Grundbegriffe der Informatik

Übung

Simon Wacker

Karlsruher Institut für Technologie

Wintersemester 2015/2016

Relationen

Beispiel aus der Zahlentheorie

- «kleiner als»-Relation auf $\mathbb{Z}$

$$< = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \text{es gibt ein } z \in \mathbb{N}_+ \text{ so, dass } x + z = y\}$$

Schreibe $x < y$ anstelle von $(x, y) \in <$

Beispiele aus der Softwareverifikation und -sicherheit

- Erreichbarkeits- und Datenflussrelation auf dem Zustandsraum eines Programms

Primzahlen

Teilbarkeitsrelation

$$| = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \text{es gibt ein } n \in \mathbb{Z} \text{ so, dass } x \cdot n = y\}$$

$n \in \mathbb{N}_+$ prim gdw. $n \neq 1$ und für jedes $k \in \mathbb{N}_+$ gilt:

Wenn $k \mid n$, dann $k = 1$ oder $k = n$.

$P = \{n \in \mathbb{N}_+ \mid n \text{ ist prim}\}$

Potenzen von Mengen ganzer Zahlen

Produkt zweier Teilmengen A und B von $\mathbb{Z}$

$$A \cdot B = \{a \cdot b \mid a \in A \text{ und } b \in B\}$$

Potenzen einer Teilmenge A von $\mathbb{Z}$

$$A^0 = \{1\},$$
$$\text{für jedes } n \in \mathbb{N}_+ \colon A^n = A \cdot A^{n-1}$$

$A^1 = A \cdot A^0 = A \cdot \{1\} = A,$
$A^2 = A \cdot A^1 = A \cdot A,$
$A^3 = A \cdot A^2 = A \cdot (A \cdot A)$, usw.

Achtung: Mit A^n wurde in der Vorlesung das n-fache kartesische Produkt von A mit sich selbst bezeichnet.

Fundamentalsatz der Arithmetik

Jede positive ganze Zahl ist ein Produkt endlich vieler Primzahlen. In anderen Worten,

$$\mathbb{N}_+ = \bigcup_{n \in \mathbb{N}_0} P^n.$$

Beweis per vollständige Induktion über die Anzahl n der Primfaktoren.

Gleichheit von Relationen und Abbildungen

R, S Relationen von A nach B

- $R = S$ genau dann, wenn für jedes $(a, b) \in A \times B$ gilt:

$$(a, b) \in R \text{ genau dann, wenn } (a, b) \in S.$$

f, g Abbildungen von A nach B

- $f = g$ genau dann, wenn für jedes $(a, b) \in A \times B$ gilt:

$$(a, b) \in f \text{ genau dann, wenn } (a, b) \in g.$$

Gleichheit von Relationen und Abbildungen

R, S Relationen von A nach B

- $R = S$ genau dann, wenn für jedes $(a, b) \in A \times B$ gilt:

$$(a, b) \in R \text{ genau dann, wenn } (a, b) \in S.$$

f, g Abbildungen von A nach B

- $f = g$ genau dann, wenn für jedes $(a, b) \in A \times B$ gilt:

$$f(a) = b \text{ genau dann, wenn } g(a) = b.$$

Gleichheit von Relationen und Abbildungen

R, S Relationen von A nach B

- $R = S$ genau dann, wenn für jedes $(a, b) \in A \times B$ gilt:

$$(a, b) \in R \text{ genau dann, wenn } (a, b) \in S.$$

f, g Abbildungen von A nach B

- $f = g$ genau dann, wenn für jedes $a \in A$ gilt:

$$\text{Für jedes } b \in B \text{ gilt } f(a) = b \text{ gdw. } g(a) = b. \tag{1}$$

Gleichheit von Relationen und Abbildungen

R, S Relationen von A nach B

- $R = S$ genau dann, wenn für jedes $(a, b) \in A \times B$ gilt:

$$(a, b) \in R \text{ genau dann, wenn } (a, b) \in S.$$

f, g Abbildungen von A nach B

- $f = g$ genau dann, wenn für jedes $a \in A$ gilt:

$$\text{Für jedes } b \in B \text{ gilt } f(a) = b \text{ gdw. } g(a) = b. \tag{1}$$

Überlegung:

- Falls $f(a) = g(a)$, so gilt (1).
- Falls $f(a) \neq g(a)$, so gilt (1) nicht.

