

11.11.2011

Willkommen zur vierten Übung zur Vorlesung

Grundbegriffe der Informatik



Matthias Janke

email: matthias.janke@kit.edu

Invarianten

Algorithmen

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Ist am Ende mehr Zucker im Salzfaß oder mehr Salz im Zuckerfaß?

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Ist am Ende mehr Zucker im Salzfaß oder mehr Salz im Zuckerfaß?

Und was hat das mit Invarianten zu tun?

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Genau so viel Zucker im Salzfaß wie Salz im Zuckerfaß.

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Invariant: (Volumen-)Menge in Salzfaß.

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Invariant: (Volumen-)Menge in Salzfaß.

Invariant: Menge an Salz.

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Anfangs gilt: Genau so viel Zucker in Salzfaß wie Salz in Zuckerfaß.

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Zucker in Zuckerfaß: z_z , Zucker in Salzfaß: z_s

Salz in Zuckerfaß: s_z , Salz in Salzfaß: s_s

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Zucker in Zuckerfaß: z_z , Zucker in Salzfaß: z_s

Salz in Zuckerfaß: s_z , Salz in Salzfaß: s_s

Es gilt immer: $s_z + s_s = z_s + s_s$

Gegeben: Ein Fass Salz, ein Fass Zucker.

Wiederhole folgenden Prozess:

- ▶ Einen Löffel Inhalt des Salzfaßes ins Zuckerfaß.
- ▶ Einen Löffel Inhalt des Zuckerfaßes ins Salzfaß.

Zucker in Zuckerfaß: z_z , Zucker in Salzfaß: z_s

Salz in Zuckerfaß: s_z , Salz in Salzfaß: s_s

Es gilt immer: $s_z + s_s = z_s + s_s$

Also $s_z = z_s$

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

$(3, 2, 4) \rightarrow (2, 1, 5) \rightarrow (1, 2, 4) \rightarrow (2, 1, 3) \rightarrow (1, 2, 2) \rightarrow (2, 1, 1) \rightarrow$
 $(1, 0, 2) \rightarrow (0, 1, 1) \rightarrow (1, 0, 0)$

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

Bekannt: Am Ende bleibe eine einzelne Kugel übrig. Welche Farbe?

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

Bekannt: Am Ende bleibe eine einzelne Kugel übrig. Welche Farbe?

Suche Invariante ...

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

Bekannt: Am Ende bleibe eine einzelne Kugel übrig. Welche Farbe?

$$(a, b, c) \rightarrow (a - 1, b - 1, c + 1)$$

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

Bekannt: Am Ende bleibe eine einzelne Kugel übrig. Welche Farbe?

$$(a, b, c) \rightarrow (a - 1, b - 1, c + 1)$$

Alles ändert sich!

$$(a, b, c) \rightarrow (a - 1, b - 1, c + 1)$$

Wie siehts mit Differenzen aus?

$$(a - 1) - (b - 1) = a - b$$

$$(a - 1) - (c + 1) = a - c - 2$$

$$(b - 1) - (c + 1) = b - c - 2$$

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

Bekannt: Am Ende bleibe eine einzelne Kugel übrig. Welche Farbe?

$$(a, b, c) \rightarrow (a - 1, b - 1, c + 1)$$

- Differenzen modulo 2 bleiben gleich.

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

Bekannt: Am Ende bleibe eine einzelne Kugel übrig. Welche Farbe?

Ende: $(0, 1, 0)$:

Für nicht vorhandene Kugelfarben gilt $|(x - y)| \bmod 2 = 0$ Für vorhandene Kugelfarbe gilt $|(y - x)| \bmod 2 = 1$

Schale mit a blauen, b roten und c grünen Kugeln.

Wiederhole: Nimm zwei verschiedenfarbige Kugeln und ersetze sie durch eine Kugel der dritten Farbe.

Bekannt: Am Ende bleibe eine einzelne Kugel übrig. Welche Farbe?

Also: Farbe mit Anzahl modulo 2 ungleich Anzahl andere Farben modulo 2 bleibt übrig.

