Informatik I

8. Mathematische Exkursion: Binäre Relationen

Jan-Georg Smaus

Albert-Ludwigs-Universität Freiburg

23. November 2010

Informatik I

23. November 2010 — 8. Mathematische Exkursion: Binäre Relationen

Relationen

Definition

Eine binäre Relation R ist eine Teilmenge ($\subseteq$) von $A \times B$, wobei A, B Mengen sind.
Wir schreiben $(a, b) \in R$ oder $a\ R\ b$.

Zu einer binären Relation R ist $R^{-1} \subseteq B \times A$ die Umkehrrelation mit $R^{-1} = \{(b, a) \mid (a, b) \in R\}$.

Im Folgenden betrachten wir ausschließlich binäre Relationen.

Beispiele

1. $\emptyset \subseteq A \times B$, die leere Relation;
2. $A \times B$, die volle Relation;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$, die Gleichheit;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$;
6. $| \subseteq \mathbb{N} \times \mathbb{N}$ mit $m|n$ falls ein $c \in \mathbb{N}$ existiert mit $c \cdot m = n$;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$, wobei $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$.

8.1 Darstellung

Darstellung von Relationen

Matrix

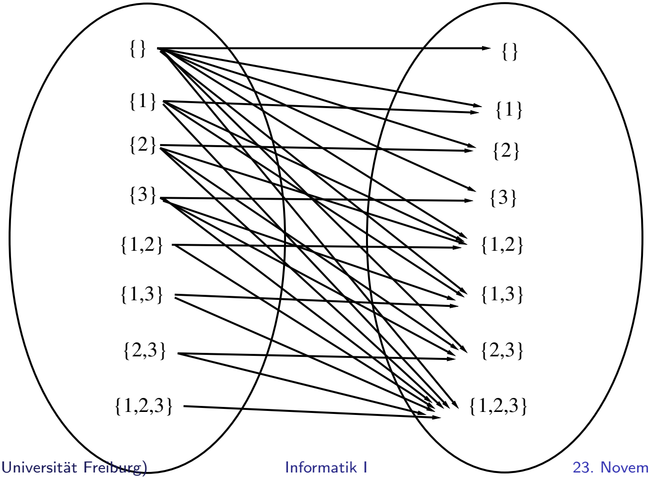
$\subseteq\, \subseteq\, \mathcal{P}(\{1,2,3\}) \times \mathcal{P}(\{1,2,3\})$, wobei $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$, lässt sich gut als Matrix darstellen:

$\subseteq$	$\emptyset$	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$
$\emptyset$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$	$\surd$
$\{1\}$		$\surd$			$\surd$	$\surd$		$\surd$
$\{2\}$			$\surd$		$\surd$		$\surd$	$\surd$
$\{3\}$				$\surd$		$\surd$	$\surd$	$\surd$
$\{1,2\}$					$\surd$			$\surd$
$\{1,3\}$						$\surd$		$\surd$
$\{2,3\}$							$\surd$	$\surd$
$\{1,2,3\}$								$\surd$

Darstellung von Relationen

Pfeildiagramm

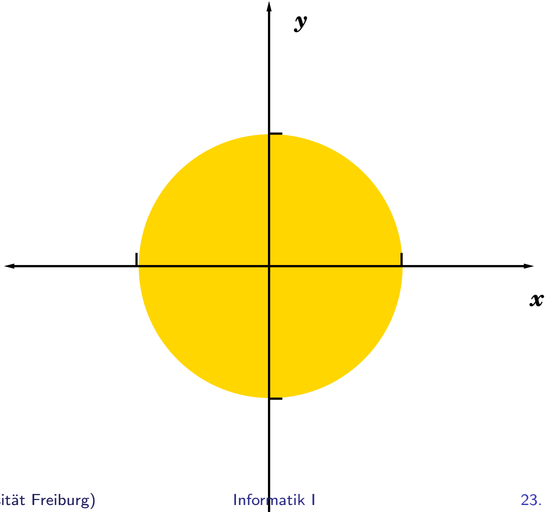
$\subseteq \subseteq\ \mathcal{P}(\{1,2,3\}) \times \mathcal{P}(\{1,2,3\})$, wobei $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$, lässt sich auch als Pfeildiagramm darstellen:



Darstellung von Relationen

Graph

$K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ (7) ist eine Kreisfläche und lässt sich gut als Graph darstellen.