Gleichheit von Relationen und Abbildungen

R, S Relationen von A nach B

- $R = S$ genau dann, wenn für jedes $(a, b) \in A \times B$ gilt:

$$(a, b) \in R \text{ genau dann, wenn } (a, b) \in S.$$

f, g Abbildungen von A nach B

- $f = g$ genau dann, wenn für jedes $a \in A$ gilt:

$$f(a) = g(a).$$

Gleichheit von Relationen und Abbildungen

R, S Relationen von A nach B

- $R = S$ genau dann, wenn für jedes $(a, b) \in A \times B$ gilt:

$$(a, b) \in R \text{ genau dann, wenn } (a, b) \in S.$$

f, g Abbildungen von A nach B

- $f = g$ genau dann, wenn für jedes $a \in A$ gilt:

$$f(a) = g(a).$$

Abbildung f von A nach B

- eindeutig durch Angabe von $f(a) \in B$ für jedes $a \in A$ festgelegt
- $f(a)$ heißt *Bild von a unter f*

B^A bezeichnet Menge aller Abbildungen von A nach B

Charakteristische Funktionen

Charakteristische Funktion einer Teilmenge A von M

$$\chi_A \colon M \to \{0,1\}, m \mapsto \begin{cases} 1, & \text{falls } m \in A, \\ 0, & \text{falls } m \notin A. \end{cases}$$

Bijektion von 2^M nach $\{0,1\}^M$

$$\chi \colon 2^M \to \{0,1\}^M, A \mapsto \chi_A.$$

Charakteristische Funktionen

Charakteristische Funktion einer Teilmenge A von M

$$\chi_A \colon M \to \{0,1\}, m \mapsto \begin{cases} 1, & \text{falls } m \in A, \\ 0, & \text{falls } m \notin A. \end{cases}$$

Bijektion von 2^M nach $\{0,1\}^M$

$$\chi \colon 2^M \to \{0,1\}^M, A \mapsto \chi_A.$$

- Injektiv: Für jedes $A \in 2^M$ gilt:

$$A = \{m \in M \mid \chi_A(m) = 1\}.$$

Also gilt für alle $A, B \in 2^M$:

$$\text{Wenn } \chi_A = \chi_B, \text{ dann } A = B.$$

Charakteristische Funktionen

Charakteristische Funktion einer Teilmenge A von M

$$\chi_A \colon M \to \{0,1\}, m \mapsto \begin{cases} 1, & \text{falls } m \in A, \\ 0, & \text{falls } m \notin A. \end{cases}$$

Bijektion von 2^M nach $\{0,1\}^M$

$$\chi \colon 2^M \to \{0,1\}^M, A \mapsto \chi_A.$$

- Surjektiv: Für jedes $f \in \{0,1\}^M$ gilt:

$$\chi_{\{m \in M \mid f(m)=1\}} = f.$$

Charakteristische Funktionen

Charakteristische Funktion einer Teilmenge A von M

$$\chi_A \colon M \to \{0,1\}, m \mapsto \begin{cases} 1, & \text{falls } m \in A, \\ 0, & \text{falls } m \notin A. \end{cases}$$

Bijektion von 2^M nach $\{0,1\}^M$

$$\chi \colon 2^M \to \{0,1\}^M, A \mapsto \chi_A.$$

Ist M endlich, so gilt:

$$|2^M| = |\{0,1\}^M| = |\{0,1\}|^{|M|} = 2^{|M|}.$$

Kombinatorik — Zählen von charakteristischen Funktionen

$\{0,1\}^{\{a\}}$

x	a
$f(x)$	0
	1

$\{0,1\}^{\{a,b\}}$

x	a	b
$f(x)$	0	0
	1	0
	0	1
	1	1

$\{0,1\}^{\{a,b,c\}}$

x	a	b	c	A mit $\chi_A = f$
$f(x)$	0	0	0	$\{\}$
	1	0	0	$\{a\}$
	0	1	0	$\{b\}$
	1	1	0	$\{a, b\}$
	0	0	1	$\{c\}$
	1	0	1	$\{a, c\}$
	0	1	1	$\{b, c\}$
	1	1	1	$\{a, b, c\}$

$$|\{0,1\}^M| = 2^{|M|}$$

Kombinatorik — Zählen von Abbildungen

A, B endliche Mengen

Behauptung: $|B^A| = |B|^{|A|}$

Erklärung:

- Für jedes $a \in A$
  gibt es $|B|$ Möglichkeiten
  für das Bild von a

Kombinatorik — Zählen von Tupeln

A, B endliche Mengen

Behauptung: $|A \times B| = |A| \cdot |B|$

Erklärung:

