Diskrete Strukturen und Logik

WiSe 2007/08 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

$\boxed{\textbf{Diskrete Strukturen und Logik}}$ Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- Kombinatorik: Die Kunst des Zählens
- algebraische Strukturen

Spezielle Relationen

- Äquivalenzrelationen
- Halbordnungen
- Funktionen

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 $A \subseteq B$, so kann man die Diagonale Δ_A auch als Abbildung $\iota : A \to B$ auffassen: diese heißt auch *natürliche Einbettung*. Für $A = \emptyset$ 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 $R \circ S$.

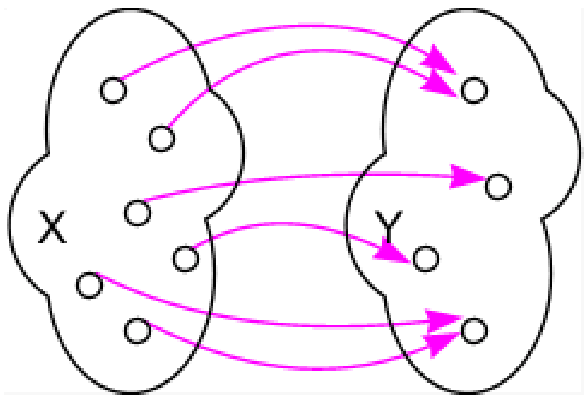
Das Relationenprodukt wird im Falle (partieller) Funktionen auch oft als *Komposition* oder *Hintereinanderausführung* angesprochen.

Vom Relationenprodukt erben wir die folgende Eigenschaft:
Satz: Die Komposition von (partiellen) Funktionen ist assoziativ.
ACHTUNG: Veränderte Reihenfolge bei Komposition von Funktionen gegenüber Meinel/Mundhenk, d.h.: $(f \circ g)(x) = g(f(x))$.

Funktionen: Eigenschaften I

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

Im Bild:



Surjektive Funktionen

Satz: Es sei $f : A \longrightarrow B$ eine Funktion.
Die folgenden Aussagen sind logisch äquivalent:
(1) f ist surjektiv.
(2) $\forall b \in B : f^{-}(\{b\}) \neq \emptyset$.
(3) $\exists g : B \longrightarrow A : g \circ f = \Delta_B$.
(4) Es sei C eine weitere Menge und $r, s : B \longrightarrow C$ beliebige Funktionen, so gilt die folgende Kürzungsregel: $f \circ r = f \circ s \Rightarrow r = s$.

Surjektive Funktionen—Anmerkungen zum Beweis:

Beweisstrategie: Statt (1) $\iff$ (2), (1) $\iff$ (3) und (1) $\iff$ (4) beweisen wir im *Ringschluss*:
(1) $\Longrightarrow$ (2), (2) $\Longrightarrow$ (3), (3) $\Longrightarrow$ (4), (4) $\Longrightarrow$ (1).
Die “fehlenden” Implikationen liefert die “Transitivität” der Implikation.

Bei der Implikation (2) $\Longrightarrow$ (3) machen wir Gebrauch vom *Auswahlaxiom von Zermelo*: Zu jeder Menge $\mathcal{M}$ von nichtleeren Mengen eines Universums U gibt es eine Abbildung $f : \mathcal{M} \to \mathrm{U}$ mit $f(A) \in A$.
Das Auswahlaxiom ist zum Maximalkettenprinzip äquivalent.

Einzelheiten zum Beweis

(1) $\Rightarrow$ (2): f surj. $\rightsquigarrow f(A) = B$, d.h., für $b \in B$ gibt es ein $a \in A$ mit $f(a) = b$, also $f^{-}(\{b\}) \neq \emptyset$.
(2) $\Rightarrow$ (3): Mit dem Auswahlaxiom können wir uns wegen $f^{-}(\{b\}) \neq \emptyset$ zu jedem $b \in B$ ein $g(b) \in f^{-}(\{b\})$ auswählen; es gilt nach Def.: $f(g(b)) = b$.
Damit gilt: $(g \circ f)(b) = f(g(b)) = b$ für alle $b \in B$.
(3) $\Rightarrow$ (4): Betrachte zwei bel. Abb. $r, s : B \to C$ mit $f \circ r = f \circ s$.
Wegen (3) gibt es $g : B \to A : g \circ f = \Delta_B$. Mit der Assoziativität der Komposition folgt:

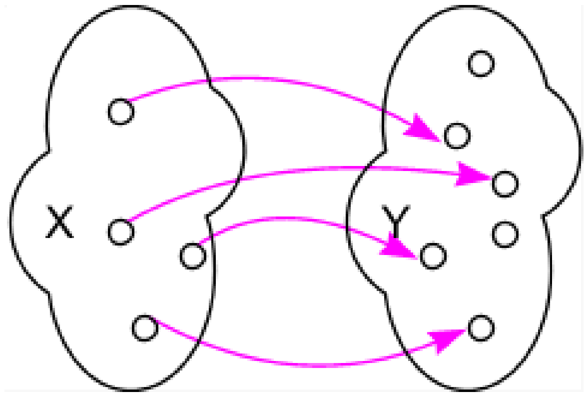
$$r = \Delta_B \circ r = (g \circ f) \circ r = g \circ (f \circ r) = g \circ (f \circ s) = (g \circ f) \circ s = \Delta_B \circ s = s.$$

(4) $\Rightarrow$ (1) mit Kontraposition: Annahme, f ist nicht surjektiv, d.h., es gibt ein $b_0 \in B \setminus f(A)$.
Für $C = \{0, 1\}$ betrachte Abbildungen $r, s : B \to \{0, 1\}$ mit $r(b) = s(b) = 0$ für alle $b \neq b_0$ und $r(b_0) = 0$ und $s(b_0) = 1$.
Offenbar gilt $r \neq s$, aber sehr wohl $f \circ r = f \circ s$, da der Unterschied außerhalb von $f(A)$ auftritt.

Funktionen: Eigenschaften II

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

Im Bild:



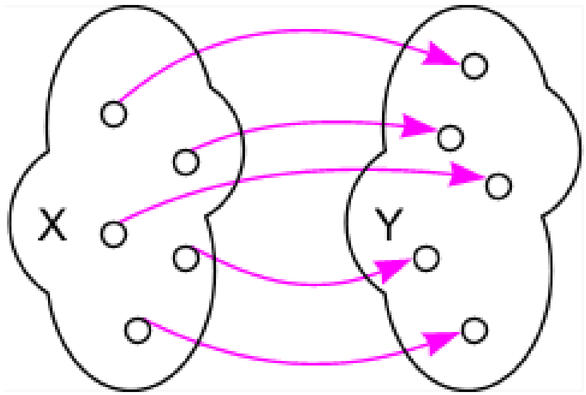
Injektive Funktionen

Satz: Es sei $f : A \to B$ eine Funktion.
Die folgenden Aussagen sind logisch äquivalent:
(1) f ist injektiv.
(2) $\forall b \in B : f^{-}(\{b\})$ enthält höchstens ein Element.
(3) $\exists g : B \to A : f \circ g = \Delta_A$.
(4) Es sei C eine weitere Menge und $r, s : C \to A$ beliebige Funktionen, so gilt die folgende Kürzungsregel: $r \circ f = s \circ f \Rightarrow r = s$.
Beweis ähnlich zur Surjektivität.

Funktionen: Eigenschaften III

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

Im Bild:



Bijektive Funktionen

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

Bijektive 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.

<u>Beweis:</u> Wir (nur) zeigen die Aussage:

$\forall n$: Ist A Menge mit n Elementen und $f : A \to A$ surjektiv, so ist A injektiv.

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 $f : A \to A$.

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) $f'(x) = f(x)$ <u>ausgenommen</u> (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. $z = a$.

Nach IV ist die wohldefinierte Einschränkung von f' auf $A \setminus \{a\}$ eine Surjektion, die ebenfalls Injektion ist. Damit wäre dann aber auch f' auf A eine Injektion.