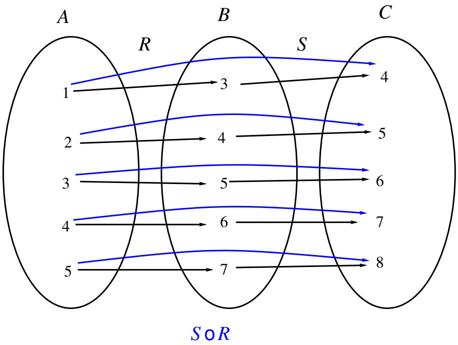


8.2 Komposition

Komposition

Definition

Seien $R \subseteq A \times B$ und $S \subseteq B \times C$. Dann ist $S \circ R$ die Komposition von R und S mit $S \circ R \subseteq A \times C$ und
$S \circ R = \{(a, c) \mid \text{es gibt } b \in B \text{ mit } (a, b) \in R \text{ und } (b, c) \in S\}$.



Beachte: Man findet in der Literatur auch die Notation $R \circ S$.

$I_A = R^{-1} \circ R$?

- Gilt im Allgemeinen $I_A = R^{-1} \circ R$?
  Nein!
- Gilt im Allgemeinen $R^{-1} \circ R \subseteq I_A$?
  Nein, nimm $A = \{0, 1, 2\}$ und $R = \{(0, 1), (2, 1)\}$. Dann gilt $(0, 2) \in R^{-1} \circ R$, aber $(0, 2) \notin I_A = \{(0, 0), (1, 1), (2, 2)\}$.
- Gilt im Allgemeinen $I_A \subseteq R^{-1} \circ R$?
  Nein, nimm $A = \{0, 1, 2\}$ und $R = \emptyset$. Dann gilt $(0, 0) \in I_A$, aber $(0, 0) \notin R^{-1} \circ R = \emptyset$.
  Oder nimm $A = \{0, 1, 2\}$ und $R = \{(0, 1), (2, 1)\}$. Dann ist $R^{-1} \circ R = \{(0, 0), (0, 2), (2, 0), (2, 2)\}$ und somit $(1, 1) \notin R^{-1} \circ R$.

8.3 Wichtige Eigenschaften

. . . eindeutigkeit

Definition

Sei $R \subseteq A \times B$.

1. R ist linkseindeutig (injektiv) falls gilt: wenn $a\ R\ b$ und $a'\ R\ b$, dann $a = a'$.
2. R ist rechtseindeutig falls gilt: wenn $a\ R\ b$ und $a\ R\ b'$, dann $b = b'$. Rechtseindeutige Relationen heißen partielle Funktionen.

...eindeutigkeit

1. $\emptyset \subseteq A \times B$ ist links- und rechtseindeutig;
2. $A \times B$ ist weder noch;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$ ist links- und rechtseindeutig;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ ist weder noch;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$ ist weder noch;
6. $\mid \subseteq \mathbb{N} \times \mathbb{N}$, mit $m|n$ falls ein $c \in \mathbb{N}$ existiert mit $c \cdot m = n$, ist weder noch;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ ist weder noch;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ ist weder noch;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ ist weder noch.

Äquivalenzrelationen u.ä.

Definition

Sei $R \subseteq A \times A$ eine Relation über A.

1. R heißt reflexiv, falls $(\forall a \in A)\ a\,R\,a$;
2. R heißt irreflexiv, falls $(\forall a \in A)\ \neg(a\,R\,a)$;
3. R heißt symmetrisch, falls $(\forall x, y \in A)$: wenn $x\,R\,y$ dann auch $y\,R\,x$;
4. R heißt antisymmetrisch, falls $(\forall x, y \in A)$: wenn $x\,R\,y$ und $y\,R\,x$ dann $x = y$;
5. R heißt transitiv, falls $(\forall x, y, z \in A)$: wenn $x\,R\,y$ und $y\,R\,z$ dann $x\,R\,z$;
6. R heißt Äquivalenzrelation, falls R reflexiv, transitiv und symmetrisch ist.

Reflexiv?

R heißt reflexiv, falls $(\forall a \in A)\ a\ R\ a$.

1. $\emptyset \subseteq A \times A$ nein
2. $A \times A$ ja;
3. $I_A \subseteq A \times A$ ja;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ ja;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$ nein;
6. $| \subseteq \mathbb{N} \times \mathbb{N}$ ja;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ nein;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ ja;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ ja.

Irreflexiv?