- Jedes $a \in A$ kann mit jedem $b \in B$ gepaart werden
- Anschaulich: Ist $A = \{a_1, a_2, \ldots, a_{|A|}\}$ und $B = \{b_1, b_2, \ldots, b_{|B|}\}$, so führt die Tabelle

$$\begin{array}{cccc} (a_1, b_1) & (a_2, b_1) & \ldots & (a_{|A|}, b_1) \\ (a_1, b_2) & (a_2, b_2) & \ldots & (a_{|A|}, b_2) \\ \ldots & \ldots & \ldots & \ldots \\ (a_1, b_{|B|}) & (a_2, b_{|B|}) & \ldots & (a_{|A|}, b_{|B|}) \end{array}$$

  jedes Tupel genau einmal auf und hat $|A| \cdot |B|$ viele Einträge.

Kombinatorik — Zählen von Relationen

A, B endliche Mengen

Behauptung: Anzahl Relationen von A nach B ist $2^{|A|\cdot|B|}$

Erklärung:

- $2^{A\times B}$ ist Menge aller Relationen von A nach B
- $|2^{A\times B}| = 2^{|A\times B|} = 2^{|A|\cdot|B|}$

Grundlage der Mathematik — Zermelo-Fraenkel-Mengenlehre

Mengen werden axiomatisch in der Sprache der Prädikatenlogik definiert

Jedes mathematische Objekt ist eine Menge

Jede mathematische Aussage ist eine Aussage in Prädikatenlogik über Mengen

Mengenlehre — Tupel

Tupel mit erster Komponente aus A und zweiter aus B

- Für jedes $a \in A$ und jedes $b \in B$
  stehe (a, b) für $\{\{a\}, \{a, b\}\}$ aus $2^{2^{A \cup B}}$
- $(1, 2) = \{\{1\}, \{1, 2\}\} \quad \neq \quad \{\{2\}, \{2, 1\}\} = (2, 1)$
  $(1, 1) = \{\{1\}, \{1, 1\}\} = \{\{1\}\}$

Alle solche Tupel

$$A \times B = \{(a, b) \mid a \in A \text{ und } b \in B\} \subseteq 2^{2^{A \cup B}}$$

Mengenlehre — Tupel

Tupel mit erster Komponente aus A und zweiter aus B

- Für jedes $a \in A$ und jedes $b \in B$
  stehe (a, b) für $\{\{a\}, \{a, b\}\}$ aus $2^{2^{A \cup B}}$
- *Behauptung:* Tupel haben eine erste und eine zweite Komponente und sind eindeutig durch diese bestimmt!

Mengenlehre — Tupel

Tupel mit erster Komponente aus A und zweiter aus B

- Für jedes $a \in A$ und jedes $b \in B$
  stehe (a, b) für $\{\{a\}, \{a, b\}\}$ aus $2^{2^{A \cup B}}$
- *Behauptung:* Tupel haben eine erste und eine zweite Komponente und sind eindeutig durch diese bestimmt!
  Beweis: Es seien $a_1, a_2 \in A$ und es seien $b_1, b_2 \in B$.

Mengenlehre — Tupel

Tupel mit erster Komponente aus A und zweiter aus B

- Für jedes $a \in A$ und jedes $b \in B$
  stehe (a, b) für $\{\{a\}, \{a, b\}\}$ aus $2^{2^{A \cup B}}$
- *Behauptung:* Tupel haben eine erste und eine zweite Komponente und sind eindeutig durch diese bestimmt!
  Beweis: Es seien $a_1, a_2 \in A$ und es seien $b_1, b_2 \in B$.
  Dann gilt $(a_1, b_1) = (a_2, b_2)$ genau dann, wenn $\{\{a_1\}, \{a_1, b_1\}\} = \{\{a_2\}, \{a_2, b_2\}\}$ gilt.

Mengenlehre — Tupel

Tupel mit erster Komponente aus A und zweiter aus B

- Für jedes $a \in A$ und jedes $b \in B$
  stehe (a, b) für $\{\{a\}, \{a, b\}\}$ aus $2^{2^{A \cup B}}$
- *Behauptung:* Tupel haben eine erste und eine zweite Komponente und sind eindeutig durch diese bestimmt!
  Beweis: Es seien $a_1, a_2 \in A$ und es seien $b_1, b_2 \in B$.
  Dann gilt $(a_1, b_1) = (a_2, b_2)$ genau dann, wenn $\{\{a_1\}, \{a_1, b_1\}\} = \{\{a_2\}, \{a_2, b_2\}\}$ gilt.
  Letzteres gilt genau dann, wenn
  - $\{a_1\} = \{a_2\}$ und $\{a_1, b_1\} = \{a_2, b_2\}$, oder
  - $\{a_1\} = \{a_2, b_2\}$ und $\{a_1, b_1\} = \{a_2\}$.