Ein bisschen was zu **mod** und **div**

n	div 3	mod 3
0	0	0
1	0	1
2	0	2
3	1	0
4	1	1
5	1	2
6	2	0
7	2	1
8	2	2
9	3	0

Ein bisschen was zu **mod** und **div**

n	div 2	mod 2
0	0	0
1	0	1
2	1	0
3	1	1
4	2	0
5	2	1
6	3	0
7	3	1
8	4	0
9	4	1

$\forall n, m \in \mathbb{N}_0 : \forall k \in \mathbb{N}_+ : n \text{ **mod** } k = m \text{ **mod** } k \Rightarrow |n - m| \text{ ist durch } k \text{ teilbar.}$

$\rightarrow n \text{ durch } k \text{ teilbar bzw. } k \text{ teilt } n \iff \exists m \in \mathbb{N}_0(\mathbb{Z}) : km = n.$

Vergleiche: $\forall n \in \mathbb{N}_0 : \forall k \in \mathbb{N}_+ :$

$$k \cdot (n \text{ **div** } k) + (n \text{ **mod** } k) = n.$$

k heißt Teiler von n falls gilt: $\exists m \in \mathbb{N}_0(\mathbb{Z}) : km = n$.

k ist gemeinsamer Teiler von a, b : k teilt a und k teilt b .

Jede natürliche Zahl teilt 0.

Ein bisschen was zu ((größten) gemeinsamen) Teilern

k ist größter gemeinsamer Teiler von a, b ($\text{ggT}(a, b)$):

- ▶ k ist gemeinsamer Teiler von a und b und jeder gemeinsame Teiler k' von a und b erfüllt $k' \leq k$

ODER

- ▶ k ist gemeinsamer Teiler von a und b und jeder gemeinsame Teiler k' von a und b erfüllt k' teilt k .

Formal für $k = \text{ggT}(a, b)$:

- ▶ $(\exists m_1, m_2 \in \mathbb{N}_0 : m_1 k = a \wedge m_2 k = b) \wedge \forall k' \in \mathbb{N}_0 :$
 $((\exists m'_1, m'_2 \in \mathbb{N}_0 : m'_1 k' = a \wedge m'_2 k' = b) \Rightarrow k' \leq k).$
- ▶ $(\exists m_1, m_2 \in \mathbb{N}_0 : m_1 k = a \wedge m_2 k = b) \wedge \forall k' \in \mathbb{N}_0 :$
 $((\exists m'_1, m'_2 \in \mathbb{N}_0 : m'_1 k' = a \wedge m'_2 k' = b) \Rightarrow \exists m_3 \in \mathbb{N}_0 :$
 $m_3 k' = k).$

Ein bisschen was zu ((größten) gemeinsamen) Teilern

a	b	$\text{ggt}(a, b)$
5	5	5
4	4	4
3	3	3
2	2	2
1	1	1
0	0	?

Ein bisschen was zu ((größten) gemeinsamen) Teilern

$\forall n \in \mathbb{N}_+ : \text{ggt}(0, n) = \text{ggt}(n, 0) = n.$

$\text{ggt}(0, 0)$ undefiniert nach Definition 1.

$\text{ggt}(0, 0) = 0$ nach Definition 2.

Invarianten

Algorithmen

```
 $x \leftarrow n$   
 $y \leftarrow 0$   
 $z \leftarrow 0$   
 $e \leftarrow 1$   
 $v \leftarrow 1$   
for  $i \leftarrow 0$  to  $\lceil \log_2 n \rceil$  do  
     $y \leftarrow y + e \cdot x \bmod 2$   
     $z \leftarrow z + v \cdot x \bmod 2$   
     $x \leftarrow x \operatorname{div} 2$   
     $e \leftarrow 2 \cdot e$   
     $v \leftarrow -v$   
od
```

Anfang:	n	0	0	1	1
	x	y	z	e	v
\rightarrow	$x \mathbf{div} 2$	$y + e(x \mathbf{mod} 2)$	$z + v(x \mathbf{mod} 2)$	$2e$	$-v$

Wiederhole $1 + \lceil \log_2 n \rceil$ mal.

Anfang:	n	0	0	1	1
	x	y	z	e	v
\rightarrow	$x \mathbf{div} 2$	$y + e(x \mathbf{mod} 2)$	$z + v(x \mathbf{mod} 2)$	$2e$	$-v$
Init. $n=5$:	5	0	0	1	1

Wiederhole $1 + \lceil \log_2 n \rceil$ mal. $\rightarrow 4$ mal.

Anfang:	n	0	0	1	1
	x	y	z	e	v
\rightarrow	$x \mathbf{div} 2$	$y + e(x \mathbf{mod} 2)$	$z + v(x \mathbf{mod} 2)$	$2e$	$-v$
Init. $n=5$:	5	0	0	1	1
1. Iter.	2	1	1	2	-1

Wiederhole $1 + \lceil \log_2 n \rceil$ mal. $\rightarrow 4$ mal.

