 0$ gilt,

gilt das auch nach der Schleife.

$$0 = A \cdot \begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \to A \cdot \begin{pmatrix} x & y \\ s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = 0 \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = 0$$

.

Schleifeninvarianten

Anfang:

$$A \cdot \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

.

Schleifeninvarianten

Anfang:

$$A \cdot \begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

$$A = \begin{pmatrix} 1 & -a & -b \end{pmatrix}$$

.

Schleifeninvarianten

Schleifeninvariante: $x - s_1 a - t_1 b = y - s_2 a - t_2 b = 0$

.

Schleifeninvarianten

Nachrechnen: Zu Beginn der Schleife gelte SI für Belegung x, y, s_1, s_2, t_1, t_2.

Berechne Belegung am Ende der Schleife $x', y', s_1', s_2', t_1', t_2'$.

Zeige: SI gilt für $x', y', s_1', s_2', t_1', t_2'$.

.

Schleifeninvarianten

Bemerkung: Am Ende gilt $x = ggt(a, b)$, und es gilt $s_1 a + t_1 b = ggt(a, b)$.

Nützlich zum Invertieren modulo n!

.

O-Kalkül

Präziser Formalismus ...

.

O-Kalkül

Präziser Formalismus ...

für grobes Abschätzen.

.

O-Kalkül

Aufgabentypen:

- Zeigen Sie: $f(n) \in O(g(n)) \Rightarrow O(f(n)) \subseteq O(g(n))$.
- Zeigen Sie: $f(n) \in O(g(n))$.
- Zeigen Sie: $f(n) \notin O(g(n))$.

.

O-Kalkül

Zeigen Sie: $f(n) \in O(g(n)) \Rightarrow O(f(n)) \subseteq O(g(n))$.

Sei $h(n) \in O(f(n))$. Dann gilt:

$\exists n_1, n_2 \in \mathbb{N}_0 \exists c_1, c_2 \in \mathbb{R}_+ :$
$\forall n \geq n_1 : h(n) \leq c_1 f(n) \land \forall n \geq n_2 : f(n) \leq c_2 g(n)$

.

O-Kalkül

Zeigen Sie: $f(n) \in O(g(n)) \Rightarrow O(f(n)) \subseteq O(g(n))$.

Sei $h(n) \in O(f(n))$. Dann gilt:

$\exists n_1, n_2 \in \mathbb{N}_0 \exists c_1, c_2 \in \mathbb{R}_+$:
$\forall n \geq n_1 : h(n) \leq c_1 f(n) \wedge \forall n \geq n_2 : f(n) \leq c_2 g(n)$

Sei $n_0 = \max\{n_1, n_2\}$ und $c = c_1 c_2$.

Dann gilt: $\forall n \geq n_0 : h(n) \leq c_1 f(n) \leq c_1 c_2 g(n) = c g(n)$.

.

O-Kalkül

Zeigen Sie: $f(n) \in O(g(n)) \Rightarrow O(f(n)) \subseteq O(g(n))$.

Also gilt $h(n) \in O(g(n)) \Rightarrow O(f(n)) \subseteq O(g(n))$.

.

O-Kalkül

Zeigen Sie: $\sum_{i=2}^{n} \frac{1}{i} \in O(log(n))$

.

O-Kalkül

Zeigen Sie: $\sum_{i=2}^{n} \frac{1}{i} \in O(\log(n))$

Suche n_0, c so, dass gilt: $\forall n \geq n_0 : \sum_{i=2}^{n} \frac{1}{i} \leq c \log_2 n$.

.

O-Kalkül

Zeigen Sie: $\sum_{i=2}^{n} \frac{1}{i} \in O(\log(n))$

Suche n_0, c so, dass gilt: $\forall n \geq n_0 : \sum_{i=2}^{n} \frac{1}{i} \leq c \log_2 n$.

Wir wählen $n_0 = 2$ und $c = 2$.