Mengenlehre — Tupel

Tupel mit erster Komponente aus A und zweiter aus B

- Für jedes $a \in A$ und jedes $b \in B$
  stehe (a, b) für $\{\{a\}, \{a, b\}\}$ aus $2^{2^{A \cup B}}$
- *Behauptung:* Tupel haben eine erste und eine zweite Komponente und sind eindeutig durch diese bestimmt!
  Beweis: Es seien $a_1, a_2 \in A$ und es seien $b_1, b_2 \in B$.
  Dann gilt $(a_1, b_1) = (a_2, b_2)$ genau dann, wenn $\{\{a_1\}, \{a_1, b_1\}\} = \{\{a_2\}, \{a_2, b_2\}\}$ gilt.
  Letzteres gilt genau dann, wenn
  - $\{a_1\} = \{a_2\}$ und $\{a_1, b_1\} = \{a_2, b_2\}$, oder
  - $\{a_1\} = \{a_2, b_2\}$ und $\{a_1, b_1\} = \{a_2\}$.

  Der erste Fall gilt genau dann, wenn $a_1 = a_2$ und $b_1 = b_2$, und der zweite Fall genau dann, wenn $a_1 = a_2 = b_1 = b_2$.

Mengenlehre — Tupel

Tupel mit erster Komponente aus A und zweiter aus B

- Für jedes $a \in A$ und jedes $b \in B$
  stehe (a, b) für $\{\{a\}, \{a, b\}\}$ aus $2^{2^{A \cup B}}$
- *Behauptung:* Tupel haben eine erste und eine zweite Komponente und sind eindeutig durch diese bestimmt!
  Beweis: Es seien $a_1, a_2 \in A$ und es seien $b_1, b_2 \in B$.
  Dann gilt $(a_1, b_1) = (a_2, b_2)$ genau dann, wenn $\{\{a_1\}, \{a_1, b_1\}\} = \{\{a_2\}, \{a_2, b_2\}\}$ gilt.
  Letzteres gilt genau dann, wenn
  - $\{a_1\} = \{a_2\}$ und $\{a_1, b_1\} = \{a_2, b_2\}$, oder
  - $\{a_1\} = \{a_2, b_2\}$ und $\{a_1, b_1\} = \{a_2\}$.

  Der erste Fall gilt genau dann, wenn $a_1 = a_2$ und $b_1 = b_2$, und der zweite Fall genau dann, wenn $a_1 = a_2 = b_1 = b_2$.
  Insgesamt gilt $(a_1, b_1) = (a_2, b_2)$ genau dann, wenn $a_1 = a_2$ und $b_1 = b_2$.

Mengenlehre — Nicht-negative ganze Zahlen

Jede nicht-negative ganze Zahl

- 0 stehe für $\emptyset$
- 1 stehe für $0 \cup \{0\} = \{0\}$
- 2 stehe für $1 \cup \{1\} = \{0, 1\}$
- 3 stehe für $2 \cup \{2\} = \{0, 1, 2\}$
- usw.

Diese Mengen sind paarweise verschieden!

Alle solche Zahlen

$$\mathbb{N}_0 = \bigcap_{\substack{\emptyset \in A \\ \text{und für jedes } a \in A \text{ gilt } a \cup \{a\} \in A}} A$$

Mengenlehre — Ordnungsrelation und Addition

Ordnungsrelation

$$\leq = \{(n_1, n_2) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n_1 \subseteq n_2\}$$

Nachfolgerabbildung

$$s \colon \mathbb{N}_0 \to \mathbb{N}_0, n \mapsto n \cup \{n\}$$

Addition

$$+ \colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0,$$

$$(n_1, n_2) \mapsto \begin{cases} n_1, & \text{falls } n_2 = 0, \\ s(n_1 + n_3), & \text{falls } n_2 = s(n_3) \text{ für ein } n_3 \in \mathbb{N}_0. \end{cases}$$

Zu beweisen: + ist wohldefiniert, das heißt, die Selbstrekursion terminiert.

fin.