Grundlagen Theoretischer Informatik I

SoSe 2011 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

Grundlagen Theoretischer Informatik I Gesamtübersicht

- Organisatorisches; Einführung
- Logik & Beweisverfahren
- Mengenlehre
- reguläre Sprachen

Spezielle Relationen

- Äquivalenzrelationen
- Halbordnungen
- Funktionen

Äquivalenzrelationen

Eine *Äquivalenzrelation* ist eine binäre Relation über M, die reflexiv, symmetrisch und transitiv ist.

Beispiel: Allrelation und Diagonale sind Äquivalenzrelationen.

Beispiel: $R = \{(a, b), (b, a)\} \cup \Delta_{\{a,b,c,d\}}$ ist eine Äquivalenzrelation.

Beispiel: Betrachte das Warenangebot eines Supermarktes. Die Preisgleichheit liefert eine Äquivalenzrelation auf der Menge der angebotenen Waren.

Beispiel: $R_m = \{(a, b) \in \mathbb{Z}^2 : m \mid (a - b)\}$. Eigenschaften nachrechnen!
Schreibweise: $a \equiv b \mod m$ statt aR_mb.

Partitionen

Es sei M eine Menge, $M \neq \emptyset$. Eine *Zerlegung*, *Klasseneinteilung* oder *Partition* von M ist eine *Mengenfamilie* $Z \subseteq 2^M$ mit:

1. $M = \bigcup_{A \in Z} A$.

2. $\emptyset \notin Z$.

3. $\forall A, B \in Z : A \cap B \neq \emptyset \implies A = B$.

Die Elemente von Z heißen auch *Klassen*.

Partitionen und Äquivalenzrelationen

Lemma: Eine Klasseneinteilung Z von M induziert eine Äquivalenzrelation $\sim_Z$ über M durch $a \sim_Z b \iff$ a und b liegen in derselben Z-Klasse.

Lemma: Ist R eine Äquivalenzrelation über M, so ist

$$Z_R = \left\{ \underbrace{\{a \in M \mid aRb\}}_{=:[b]_R} \mid b \in M \right\}$$

eine Zerlegung von M, die so genannte *Quotientenmenge*, oft geschrieben M/R. b heißt auch *Repräsentant* der *Äquivalenzklasse* $[b]_R$.

Genauer gilt: Lemma: Ist R ÄR, so gilt $R = (\sim_{Z_R})$.

Partitionen und Äquivalenzrelationen: Beispiele

Beispiel: Allrelation: $[x]_{M\times M} = M$ für alle $x \in M$.

Beispiel: Diagonale: $[x]_{\Delta_M} = \{x\}$ für alle $x \in M$.

Beispiel: $R_m \subset \mathbb{Z} \times \mathbb{Z}$: Äquivalenzklassen sind $[0]$, $[1]$, $\ldots$, $[m-1]$.

Hinweis: Zwei ganze Zahlen sind äquivalent gdw. sie lassen beim Teilen durch m denselben Rest. Schreibweise: $\mathbb{Z}_m := \mathbb{Z}/R_m$.

Partitionen und Äquivalenzrelationen: $\mathbb{Q}$ als Beispiel

Wir hatten bislang verschiedentlich $\mathbb{N}$ *axiomatisch* eingeführt.
Daraus könnte man $\mathbb{Z}$ einführen als Quotientenmenge auf $\{+,-\} \times \mathbb{N}$ mit der Äquivalenzrelation $(v, n) \sim (v', n')$ gdw. $n = n' \wedge (v = v' \vee n = 0)$.

Über $M = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ definiere: $(a, b) \sim (a', b') \iff ab' = ba'$. Dann ist die Menge der rationalen Zahlen $\mathbb{Q}$ definiert als $\mathbb{Q} = M/\sim$.
Statt $[(a, b)] \in M/\sim$ schreiben wir auch $\frac{a}{b}$.
(a, b) und (a', b') liegen in derselben Äquivalenzklasse gdw. $\frac{a}{b} = \frac{a'}{b'}$ gdw. $ab' = ba'$.