.

O-Kalkül

Zeigen Sie: $\sum_{i=2}^{n} \frac{1}{i} \in O(\log(n))$

$$\sum_{i=2}^{2^n} \frac{1}{i} = \sum_{k=1}^{n} \Big(\sum_{i=2^{k-1}+1}^{2^k} \frac{1}{i} \Big)$$

.

O-Kalkül

Zeigen Sie: $\sum_{i=2}^{n} \frac{1}{i} \in O(\log(n))$

$$\sum_{i=2}^{2^n} \frac{1}{i} = \sum_{k=1}^{n} (\sum_{i=2^{k-1}+1}^{2^k} \frac{1}{i}) \leq \sum_{k=1}^{n} (\sum_{i=2^{k-1}+1}^{2^k} \frac{1}{2^{k-1}+1})$$

.

O-Kalkül

Zeigen Sie: $\sum_{i=2}^{n} \frac{1}{i} \in O(\log(n))$

$$\sum_{i=2}^{2^n} \frac{1}{i} \leq \sum_{k=1}^{n} \Big(\sum_{i=2^{k-1}+1}^{2^k} \frac{1}{2^{k-1}+1} \Big) = \sum_{k=1}^{n} \frac{2^{k-1}}{2^{k-1}+1}$$

.

O-Kalkül

Zeigen Sie: $\sum_{i=2}^{n} \frac{1}{i} \in O(\log(n))$

$$\sum_{i=2}^{2^n} \frac{1}{i} \leq \sum_{k=1}^{n} \frac{2^{k-1}}{2^{k-1}+1} \leq n$$

.

O-Kalkül

Zeigen Sie: $\sum_{i=2}^{n} \frac{1}{i} \in O(\log(n))$

$$\sum_{i=2}^{2^n} \frac{1}{i} \leq \sum_{k=1}^{n} \frac{2^{k-1}}{2^{k-1}+1} \leq n$$

$\Rightarrow$ für $2^{n-1} < k \leq 2^n$ gilt
$\sum_{i=2}^{k} \leq \sum_{i=2}^{2^n} \leq n \leq \log_2 k + 1 \leq 2 \log_2 k$.

.

O-Kalkül

Für $n \in \mathbb{N}_0$ sei $f(n)$ die größte Primzahl, die n teilt.

Zeigen Sie: $f(n) \notin O(\sqrt{n})$

.

O-Kalkül

Für $n \in \mathbb{N}_0$ sei $f(n)$ die größte Primzahl, die n teilt.

Zeigen Sie: $f(n) \notin O(\sqrt{n})$

Angenommen, für $n_0 \in \mathbb{N}_0$ und $c > 0$ gilt:

$\forall n \geq n_0 : f(n) \leq c\sqrt{n}$

.

Für $n \in \mathbb{N}_0$ sei $f(n)$ die größte Primzahl, die n teilt.

Zeigen Sie: $f(n) \notin O(\sqrt{n})$

Angenommen, für $n_0 \in \mathbb{N}_0$ und $c > 0$ gilt:

$\forall n \geq n_0 : f(n) \leq c\sqrt{n}$

Idee: Wir suchen $n > n_0$ so, dass $f(n)$ verglichen mit $\sqrt{n}$ möglichst groß ist.

.

O-Kalkül

Für $n \in \mathbb{N}_0$ sei $f(n)$ die größte Primzahl, die n teilt.

Zeigen Sie: $f(n) \notin O(\sqrt{n})$

Angenommen, für $n_0 \in \mathbb{N}_0$ und $c > 0$ gilt:

$\forall n \geq n_0 : f(n) \leq c\sqrt{n}$

Idee: Wir suchen $n > n_0$ so, dass $f(n)$ verglichen mit $\sqrt{n}$ möglichst groß ist.

Also: n Primzahl $> n_0$ (gibt es immer!)

.