R heißt irreflexiv, falls $(\forall a \in A)\ \neg(a\ R\ a)$.

1. $\emptyset \subseteq A \times A$ ja
2. $A \times A$ nein
3. $I_A \subseteq A \times A$ nein
4. $\leq\ \subseteq\ \mathbb{N} \times \mathbb{N}$ nein
5. $<\ \subseteq\ \mathbb{N} \times \mathbb{N}$ ja
6. $|\ \subseteq\ \mathbb{N} \times \mathbb{N}$ nein
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ nein
8. $\subseteq\ \subseteq\ \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ nein;
9. $\sim\ \subseteq\ (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ nein.

Symmetrisch?

R heißt symmetrisch, falls $(\forall x, y \in A)$: wenn $x\,R\,y$ dann auch $y\,R\,x$.

1. $\emptyset \subseteq A \times A$ ja;
2. $A \times A$ ja;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$ ja;
4. $\leq\ \subseteq\ \mathbb{N} \times \mathbb{N}$ nein;
5. $<\ \subseteq\ \mathbb{N} \times \mathbb{N}$ nein;
6. $\mid\ \subseteq\ \mathbb{N} \times \mathbb{N}$ nein;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ ja;
8. $\subseteq\ \subseteq\ \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ nein;
9. $\sim\ \subseteq\ (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ ja.

Antisymmetrisch?

R heißt antisymmetrisch, falls $(\forall x, y \in A)$: wenn $x\,R\,y$ und $y\,R\,x$ dann $x = y$.

1. $\emptyset \subseteq A \times A$ ja;
2. $A \times A$ nein;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$ ja;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ ja;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$ ja;
6. $\mid \subseteq \mathbb{N} \times \mathbb{N}$ ja;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ nein;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ ja;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ nein.

Transitiv?

R heißt transitiv, falls $(\forall x, y, z \in A)$: wenn $x\,R\,y$ und $y\,R\,z$ dann $x\,R\,z$.

1. $\emptyset \subseteq A \times A$ ja;
2. $A \times A$ ja;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$ ja;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ ja;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$ ja;
6. $\mid \subseteq \mathbb{N} \times \mathbb{N}$ ja;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ nein;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ ja;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ ja.

Äquivalenzrelation?

R heißt Äquivalenzrelation, falls R reflexiv, transitiv und symmetrisch ist.

1. $\emptyset \subseteq A \times A$ nein;
2. $A \times A$ ja;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$ ja;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ nein;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$ nein;
6. $\mid \subseteq \mathbb{N} \times \mathbb{N}$ nein;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ nein;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ nein;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ ja.

8.4 Die Relation $\sim$

Die Relation $\sim$

Die Relation $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$, kann man benutzen, um aus den natürlichen Zahlen die ganzen Zahlen zu konstruieren.
Idee: stelle jede ganze Zahl als Differenz von zwei natürlichen Zahlen dar.

$$\begin{array}{rcl} 0 & \hat{=} & (0,0) \sim (1,1) \sim (150000, 150000) \\ 2 & \hat{=} & (2,0) \sim (3,1) \sim (150002, 150000) \\ -2 & \hat{=} & (0,2) \sim (1,3) \sim (150000, 150002) \end{array}$$

Es gilt z.B. $2 + 1 = 3 + 0$ oder $0 + 3 = 2 + 1$.
Trick: man verwendet $-$ in der Definition nicht, denn $+$ ist auf den natürlichen Zahlen total definiert, $-$ aber nicht.

Die Addition und Subtraktion auf den ganzen Zahlen

$$(n, m) \oplus (n', m') = (n + n', m + m')$$

denn $(n - m) + (n' - m') = (n + n') - (m + m')$.

$$(n, m) \ominus (n', m') = (n + m', m + n')$$

Wir dürfen $-$ „offiziell" nicht benutzen.
Nebenrechnung: $(n - m) - (n' - m') = (n + m') - (m + n')$.

Übung: definiere $\odot$, die Multiplikation auf den ganzen Zahlen.

Die Relation $\bowtie$

Definiere $\bowtie \subseteq (\mathbb{N} \times (\mathbb{Z} \setminus \{0\})) \times (\mathbb{N} \times (\mathbb{Z} \setminus \{0\}))$ mit $(m, n) \bowtie (m', n')$ gdw. $m \cdot n' = n \cdot m'$.
Was ist das und wozu könnte es gut sein?