Weiter Sätze und Begriffe

Satz: Sind R und S ÄR über M, so auch $R \cap S$.

Beweis: an der Tafel

Satz: Es seien R und S ÄR über M. $R \circ S$ und $S \circ R$ ist ÄR gdw. $R \circ S$ ist ÄR gdw. es gilt $R \circ S = S \circ R$.

Beweis: an der Tafel

Die *Äquivalenzhülle* von einer binären Relation R heißt auch *von R induzierte Äquivalenzrelation*, geschrieben R^*_E.

Induzierte Äquivalenzrelation—ein Beispiel

Sei $M = \{a, b, c, e, d, f\}$ und
$R = \{(a, b), (c, b), (d, e), (e, f)\}$.
Konstruiere Äquivalenzhülle R_E^* von R.
R_E^* ist symmetrisch $\rightsquigarrow \Delta_M \subseteq R_E^*$.
R_E^* ist reflexiv $\rightsquigarrow R^- \subseteq R_E^*$.
Transitivität liefert vier weitere Paare (welche ?)
Die Äquivalenzklassen von R_E^* sind:
$[a] = \{a, b, c\}$ und $[d] = \{d, e, f\}$.

Graphentheoretische Interpretation: R ist Kantenrelation; die induzierten Äquivalenklassen sind die *schwachen Zusammenhangskomponenten*. (siehe Tafelbild)

Induzierte Äquivalenzrelationen—ein Satz

Satz: Für $R \subseteq M \times M$ gilt:

$$R_E^* = \underbrace{(R \cup R^- \cup \Delta_M)^+}_{=:S} = \underbrace{(R \cup R^-)^+ \cup \Delta_M}_{=:T}.$$

In Worten:

R_E^* ist die reflexive Hülle der transitiven Hülle der symmetrischen Hülle von R.

Graphentheoretische Interpretation: xR_E^*y gdw. es gibt in dem ungerichteten Graphen mit Knotenmenge M und Kantenmenge $R \cup R^-$ einen Weg von x nach y (evtl. der Länge null). $\rightsquigarrow$ Begriff des *schwachen Zusammenhangs*.

Induzierte Äquivalenzrelationen—ein Satz

Satz: Für $R \subseteq M \times M$ gilt:

$$R_E^* = \underbrace{(R \cup R^- \cup \Delta_M)^+}_{=:S} = \underbrace{(R \cup R^-)^+ \cup \Delta_M}_{=:T}.$$

Beweis: Wegen $\Delta_M \cup R^- \subseteq S \cap T$ sind S und T reflexiv und symmetrisch; S und T sind per def. transitiv. $\rightsquigarrow S$ und T sind ÄR, d.h., $R \subseteq R_E^* \subseteq T \subseteq S$.

Angenommen, es gäbe $(x, y) \in S$, $(x, y) \notin R_E^*$.

Wohlordnungsaxiom $\rightsquigarrow$ es gibt minimales n mit der Eigenschaft, dass es irgendwelche $(s, u) \in (R \cup R^- \cup \Delta_M)^n$ gibt mit $(s, u) \notin R_E^*$.

Klar: $n > 1$, denn $R_E^* \supseteq (R \cup R^- \cup \Delta_M) = (R \cup R^- \cup \Delta_M)^1$

$\rightsquigarrow \exists t (s, t) \in (R \cup R^- \cup \Delta_M)^{n-1} \wedge (t, u) \in (R \cup R^- \cup \Delta_M)$

n minimal $\rightsquigarrow (s, t) \in R_E^*$; "klar": $(t, u) \in R_E^*$; also: $(s, u) \in R_E^*$, da R_E^* transitiv.