O-Kalkül

Für $n \in \mathbb{N}_0$ sei $f(n)$ die größte Primzahl, die n teilt.

Zeigen Sie: $f(n) \notin O(\sqrt{n})$

Angenommen, für $n_0 \in \mathbb{N}_0$ und $c > 0$ gilt:

$\forall n \geq n_0 : f(n) \leq c\sqrt{n}$

n Primzahl $> n_0$ (gibt es immer!)

Dann ist $f(n) = n = \sqrt{n} \cdot \sqrt{n}$.

.

O-Kalkül

Für $n \in \mathbb{N}_0$ sei $f(n)$ die größte Primzahl, die n teilt.

Zeigen Sie: $f(n) \notin O(\sqrt{n})$

Angenommen, für $n_0 \in \mathbb{N}_0$ und $c > 0$ gilt:

$\forall n \geq n_0 : f(n) \leq c\sqrt{n}$

n Primzahl $> n_0$ (gibt es immer!)

Dann ist $f(n) = n = \sqrt{n} \cdot \sqrt{n}$.

Wenn $\sqrt{n} > c$ ist, haben wir Widerspruch.

.

O-Kalkül

Für $n \in \mathbb{N}_0$ sei $f(n)$ die größte Primzahl, die n teilt.

Zeigen Sie: $f(n) \notin O(\sqrt{n})$

Angenommen, für $n_0 \in \mathbb{N}_0$ und $c > 0$ gilt:

$\forall n \geq n_0 : f(n) \leq c\sqrt{n}$

Sei n Primzahl $> \max(n_0, c^2)$.

Dann gilt $f(n) = n = \sqrt{n} \cdot \sqrt{n} > \sqrt{c^2}\sqrt{n} = c\sqrt{n}$, im Widerspruch zur Annahme.

.

O-Kalkül

Zeigen Sie: $\sum_{i=0}^{n} i^k \in \Omega(n^{k+1})$

.

Zeigen Sie: $\sum_{i=0}^{n} i^k \in \Omega(n^{k+1})$

$(n+1)^{k+1} = n^{k+1} + \sum_{i=1}^{k} \binom{k+1}{i} n^i$

.

O-Kalkül

Zeigen Sie: $\sum_{i=0}^{n} i^k \in \Omega(n^{k+1})$

$(n+1)^{k+1} = n^{k+1} + \sum_{i=1}^{k} \binom{k+1}{i} n^i$
$\leq n^{k+1} + (2^{k+1} - 1)n^k$

.

Zeigen Sie: $\sum_{i=0}^{n} i^k \in \Omega(n^{k+1})$

$(n+1)^{k+1} = n^{k+1} + \sum_{i=1}^{k} \binom{k+1}{i} n^i$
$\leq n^{k+1} + (2^{k+1} - 1)n^k$

Wähle $c = \frac{1}{2^{k+1}-1}$ und $n_0 = 1$

.

Zeigen Sie: $\sum_{i=0}^{n} i^k \in \Omega(n^{k+1})$

$(n+1)^{k+1} \leq n^{k+1} + (2^{k+1}-1)n^k$

Wähle $c = \frac{1}{2^{k+1}-1}$ und $n_0 = 1$

$\sum_{i=0}^{1} i^k = 1^k = 1 \geq c \cdot 1^{k+1}$ ✓

.

O-Kalkül

Zeigen Sie: $\sum_{i=0}^{n} i^k \in \Omega(n^{k+1})$

$(n+1)^{k+1} \leq n^{k+1} + (2^{k+1}-1)n^k$

Wähle $c = \frac{1}{2^{k+1}-1}$ und $n_0 = 1$

$\sum_{i=0}^{n+1} i^k = \sum_{i=0}^{n} i^k + (n+1)^k \overset{IV}{\geq} cn^{k+1} + n^k$
$= c(n^{k+1} + (2^{k+1}-1)n^k) \geq c(n+1)^{k+1}$ ✓

.