Die Relation $\bowtie$ kann man benutzen, um aus den natürlichen und ganzen Zahlen die rationalen Zahlen zu konstruieren.

Das nennen wir Bruch und schreiben normalerweise $\frac{n}{m}$. Dass eine Zahl sich auf verschiedene Arten als Bruch schreiben lässt, ist bekannt.

8.5 Ordnungen

- Definitionen
- Minimale, kleinste, maximale, größte Elemente
- Wohlfundiertheit
- Induktion
- Wohlordnungen

Ordnungen

Definition

Sei R eine Relation über A.

- R ist eine Quasiordnung, falls R reflexiv und transitiv ist.
- R ist eine Halbordnung, falls R reflexiv, transitiv und antisymmetrisch ist.
- R ist eine totale Ordnung, falls R eine Halbordnung ist und $(\forall a, b \in R)$ gilt $a\,R\,b$ oder $b\,R\,a$.

Ordnungen?

- Quasiordnung: reflexiv und transitiv
- Halbordnung: reflexiv, transitiv und antisymmetrisch
- Totale Ordnung: Halbordnung und $a\,R\,b$ oder $b\,R\,a$.

1. $\emptyset \subseteq A \times A$ nein;
2. $A \times A$ Quasiordnung;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$ Halbordnung;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ totale Ordnung;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$ nein;
6. $\mid \subseteq \mathbb{N} \times \mathbb{N}$ Halbordnung;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ nein;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ Halbordnung;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ Quasiordnung.

Strikte (strenge) Ordnungen

Die Definitionen von Halbordnung und totale Ordnung lassen sich abwandeln, indem wir Irreflexivität statt Reflexivität annehmen:

Definition

Sei R eine Relation über A.

- R ist eine strikte (strenge) Ordnung, falls R irreflexiv, transitiv (und antisymmetrisch) ist.
- R ist eine strikte (strenge) totale Ordnung, falls R eine strikte Ordnung ist und $(\forall a, b \in R)$ gilt $a\,R\,b$ oder $b\,R\,a$ oder $a = b$.

Was ist mit Quasiordnungen? Es bleibt nur Transitivität übrig; hierfür führen wir keinen neuen Namen ein.

Strikte Ordnungen?

- Strikte Ordnung: irreflexiv, transitiv (und antisymmetrisch)
- Strikte totale Ordnung: strikte Ordnung und $a\,R\,b$ oder $b\,R\,a$ oder $a = b$.

1. $\emptyset \subseteq A \times A$ strikte Ordnung;
2. $A \times A$ nein;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$ nein;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ nein;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$ strikte totale Ordnung;
6. $| \subseteq \mathbb{N} \times \mathbb{N}$ nein, aber man kann die strikte Ordnung „teilt echt“ definieren;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ nein;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ nein, aber $\subset$ ist eine strikte Ordnung;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ nein.

Minimale und kleinste Elemente

Sei $R \subseteq A \times A$ eine Relation und sei $B \subseteq A$ (es hilft, sich R als $\leq$ vorzustellen).

Definition

- Ein Element $z \in B$ heißt minimales Element von B bzgl. R falls $(\forall y \in B)$ gilt: $y \mathrel{R} z$ impliziert $y = z$.
- Ein Element $z \in B$ heißt kleinstes Element von B bzgl. R falls $(\forall y \in B)$ gilt: $z \mathrel{R} y$.
- Ein Element $z \in B$ heißt maximales Element von B bzgl. R falls $(\forall y \in B)$ gilt: $z \mathrel{R} y$ impliziert $y = z$.
- Ein Element $z \in B$ heißt größtes Element von B bzgl. R falls $(\forall y \in B)$ gilt: $y \mathrel{R} z$.

Wenn R aus dem Zusammenhang klar ist, kann man den Zusatz „bzgl. R“ auch weglassen.

Minimale und kleinste Elemente

Beispiele

$A = B = \mathbb{N}$ mit $R = \leq$: 0 ist sowohl ein minimales als auch das kleinste Element.

Es existieren kein maximales oder größtes Element.

Betrachten wir wieder $\subseteq \subseteq \mathcal{P}(\{1,2,3\}) \times \mathcal{P}(\{1,2,3\})$ und $B = \{\{1\},\{2\},\{1,2,3\}\}$.

$\{1\}$ und $\{2\}$ sind beide minimal, aber keines der beiden ist das kleinste Element. Es gibt kein kleinstes.