Hinweis: Alternative: Induktionsbeweis

Quasiordnung

Eine reflexive und transitive Relation R über M heißt auch *Quasiordnung*.

Beispiel: Jede Äquivalenzrelation ist eine Quasiordnung.
Genauer gilt: Eine Quasiordnung ist genau dann eine Äquivalenzrelation, wenn sie symmetrisch ist.

Beispiel: Betrachte über der Menge $\mathbb{C}$ der komplexen Zahlen die Relation $y \prec z \iff |y| \leq |z|$.
Beobachte: $\prec$ ist weder symmetrisch noch antisymmetrisch.

Satz: Ist R eine Relation über M, so ist R^* die kleinste R umfassende Quasiordnung.

Halbordnungen

Eine antisymmetrische Quasiordnung R über M heißt auch *Halbordnung* (auf der gegebenen Grundmenge). Gilt xRy, so heißt x auch *Vorgänger* von y und y *Nachfolger* von x.

Beispiel: $\leq$ oder $\geq$ auf $\mathbb{R}$ sind Halbordnungen.

Beispiel: $\prec$ auf $\mathbb{C}$ ist keine Halbordnung.

Beispiel: Die Teilerrelation ist eine Halbordnung auf $\mathbb{N}$, aber nicht auf $\mathbb{Z}$.

Beispiel: Auf der Potenzmenge von M ist $\subseteq$ oder auch $\supseteq$ eine Halbordnung.

Lineare Ordnungen

Eine Halbordnung $\leq$ auf M heißt *linear* (*total*) gdw. $\forall x, y \in M(x \leq y \vee y \leq x)$.

Zwei Elemente $x, y \in M$ heißen *vergleichbar* gdw. $(x \leq y \vee y \leq x)$; andernfalls heißen sie *unvergleichbar*. Die HO $\leq$ ist also linear gdw. alle Elemente von M untereinander paarweise vergleichbar sind.

Satz: Ist Vergleichbarkeit transitiv, so ist sie eine Äquivalenzrelation.
Dann gilt: Eine HO ist linear gdw. die von ihr induzierte Vergleichbarkeitsrelation hat nur eine Äquivalenzklasse.

Beispiel: Lexikalische Ordnung in einem Wörterbuch

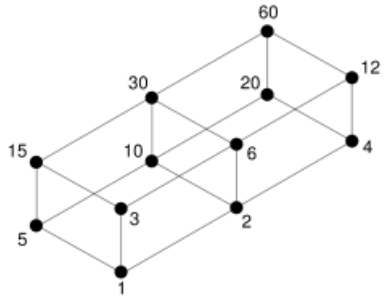
Lineare Ordnungen sind eminent wichtig für unser Leben (als Informatiker)

Bezeichnungen für “Computer”: ordinateur / ordenador

“Ordnen” (Sortieren) ist die “Rechnertätigkeit”, die am meisten Rechenzeit weltweit benötigt.

Für manche “gutartige” Sortierverfahren ist es entscheidend für ihre Laufzeit, wie “wenig linear” die Eingangsreihenfolge ist.

Halbordungsrelationen: ein Beispiel zum Hasse-Diagramm



Bei diesem *Hasse-Diagramm* werden “passende” unvergleichbare Elemente auf einer Ebene dargestellt.

Überführung in “normale” Graphendarstellung einer Relation durch:

(a) Einfügen von Pfeilspitzen (nach oben),
(b) Einfügen von Schlingen (Reflexivität),
(c) Einfügen weiterer Bögen (Transitivität)

echte und unmittelbare Nachfolger / Hasse-Diagramme

Es sei $\leq$ eine Halbordnung auf M. $z \in M$ heißt *unmittelbarer Nachfolger* von $x \in M$, falls (1) $x \leq z$, (2) $x \neq z$ und (3) falls aus $x \leq y \leq z$ $y = x$ oder $y = z$ folgt. Gelten nur (1) und (2), so heißt z *echter Nachfolger* von x, i.Z. $x < z$.