Anfang:	n	0	0	1	1
	x	y	z	e	v
\rightarrow	$x \text{ div } 2$	$y + e(x \bmod 2)$	$z + v(x \bmod 2)$	$2e$	$-v$
Init. $n=5$:	5	0	0	1	1
1. Iter.	2	1	1	2	-1
2. Iter.	1	1	1	4	1

Wiederhole $1 + \lceil \log_2 n \rceil$ mal. $\rightarrow 4$ mal.

Anfang:	n	0	0	1	1
	x	y	z	e	v
\rightarrow	$x \text{ div } 2$	$y + e(x \bmod 2)$	$z + v(x \bmod 2)$	$2e$	$-v$
Init. $n=5$:	5	0	0	1	1
1. Iter.	2	1	1	2	-1
2. Iter.	1	1	1	4	1
3. Iter.	0	5	2	8	-1

Wiederhole $1 + \lceil \log_2 n \rceil$ mal. $\rightarrow 4$ mal.

Anfang:	n	0	0	1	1
	x	y	z	e	v
\rightarrow	$x \text{ div } 2$	$y + e(x \bmod 2)$	$z + v(x \bmod 2)$	$2e$	$-v$
Init. $n=5$:	5	0	0	1	1
1. Iter.	2	1	1	2	-1
2. Iter.	1	1	1	4	1
3. Iter.	0	5	2	8	-1
4. Iter.	0	5	2	16	1

Wiederhole $1 + \lceil \log_2 n \rceil$ mal. $\rightarrow 4$ mal.

$n = 9$:

Anfangsbelegung:	9	0	0	1	1
Nach 1. Schleife	4	1	1	2	-1
Nach 2. Schleife	2	1	1	4	1
Nach 3. Schleife	1	1	1	8	-1
Nach 4. Schleife	0	9	0	16	1
Nach 5. Schleife	0	9	0	32	-1

$n = 16$:

Anfangsbelegung:	16	0	0	1	1
Nach 1. Schleife	8	0	0	2	-1
Nach 2. Schleife	4	0	0	4	1
Nach 3. Schleife	2	0	0	8	-1
Nach 4. Schleife	1	0	0	16	1
Nach 5. Schleife	0	16	1	32	-1
Nach 6. Schleife	0	16	1	64	1

$n = 21$:

Anfangsbelegung:	21	0	0	1	1
Nach 1. Schleife	10	1	1	2	-1
Nach 2. Schleife	5	1	1	4	1
Nach 3. Schleife	2	5	2	8	-1
Nach 4. Schleife	1	5	2	16	1
Nach 5. Schleife	0	21	3	32	-1
Nach 6. Schleife	0	21	3	64	1

Was fällt auf?



Was fällt auf?

- ▶ Am Ende gilt $y = n$.

- ▶

- ▶

Was fällt auf?

- ▶ Am Ende gilt $y = n$.
- ▶ x wird in jedem Schritt halbiert, e wird in jedem Schritt verdoppelt.
- ▶

Was fällt auf?

- ▶ Am Ende gilt $y = n$.
- ▶ x wird in jedem Schritt halbiert, e wird in jedem Schritt verdoppelt.
- ▶ Schleifeninvariante 1: $x \cdot e + y = n$.

	x	y	z	e	f
Anfangsbelegung:	21	0	0	1	1
Nach 1. Schleife	10	1	1	2	-1
Nach 2. Schleife	5	1	1	4	1
Nach 3. Schleife	2	5	2	8	-1
Nach 4. Schleife	1	5	2	16	1
Nach 5. Schleife	0	21	3	32	-1
Nach 6. Schleife	0	21	3	64	1

Was fällt auf?



Was fällt auf?

- ▶ $y \bmod 3 = z \bmod 3$



Was fällt auf?

- ▶ $y \bmod 3 = z \bmod 3$
- ▶ Schleifeninvariante 2: $y - z$ ist durch 3 teilbar.

Skizze Beweis Schleifeninvariante 2:

$$y + e(x \bmod 2) - (z + v(x \bmod 2)) = \\ y - z + (x \bmod 2)(e - v)$$

Skizze Beweis Schleifeninvariante 2:

$$y + e(x \bmod 2) - (z + v(x \bmod 2)) = \\ y - z + (x \bmod 2)(e - v)$$

Schön wäre, wenn $e - v$ immer durch 3 teilbar ist.