$\{1,2,3\}$ ist das einzige maximale, und zugleich das größte Element.

Wohlfundiertheit

Definition

Eine Relation $R \subseteq A \times A$ heißt wohlfundiert, falls R irreflexiv ist und jedes nichtleere $B \subseteq A$ mindestens ein minimales Element bzgl. R besitzt.

Definition

Sei $R \subseteq A \times A$ ein Relation. Eine unendliche absteigende Kette bzgl. R ist eine unendliche Folge $a_1, a_2, \ldots,$ mit $a_{i+1} \mathrel{R} a_i$.

Beispiel: $<$ auf $\mathbb{Z}$. Dann ist $0, -1, -2, \ldots$ eine unendliche absteigende Kette, denn $\ldots -2 < -1 < 0$.

Satz

Eine Relation $R \subseteq A \times A$ ist wohlfundiert gdw. keine unendliche absteigende Kette bzgl. R existiert.

Beweistechniken

- Einen Beweis einer Aussage der Form „A gdw. B“ führt man normalerweise, indem man im ersten Teil A annimmt und B folgert und im zweiten Teil B annimmt und A folgert.
- Einen Beweis einer Aussage der Form „aus A folgt B“ wird häufig als Widerspruchsbeweis geführt: A ist die Voraussetzung; nun macht man die „Annahme“ $\neg$B und leitet einen Widerspruch her. Da A und $\neg$B einen Widerspruch implizieren, folgt B aus A.

Beweis, Teil 1 („Hinrichtung“)

Satz

Eine Relation $R \subseteq A \times A$ ist wohlfundiert gdw. keine unendliche absteigende Kette bzgl. R existiert.

Beweis.

„$\Rightarrow$“: Sei R wohlfundiert. Um einen Widerspruch herzuleiten, nehmen wir nun an, es existiere eine unendliche absteigende Kette $a_1, a_2, \ldots,$. Definiere $B := \{a_i \mid i \in \mathbb{N}\}$. Da R wohlfundiert und B nichtleer ist, hat B ein minimales Element a_i, d.h. $(\forall y \in B)$ gilt: $y \; R \; a_i$ impliziert $y = a_i$. Da R wohlfundiert und somit irreflexiv ist, muss gelten: $(\nexists y)$ mit $y \; R \; a_i$. Da laut Annahme $a_1, a_2, \ldots,$ eine unendliche absteigende Kette ist, gilt aber $a_{i+1} \; R \; a_i$. Somit haben wir einen Widerspruch.

Beweis, Teil 2 („Rückrichtung“)

Satz

Eine Relation $R \subseteq A \times A$ ist wohlfundiert gdw. keine unendliche absteigende Kette bzgl. R existiert.

Beweis.

„$\Leftarrow$“: Voraussetzung: es existiert keine unendliche absteigende Kette $a_1, a_2, \ldots,$ bzgl. R. Um einen Widerspruch herzuleiten, nehmen wir nun an, R sei nicht wohlfundiert, d.h. eine der beiden folgenden Aussagen gelte:

1. R ist nicht irreflexiv, d.h., es existiert ein $a \in A$ mit $(a, a) \in R$.
2. Es existiert ein nichtleeres $B \subseteq A$, das kein minimales Element besitzt, d.h, ein $B \subseteq A$ derart, dass $(\forall z \in B)\ (\exists y \in B)\ (y\ R\ z) \wedge y \neq z$.

...

Beweis, Teil 2a

Satz

Eine Relation $R \subseteq A \times A$ ist wohlfundiert gdw. keine unendliche absteigende Kette bzgl. R existiert.

Beweis.

„$\Leftarrow$“: Voraussetzung: es existiert keine unendliche absteigende Kette $a_1, a_2, \ldots,$ bzgl. R. Um einen Widerspruch herzuleiten, nehmen wir nun an, R sei nicht wohlfundiert, d.h. eine der beiden folgenden Aussagen gelte:

1. R ist nicht irreflexiv, d.h., es existiert ein $a \in A$ mit $(a, a) \in R$.
2. ...

Im ersten Fall ist $a, a, a, \ldots$ eine unendliche absteigende Kette und wir haben einen Widerspruch.

Beweis, Teil 2b

Satz

Eine Relation $R \subseteq A \times A$ ist wohlfundiert gdw. keine unendliche absteigende Kette bzgl. R existiert.

Beweis.