Hinweis: Im Hasse-Diagramm werden genau die Kanten dargestellt, die zur Relation "unmittelbarer Nachfolger" gehören.

Hinweis: Entsprechend definierbar: *echter Vorgänger*, *unmittelbarer Vorgänger*

Satz: Ist R die zu der Halbordnung $\leq$ auf M gehörige Relation des echten Nachfolgers, so ist $\leq$ gerade die reflexive Hülle von R.

Satz: Ist R die zu der Halbordnung $\leq$ auf M gehörige Relation des unmittelbaren Nachfolgers und ist M endlich, so ist $\leq$ gerade die reflexive transitive Hülle von R.

Beispiel: Teilmengenhalbordnung von $\{a, b, c\}$.

Restriktionen

Ist R eine Relation über M und ist $\mathrm{N} \subseteq \mathrm{M}$, so heißt $\leq_{\mathrm{N}} := (\leq \cap \mathrm{N} \times \mathrm{N})$ *Restriktion* von R auf N.

Satz: Mit $\leq$ ist auch $\leq_{\mathrm{N}}$ Quasiordnung bzw. Halbordnung bzw. lineare Ordnung.

Daher steckt ein Prinzip: Über Allaussagen definierte Eigenschaften übertragen sich durch Restriktion.

In einer Halbordnung $(\mathrm{M}, \leq)$ heißt $\mathrm{K} \subseteq \mathrm{M}$ *Kette* gdw. die Restriktion von $\leq$ auf K eine lineare Ordnung ist.
Eine Kette K heißt *maximal*, wenn es keine K umfassende Kette gibt.

Maximalkettenprinzip von Hausdorff / Birkhoff:
In jeder halbgeordneten Menge gibt es maximale Ketten.

klein und groß...

Es sei $(M, \leq)$ eine Halbordnung und $\emptyset \neq N \subseteq M$.
$x \in N$ heißt *größtes Element* von N, wenn $\forall y \in N : y \leq x$.
$x \in N$ heißt *kleinstes Element* von N, wenn $\forall y \in N : x \leq y$.
$x \in N$ heißt *maximales Element* in N, wenn $\forall y \in N : x \leq y \implies y = x$.
$x \in N$ heißt *minimales Element* in N, wenn $\forall y \in N : y \leq x \implies y = x$.
$x \in M$ heißt *obere Schranke* von N, wenn $\forall y \in N : y \leq x$.
$x \in M$ heißt *untere Schranke* von N, wenn $\forall y \in N : x \leq y$.
Eine kleinste obere Schranke heißt auch *obere Grenze* oder *Supremum*.
Eine größte untere Schranke heißt auch *untere Grenze* oder *Infimum*.

Satz: Eine Menge N besitzt ein größtes Element
gdw. eine obere Grenze liegt in N
gdw. eine obere Schranke liegt in N.
Größte Elemente und obere Schranken einer Menge sind eindeutig bestimmt.

Beispiel: Teilmengenhalbordnung von $\{a, b, c\}$.
Beispiel: $0 \prec 2 \prec 4 \prec \cdots \prec 1 \prec 3 \prec 5 \prec \cdots$ auf $\mathbb{N}$.

oh wie wohl. . . ein mathematisch-informatischer Blick hinaus

Eine *Wohlordnung* auf einer Menge M ist eine totale Ordnung mit der Eigenschaft, dass jede nichtleere Teilmenge von M ein bzgl. dieser Ordnung kleinstes Element hat. Die Menge M zusammen mit der Wohlordnung heißt eine wohlgeordnete Menge.

Beispiel: Die $(\mathbb{N}, \leq)$ ist eine Wohlordnung, aber weder die gewöhnliche Anordnung der ganzen Zahlen noch die der positiven reellen Zahlen ist eine Wohlordnung.

Für die Algorithmik wichtig: noch allgemeinerer Begriff der *Wohlquasiordnung*.