Schleifeninvariante:

- ▶ $x \cdot e + y = n \wedge$
- ▶ $e - v$ ist durch 3 teilbar \wedge
- ▶ $y - z$ ist durch 3 teilbar.

```
 $x \leftarrow n$   
 $y \leftarrow 0$   
 $z \leftarrow 0$   
 $e \leftarrow 1$   
 $v \leftarrow 1$   
for  $i \leftarrow 0$  to  $\lceil \log_2 n \rceil$  do  
     $y \leftarrow y + e \cdot x \bmod 2$   
     $z \leftarrow z + v \cdot x \bmod 2$   
     $x \leftarrow x \operatorname{div} 2$   
     $e \leftarrow 2 \cdot e$   
     $v \leftarrow -v$   
od
```

- ▶ Aussage S_i : Aussage der Schleifeninvariante gilt zu **Beginn** des i -ten Schleifendurchlaufs.
- ▶ Aussage R_i : Aussage der Schleifeninvariante gilt am **Ende** des i -ten Schleifendurchlaufs.

- ▶ Aussage S_i : Aussage der Schleifeninvariante gilt zu **Beginn** des i -ten Schleifendurchlaufs.
- ▶ Aussage R_i : Aussage der Schleifeninvariante gilt am **Ende** des i -ten Schleifendurchlaufs.
- ▶ Wenn es $i + 1$ -ten Schleifendurchlauf gibt, gilt $R_i = S_{i+1}$.

Vorgehen:

- ▶ Zeige S_0 .
- ▶ Zeige für zulässige i : $S_i \Rightarrow R_i$.

Vorgehen:

- ▶ Zeige S_0 .
- ▶ Zeige für zulässige i : $S_i \Rightarrow R_i$.

Dazu: Belegung der Variable V zu Anfang des i -ten Schleifendurchlaufs: V_i , am Ende des i -ten Schleifendurchlaufs: V_{i+1} .

SI 1: $x_i \cdot e_i + y_i = n$

- ▶ IA: $i = 0$: $x_0 \cdot e_0 + y_0 = n \cdot 1 + 0 = n$. ✓
- ▶ IV: Für beliebiges, aber festes $i \in \mathbb{N}_0$ gilt:
 $i < \lceil \log_2 n \rceil \Rightarrow x_i \cdot e_i + y_i = n$.
- ▶ IS: Es ist zu zeigen, dass dann auch $x_{i+1} \cdot e_{i+1} + y_{i+1} = n$:
$$\begin{aligned} x_{i+1} \cdot e_{i+1} + y_{i+1} &= \\ (x_i \mathbf{div} 2) \cdot (e_i \cdot 2) + (y_i + e_i \cdot x_i \mathbf{mod} 2) \\ &= y_i + e_i((x_i \mathbf{div} 2) \cdot 2 + x_i \mathbf{mod} 2) = y_i + e_i x_i \stackrel{IV}{=} n \end{aligned}$$

SI 2: $e_i - v_i$ ist durch 3 teilbar.

- ▶ IA: $i = 0$: $e_0 - v_0 = 1 - 1 = 0$ ist durch 3 teilbar. ✓
- ▶ IV: Für beliebiges, aber festes $i \in \mathbb{N}_0$ gilt:
 $i < \lceil \log_2 n \rceil \Rightarrow e_i - v_i$ ist durch 3 teilbar.
- ▶ IS: Es ist zu zeigen, dass dann auch $e_{i+1} - v_{i+1}$ durch 3 teilbar ist:
$$e_{i+1} - v_{i+1} = 2 \cdot e_i - (-v_i) = 2 \cdot e_i + v_i = 2(e_i - v_i) + 3v_i.$$

Nach IV ist $e_i - v_i$ durch 3 teilbar,
und damit auch $2(e_i - v_i) + 3v_i$.

SI 3: $y_i - z_i$ ist durch 3 teilbar.

- ▶ IA: $i = 0$: $y_0 - z_0 = 0 - 0 = 0$ ist durch 3 teilbar. ✓
- ▶ IV: Für beliebiges, aber festes $i \in \mathbb{N}_0$ gilt:
 $i < \lceil \log_2 n \rceil \Rightarrow y_i - z_i$ ist durch 3 teilbar.
- ▶ IS: Es ist zu zeigen, dass dann auch $y_{i+1} - z_{i+1}$ durch 3 teilbar ist:

$$y_{i+1} - z_{i+1} = y_i + e_i(x_i \bmod 2) - (z_i + v_i(x_i \bmod 2)) = (y_i - z_i) + (e_i - v_i)(x_i \bmod 2)$$

Nach IV beziehungsweise SI 2 sind beide Summanden durch 3 teilbar, also auch $y_{i+1} - z_{i+1}$.

Themen für das vierte Übungsblatt:

- ▶ Algorithmen
- ▶ Schleifeninvarianten

Schönes Wochenende!