„$\Leftarrow$“: Vorauss.: es existiert keine unendliche absteigende Kette $a_1, a_2, \ldots,$ bzgl. R. Nimm an, R sei nicht wohlfundiert, d.h.:

2. Es existiert ein nichtleeres $B \subseteq A$, das kein minimales Element besitzt, d.h, ein $B \subseteq A$ derart, dass $(\forall z \in B)\ (\exists y \in B)\ (y\ R\ z) \wedge y \neq z$.

Im zweiten Fall wähle ein beliebiges Element aus B aus und nenne es a_1. Dann existiert laut obiger Formel ein $y \in B$ sodass $(y\ R\ a_1) \wedge y \neq a_1$. Nenne dieses y fortan a_2. Dann existiert laut obiger Formel ein (i.A. anderes!) $y \in B$ sodass $(y\ R\ a_2) \wedge y \neq a_2$. Nenne dieses y fortan a_3 . . .

Beweis, Teil 2b'

Satz

Eine Relation $R \subseteq A \times A$ ist wohlfundiert gdw. keine unendliche absteigende Kette bzgl. R existiert.

Beweis.

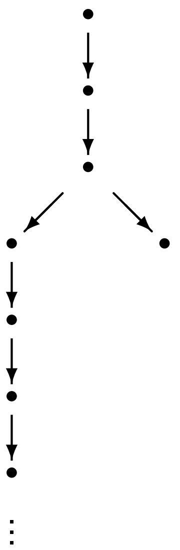
„$\Leftarrow$“: Vorauss.: es existiert keine unendliche absteigende Kette $a_1, a_2, \ldots,$ bzgl. R. Nimm an, R sei nicht wohlfundiert, d.h.:

2. Es existiert ein $B \subseteq A$, das kein minimales Element besitzt, d.h, ein $B \subseteq A$ derart, dass $(\forall z \in B)\ (\exists y \in B)\ (y\ R\ z) \wedge y \neq z$.

...

$a_1, a_2, \ldots$ ist eine unendliche absteigende Kette, also haben wir einen Widerspruch. □

Warum so kompliziert?



Warum heißt es in der Definition von Wohlfundiertheit „jedes nichtleere $B \subseteq A$ mindestens ein minimales Element bzgl. R besitzt" statt einfach „A mindestens ein minimales Element bzgl. R besitzt"?

Die Bedingung über Teilmengen erzwingt, dass jede Kette endlich ist. Die Existenz eines minimalen Elements in A reicht nicht aus.

Wohlfundiert?

Eine Relation $R \subseteq A \times A$ ist wohlfundiert gdw. keine unendliche absteigende Kette bzgl. R existiert.

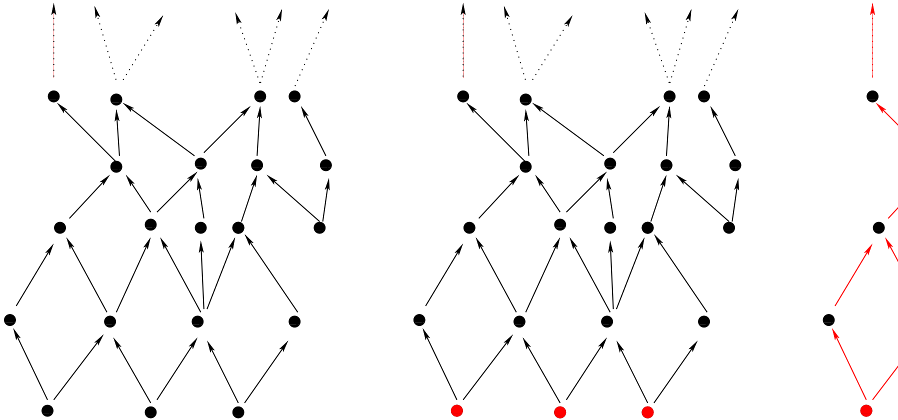
1. $\emptyset \subseteq A \times A$ ja;
2. $A \times A$ nein;
3. $I_A \subseteq A \times A$ mit $I_A = \{(a, a) \mid a \in A\}$ nein;
4. $\leq \subseteq \mathbb{N} \times \mathbb{N}$ nein;
5. $< \subseteq \mathbb{N} \times \mathbb{N}$ ja;
6. $\mid \subseteq \mathbb{N} \times \mathbb{N}$ nein;
7. $K = \{(x, y) \mid x^2 + y^2 \leq 1\} \subseteq \mathbb{R} \times \mathbb{R}$ nein;
8. $\subseteq \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ nein;
9. $\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ mit $(m, n) \sim (m', n')$ gdw. $m + n' = n + m'$ nein.