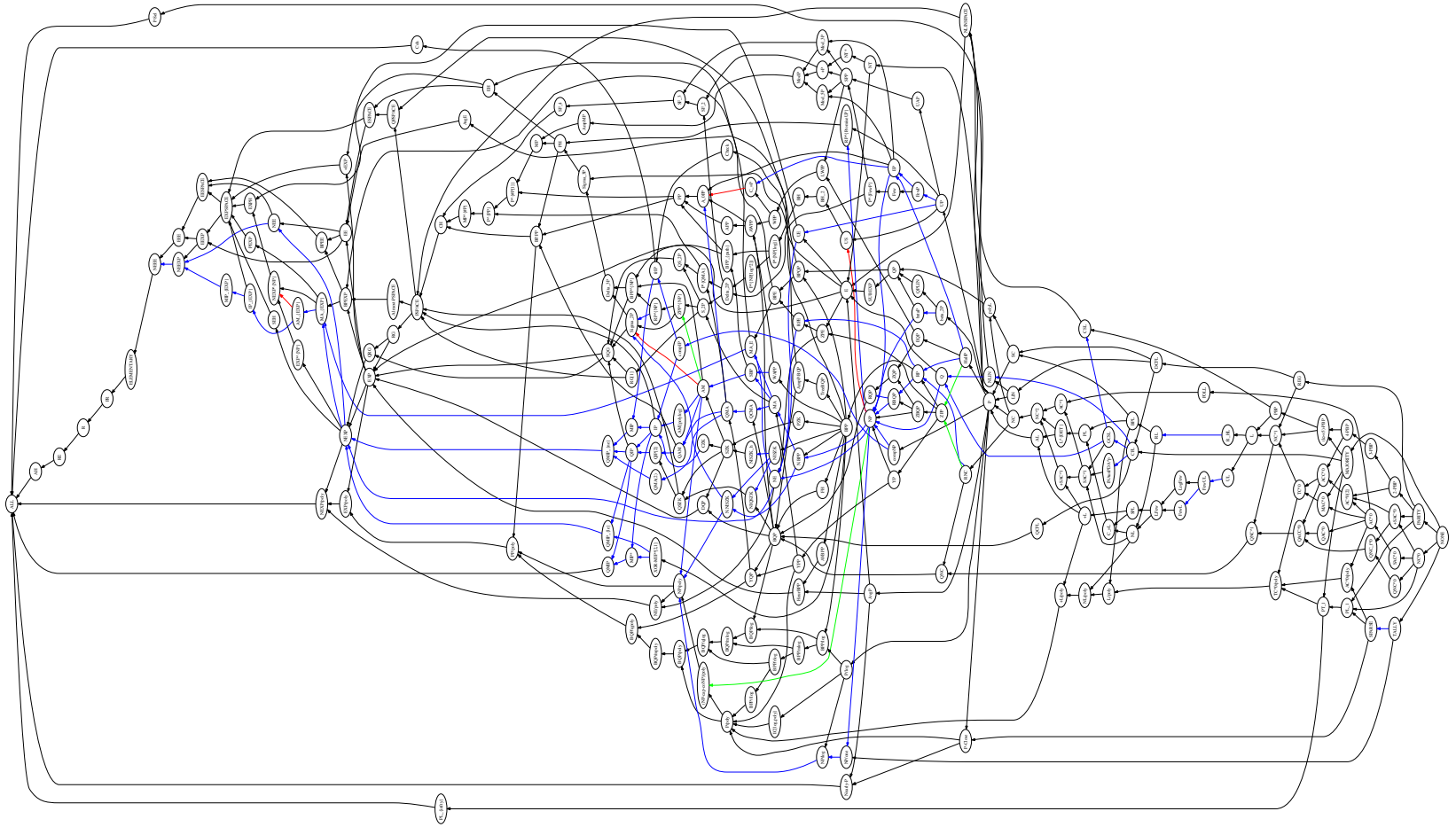
Wohlordnungssatz / Wohlordnungsprinzip: Jede Menge kann wohlgeordnet werden.
Hinweis: Äquivalent zum Maximalkettenprinzip und zum Auswahlaxiom.