Verträglichkeit

$$x \sim y \iff x \ \mathtt{div}\ 23 = y \ \mathtt{div}\ 23$$

1. Zeigen Sie, dass $\sim$ Äquivalenz ist.

2. Ist $\sim$ verträglich mit Addition? Multiplikation? Division? Subtraktion?

3. Ist $\sim$ verträglich mit Addition von $45, 46, 47$?

4. Ist $\sim$ verträglich mit Division durch $3, 4, 5$?

.

Verträglichkeit

$x \sim y \iff x \texttt{ div } 23 = y \texttt{ div } 23$

$x \texttt{ div } 23 = x \texttt{ div } 23$
Symmetrie und Transitivität vererben sich von $=$.

.

Verträglichkeit

$x \sim y \iff x \texttt{ div } 23 = y \texttt{ div } 23$

$11 \sim 12$, aber $11 + 11 = 22 \not\sim 12 + 12 = 24$

$12 \sim 1$, aber $1 = 1 \cdot 1 \not\sim 144 = 12 \cdot 12$

$12 \sim 1$, aber $24 = 25 - 1 \not\sim 13 = 25 - 12$

$2 \sim 1$, aber $46 = 46 \texttt{ div } 1 \not\sim 23 = 46 \texttt{ div } 2$

.

Verträglichkeit

$x \sim y \iff x \texttt{ div } 23 = y \texttt{ div } 23$

$1 + 45 \not\sim 0 + 45$

$x \sim y \Rightarrow x \texttt{ div } 23 = y \texttt{ div } 23 \Rightarrow x \texttt{ div } 23{+}2 = y \texttt{ div } 23{+}2 \Rightarrow$

$(x + 46) \texttt{ div } 23 = (y + 46) \texttt{ div } 23$

$22 + 47 \not\sim 21 + 47$

.

Verträglichkeit

$$x \ \texttt{div}\ k \not\sim y \ \texttt{div}\ k \Rightarrow \exists m \in \mathbb{N}_0 : x \ \texttt{div}\ k < 23m \wedge y \ \texttt{div}\ k \geq 23m$$

.

Verträglichkeit

$x \texttt{ div } k \not\sim y \texttt{ div } k \Rightarrow \exists m \in \mathbb{N}_0 : x \texttt{ div } k < 23m \wedge y \texttt{ div } k \geq 23m$

$\Rightarrow k(x \texttt{ div } k) \leq 23mk - k \wedge y \geq 23mk$

.

Verträglichkeit

$$x \;\texttt{div}\; k \not\sim y \;\texttt{div}\; k \Rightarrow \exists m \in \mathbb{N}_0 : x \;\texttt{div}\; k < 23m \wedge y \;\texttt{div}\; k \geq 23m$$

$$\Rightarrow k(x \;\texttt{div}\; k) \leq 23mk - k \wedge y \geq 23mk$$

$$\Rightarrow k(x \;\texttt{div}\; k) + x \mod k < 23mk \leq y$$

.

Verträglichkeit

$$x \ \mathtt{div} \ k \not\sim y \ \mathtt{div} \ k \Rightarrow \exists m \in \mathbb{N}_0 : x \ \mathtt{div} \ k < 23m \wedge y \ \mathtt{div} \ k \geq 23m$$

$$\Rightarrow k(x \ \mathtt{div} \ k) \leq 23mk - k \wedge y \geq 23mk$$

$$\Rightarrow k(x \ \mathtt{div} \ k) + x \mod k < 23mk \leq y$$

$$\Rightarrow x \not\sim y$$

.

Verträglichkeit

$x \;\texttt{div}\; k \not\sim y \;\texttt{div}\; k \Rightarrow x \not\sim y$

$\Rightarrow$

$x \sim y \Rightarrow x \;\texttt{div}\; k \sim y \;\texttt{div}\; k$

.