$\subset \subseteq \mathcal{P}(\{1, 2, 3\}) \times \mathcal{P}(\{1, 2, 3\})$ ja;

Wozu Wohlfundiertheit?

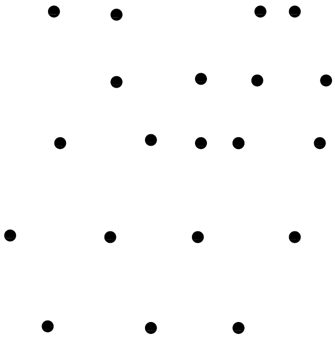
Wenn eine Menge mit einer wohlfundierten Relation ausgestattet ist, kann man Induktion benutzen, um Eigenschaften aller Elemente der Menge zu beweisen.

Induktion: Illustration



Die Menge mit wohlfundierter Relation Induktionsbasis (Teil des Beweises) Induktionsschritt (Teil des Beweises) Eigenschaft gilt für alle Elemente (folgt automatisch)

Induktion mit der leeren Menge



Das Prinzip der Induktion gilt auch für die leere Relation als wohlfundierte Relation, nur nützt es einem nichts!

Induktion formal

Sei $R \subseteq A \times A$ eine wohlfundierte Relation und $P(x)$ eine zu beweisende Eigenschaft für $x \in A$.

1. Induktionsbasis: $(\forall x \in A)\ ((\nexists y \in A)\ y\,R\,x) \Rightarrow P(x)$
2. Induktionsschritt: $(\forall x \in A)\ ((\forall y \in A)\ y\,R\,x \Rightarrow P(y)) \Rightarrow P(x)$

Hinweis: ❶ folgt aus ❷ und damit bei dieser Formulierung eigentlich überflüssig: Sei in ❷ ein $x \in A$ sodass $(\nexists y \in A)\ y\,R\,x$ gilt. Was passiert dann mit $(\forall y \in A)\ y\,R\,x \Rightarrow P(y)$? Es gilt trivialerweise, und wir müssen „ohne Hilfe irgendeines $P(y)$“ $P(x)$ zeigen, genau wie in ❶.
Wir verwenden trotzdem die Formulierung mit ❶ und ❷, weil Beweise häufig aus zwei Teilen bestehen, die ❶ und ❷ entsprechen.

Es gibt verschiedene Formulierungen von Induktion, wie wir noch sehen werden.

Wohlordnung

Definition

Eine Wohlordnung ist eine wohlfundierte strikte totale Ordnung.

Beispiele

- $< \in \mathbb{N} \times \mathbb{N}$ ist eine Wohlordnung.
  Man sagt auch: $(\mathbb{N}, <)$ ist wohlgeordnet.
- $R = \{(n, n+1) \mid n \in \mathbb{N}\}$ ist keine Wohlordnung, da nicht transitiv:
  $(1, 2) \in R$, $(2, 3) \in R$, aber $(1, 3) \notin R$.
  Aber R ist eine wohlfundierte Relation.
- $\mathcal{P}(M)$ mit $M \neq \emptyset$ und Relation $\subset$ (echte Teilmenge) ist keine Wohlordnung, da nicht total.
  Aber $\subset$ ist eine wohlfundierte Relation.

Striktheit

- Die Frage „strikt oder nicht strikt" (d.h., „reflexiv oder irreflexiv") wird manchmal etwas vage behandelt, siehe etwa den Wikipedia-Artikel zu Wohlordnung, wo die Beispiele offensichtlich irreflexiv sind, obwohl eine Wohlordnung eine totale Ordnung, also reflexiv sein soll. Dies ist vielleicht verwirrend.
- Entscheidend ist folgendes: zu jeder reflexiven Relation gibt es eine korrespondierende irreflexive (Wegnahme aller Paare (a, a)). Letztere ist die, die man bei Wohlfundiertheit wirklich meint, etwa wenn man sagt: „Diese Kette ist absteigend und somit endlich".