Transfinite Induktion verallgemeinert die uns bekannte Induktion auf beliebige wohlgeordnete Mengen: Sei $(M, \leq)$ eine Wohlordnung und 0 bezeichne das kleinstes Element. Will man beweisen, dass die Eigenschaft P für alle Elemente von M zutrifft, dann beweist man bei transfiniter Induktion folgendes:
– $P(0)$ ist wahr.
– Wenn $0 \leq a$, $a \neq 0$ und $P(b)$ ist wahr ist für alle $b \leq a$, $b \neq a$, dann ist auch $P(a)$ wahr.

Wohlordnungsprinzip $\rightsquigarrow$ Induktion ist potentiell immer anwendbar.

Definitionen mit transfiniter Rekursion erstmals von J. von Neumann (1928).

Ein informatisches Inklusionsdiagramm: Der Komplexitätszoo



Funktionen

Eine *partielle Funktion* F ist eine nacheindeutige binäre Relation zwischen A und B.
Eine partielle Funktion F heißt *total* oder einfach *Funktion* oder *Abbildung* gdw. F ist linkstotal.

Schreibweise: $f : A \to B, a \mapsto f(a)$
$f(a)$ *Bild* von a bei f; a *Urbild*;
A: *Definitionsbereich*,
B: *Wertebereich*
$f^{-}(B) = \{a \in A \mid \exists b \in B : f(a) = b\}$ *Urbildbereich*
$f(A) = \{b \in B \mid \exists a \in A : f(a) = b\}$ *Bildbereich*
Satz: Eine Funktion ist total gdw. ihr Definitions- und Urbildbereich stimmen überein.

Funktionen: Beispiele

Beispiel: Die Diagonale ist eine totale Funktion.
Beispiel: Die Vorschrift, die jedem Studenten der Universität Trier seine DSL-Note zuordnet, ist eine partielle Funktion.
Beispiel: Die Relation, die sämtlichen Elementen aus A stets dasselbe Element aus B zuordnet, ist eine totale Funktion, genannt *konstante Funktion*.
Beispiel: Ist $\mathrm{A} \subseteq \mathrm{B}$, so kann man die Diagonale Δ_{A} auch als Abbildung $\iota : \mathrm{A} \to \mathrm{B}$ auffassen: diese heißt auch *natürliche Einbettung*. Für $\mathrm{A} = \emptyset$ spricht man von der *leeren Abbildung*.

Funktionen und Äquivalenzrelationen

Satz: Es sei $f : A \to B$ eine Funktion. Dann definiert $x \sim_f y$ gdw. $f(x) = f(y)$ eine Äquivalenzrelation auf A.

Satz: Es sei $\sim$ eine Äquivalenzrelation auf A. Es bezeichne $[a]$ die $\sim$-Äquivalenzklasse von A. $f_\sim : A \to A/\sim$, $a \mapsto [a]$ ist eine Abbildung.

Satz: Mit den Bezeichnungen der voranstehenden Sätze gilt:

$$\sim = \sim_{f_\sim} \quad \text{und} \quad f = f_{\sim_f}$$

Beispiele and der Tafel.

Funktionen und Verknüpfungen

Eine (n-stellige) *Verknüpfung* oder *Operation* auf einer Grundmenge M ist eine Funktion $f : M^n \to M$.

Erinnerung: M^n bezeichnet das $(n-1)$-fache kartesische Produkt von M mit sich selbst.

Speziell: zweistellige Verknüpfungen schreibt man meist in Infixnotation.

Beispiel: Auf der Menge $B = \{w, f\}$ sind die Junktoren $\vee$, $\wedge$ zweistellige Verknüpfungen.