8.6 Natürliche Zahlen

Natürliche Zahlen

Definition (Meschkowski)

Die Menge $\mathbb{N}$ der natürlichen Zahlen ist eine total geordnete Menge mit

1. $(\mathbb{N}, <)$ besitzt kein größtes Element;
2. $(\mathbb{N}, <)$ ist wohlgeordnet;
3. Jedes $n \in \mathbb{N} \setminus \{0\}$ besitzt genau einen Vorgänger.

Beispiel für eine nicht-konstruktive Definition. Nicht offensichtlich, dass

- es überhaupt eine solche Menge $\mathbb{N}$ gibt und
- sie durch 1 bis 3 bis auf Umbenennungen eindeutig definiert ist.

Peano-Axiome

Definition (Peano-Axiome)

Die Menge $\mathbb{N}$ der natürlichen Zahlen ist definiert durch:

- P1 $0 \in \mathbb{N}$ (Null)
- P2 $(\forall n \in \mathbb{N})\ n' \in \mathbb{N}$ (Nachfolger)
- P3 $(\forall n \in \mathbb{N})\ n' \neq 0$ (Nachfolger ist nicht Null)
- P4 $(\forall m, n \in \mathbb{N})\ m \neq n \Rightarrow m' \neq n'$ (Nachfolger ist injektiv)
- P5 Für jede Menge $M \subseteq \mathbb{N}$ mit $0 \in M$ und $(\forall n)\ n \in M \Rightarrow n' \in M$ gilt $M = \mathbb{N}$ (Induktionsaxiom)

P5 schließt aus, dass man zu den natürlichen Zahlen ein „größtes Element“ hinzunimmt o.Ä.

Das Beweisschema der vollständigen Induktion

Sei $P(n)$ eine Eigenschaft einer Zahl $n \in \mathbb{N}$ (Prädikat).
Zeige $(\forall n \in \mathbb{N})\ P(n)$.
Definiere $M := \{n \in \mathbb{N} \mid P(n) \text{ gilt}\} \subseteq \mathbb{N}$.
Induktionsaxiom: Falls $0 \in M$ und $(\forall n)\ n \in M \Rightarrow n' \in M$ dann $M = \mathbb{N}$.

Induktionsschema

Falls $P(0)$ (Induktionsbasis, -anfang)
und
$(\forall n)\ P(n) \Rightarrow P(n')$ (Induktionsschritt)
dann
$(\forall n \in \mathbb{N})\ P(n)$. ($P(n)$ Induktionshypothese, -behauptung)

Beispiel I

Behauptung: für alle $n \in \mathbb{N}$ gilt

$$\sum_{i=0}^{n} i = \frac{n \cdot (n+1)}{2} \equiv P(n)$$

Induktionsbasis ($P(0)$):

$$\sum_{i=0}^{0} i = 0 = \frac{0 \cdot (0+1)}{2}$$

Induktionsschritt ($P(n) \Rightarrow P(n+1)$ für alle $n \in \mathbb{N}$):

$$\sum_{i=0}^{n+1} i = n+1+\sum_{i=0}^{n} i \overset{\text{IH}}{=}$$
$$n+1+\frac{n \cdot (n+1)}{2} = \frac{2n+2+n \cdot (n+1)}{2} = \frac{n^2+3n+2}{2} =$$
$$\frac{(n+1) \cdot (n+2)}{2} = \frac{(n+1) \cdot ((n+1)+1)}{2}$$

Beispiel II

Behauptung: für alle $n \in \mathbb{N}$ gilt

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \equiv P(n)$$

Induktionsbasis ($P(0)$):

$$\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$$

Induktionsschritt ($P(n) \Rightarrow P(n+1)$ für alle $n \in \mathbb{N}$):

$$\sum_{i=0}^{n+1} 2^i = 2^{n+1} + \sum_{i=0}^{n} 2^i \stackrel{\mathrm{IH}}{=}$$
$$2^{n+1} + 2^{n+1} - 1 = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1 = 2^{(n+1)+1} - 1$$

Zusammenfassung

- Binäre Relationen und ihre Eigenschaften: Links- und Rechtseindeutigkeit, Reflexivität, Irreflexivität, Symmetrie, Antisymmetrie, Transitivität, Äquivalenzrelation, Quasiordnung, (strikte) Halbordnung, (strikte) totale Ordnung.
- Minimale, kleinste, maximale, größte Elemente
- Wohlfundiertheit und Induktion im Allgemeinen
- Natürliche Zahlen und Beweise darauf

…und hoffentlich ein verbessertes Gespür für Mathematik und Beweisen.