Einstellige Verknüpfungen sind "normale" Abbildungen $M \to M$.
Nullstellige Verknüpfungen bezeichnen Konstanten in M.

Mengenfunktionen

Es sei $R \subseteq A \times B$ eine Relation (z.B. auch eine (partielle) Funktion).

Diese kann man auch als Mengenfunktionen deuten:

$R_1 : 2^A \to 2^B,\ X \mapsto \{y \in B \mid \exists x \in X (x, y) \in R\}$
$R_2 : 2^B \to 2^A,\ Y \mapsto \{x \in A \mid \exists y \in Y (x, y) \in R\}$

Satz: $R_1(A_1 \cup A_2) = R_1(A_1) \cup R_1(A_2)$. (entsprechend für R_2)
Satz: $R_1(A_1 \cap A_2) \subseteq R_1(A_1) \cap R_1(A_2)$. (entsprechend für R_2)

Ist R durch eine Funktion $f : A \to B$ gegeben, schreibt man auch $f(X)$ statt $R_1(X)$, und $f^-(Y)$ statt $R_2(Y)$.
Satz: $f^-(B_1 \cap B_2) = f^-(B_1) \cap f^-(B_2)$.

Komposition von Funktionen

Satz: Sind R und S nacheindeutige Relationen über M, so auch $R \circ S$.

Satz: Sind R und S vortotale Relationen über M, so auch $R \circ S$.

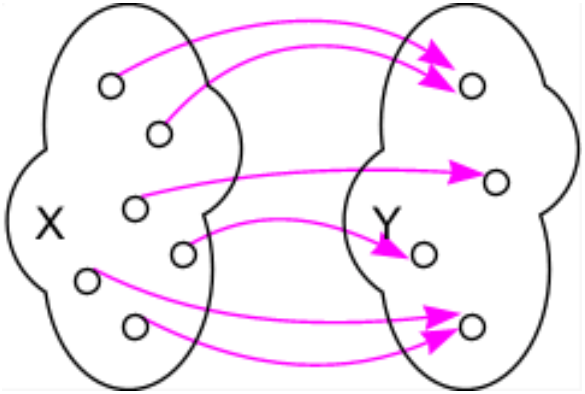
Das Relationenprodukt wird im Falle (partieller) Funktionen auch oft als *Komposition* oder *Hintereinanderausführung* angesprochen.

Vom Relationenprodukt erben wir die folgende Eigenschaft:
Satz: Die Komposition von (partiellen) Funktionen ist assoziativ.
ACHTUNG: Uneinheitliche Reihenfolge bei Komposition von Funktionen in der Literatur; gemäß unserer Festlegung gilt: $(f \circ g)(x) = g(f(x))$.

Funktionen: Eigenschaften I

Eine Funktion $f : X \to Y$ heißt *surjektiv* oder eine Abbildung von X *auf* Y gdw. ihr Bild- und Wertebereich übereinstimmen, d.h., wenn sie nachtotal ist.

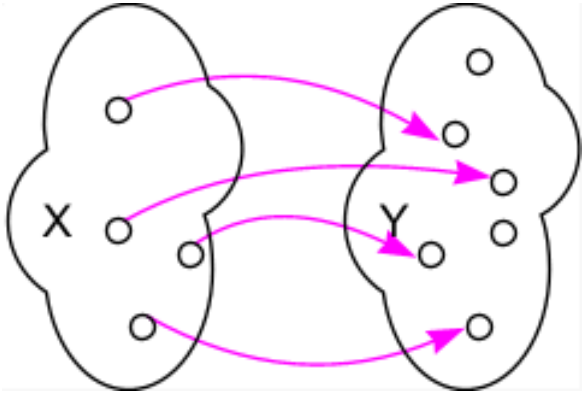
Im Bild:



Funktionen: Eigenschaften II

Eine Funktion $f : X \to Y$ heißt *injektiv* oder *eineindeutig* wenn die zugehörige Relation voreindeutig ist.

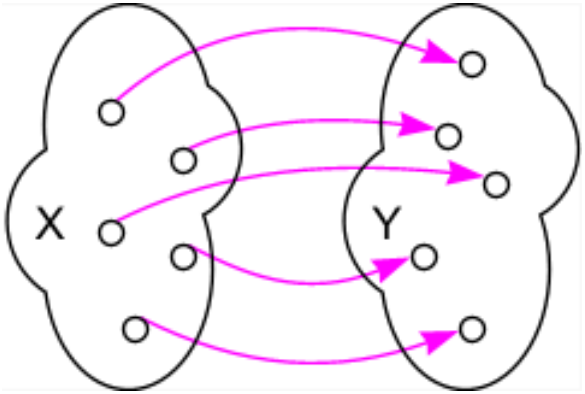
Im Bild:



Funktionen: Eigenschaften III

Eine Funktion $f : X \to Y$ heißt *bijektiv*, wenn die zugehörige Relation voreindeutig und rechtstotal ist.

Im Bild:



Bijektive Funktionen

Satz: Es sei $f : A \to B$ eine Funktion.
Die folgenden Aussagen sind logisch äquivalent:
(1) f ist bijektiv.
(2) $\forall b \in B : f^{-}(\{b\})$ enthält genau ein Element.
(3) $\exists g : B \to A : g \circ f = \Delta_B$ und $f \circ g = \Delta_A$.

Die in (3) beschriebene Inverse heißt auch *Umkehrabbildung*, geschrieben f^{-1}.
Mit f ist auch f^{-1} bijektiv, und es gilt: $(f^{-1})^{-1} = f$.

Funktionen—Weitere Aussagen

Satz: (1) Die Komposition von surjektiven Funktionen ist surjektiv.
(2) Die Komposition von injektiven Funktionen ist injektiv.
(3) Die Komposition von bijektiven Funktionen ist bijektiv.

Satz: Ist A endlich und $f : A \to A$, so sind gleichwertig:
(1) f ist surjektiv, (2) f ist injektiv, (3) f ist bijektiv.

Satz: Ist A endlich und $f : A \to A$, so sind gleichwertig:
(1) f ist surjektiv, (2) f ist injektiv, (3) f ist bijektiv.

Beweis: Wir (nur) zeigen die Aussage:
$\forall n$: Ist A Menge mit n Elementen und $f : A \to A$ surjektiv, so ist A injektiv.
Induktionsargument: IA: Für $n = 0, 1$ sind die Aussagen offenbar richtig.
IV: Die Aussage gilt für alle Mengen mit weniger als n Elementen.
Betrachte Menge A mit $n > 1$ Elementen und Surjektion $f : A \to A$.
Widerspruchsbeweis: Wäre f nicht injektiv, so gäbe es $a, b \in A$, $a \neq b$ mit $f(a) = f(b)$.
Da f surjektiv, gibt es c mit $f(c) = a$.
Gilt $c \neq a$, so wäre f' mit (1) $f'(x) = f(x)$ ausgenommen
(2) $f'(a) = a$ sowie $f'(c) = f(b)$ und (3) $f'(y) = y$ für $y \neq c$ mit $f(y) = a$
ebenfalls eine Surjektion, die nicht injektiv ist.
(Falls $c = a$, so vertausche die Rollen von a und b.)
Es gibt also ein solches Beispiel mit $f'(z) = a$ gdw. $z = a$.
Betrachte die wohldefinierte Einschränkung von f' auf $A \setminus \{a\}$.
Nach Konstruktion ist f' eine Surjektion, die nach IV Injektion ist.
Damit wäre dann aber auch f' auf A eine Injektion. Widerspruch
Nach dem Prinzip der mathematischen Induktion ist die Behauptung richtig.