Formale Grundlagen

Franz Binder

Institut für Algebra
Johannes Kepler Universität Linz

Vorlesung im 2009S

http://www.algebra.uni-linz.ac.at/Students/Win/fg

Inhalt

Grundbegriffe

Relationenprodukt

Äquivalenzrelationen

Ordnungsrelationen

Funktionale Relationen

Relationenalgebra

Wohlfundierte Relationen

Prädikate

Definition

Sei $n\colon \mathbb{N}$, und $X_1, \ldots, X_n$ Datentypen. Dann heißt jede Konstruktion P vom Typ

$$P\colon X_1 \to \cdots \to X_n \to \mathbb{P}$$

ein n-stelliges Prädikat.

Example

Die Eigenschaft, eine Primzahl zu sein, ist ein 1-stelliges Prädikat vom Typ $\mathbb{N} \to \mathbb{P}$. Dabei wird z.B. der Zahl 3 die Aussage „3 ist eine Primzahl" zugeordnet, während der Zahl 4 die Eigenschaft „4 ist eine Primzahl" zugeordnet wird. Eng assoziert mit diesem Prädikat ist die Teilmenge aller natürlichen Zahlen, welche diese Eigenschaft haben (d.h. welchen eine wahre Aussage zugeordnet wird), also die Menge aller Primzahlen.

3-stelliges Prädikat

Example

Sei L die Menge aller Lehrveranstaltungen (einer Universität), M die Menge aller Studenten, und S die Menge aller Semester.
3-stelliges Prädikat vom Typ $L \to M \to S \to \mathbb{P}$:
„Der Student m nimmt im Semester s and der Lehrveranstaltung l teil“ zuordnet.

Lehrveranstaltung	Student	Semester
Mathematik und Logik	Eike Eifrig	2008W
Mathematik und Logik	Fausto Faul	2008W
Formale Grundlagen	Eike Eifrig	2009S
Mathematik und Logik	Fausto Faul	2009W
Mathematik und Logik	Fabian Famos	2009W
Formale Grundlagen	Fabian Famos	2009S
Datenmodellierung	Eike Eifrig	2008S

Relationen

Definition

Eine Konstruktion vom Typ $A \to B \to \mathbb{P}$ heißt Relation von A nach B.
Eine Konstruktion vom Typ $A \to A \to \mathbb{P}$ heißt Relation in A.

Notation

Ist R eine Relation, so schreiben wir statt $R(a)(b)$ oder $R(a, b)$ zumeist $a\ R\ b$, oder auch $(a, b) \in R$, oder $a \in Rb$, oder $b \in aR$.

Bemerkung

Die Bezeichnungsweise ist hier nicht ganz einheitlich. So werden z.B. gerade im Zusammenhang mit relationalen Datenbanken auch Prädikate beliebiger Stelligkeit als Relationen bezeichnet. Die 2-stelligen Relationen heißen dann zur Unterscheidung binäre Relationen.

Relationen: Beispiele

Example

Gleichheitsrelation: Je zwei Elementen $x, y \colon X$ einer Menge X wird die Aussage zugeordnet, daß diese beiden gleich sind, d.h. die Aussage $x = y$.

Example

Für jede der Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ wird eine natürliche Ordnung definiert durch die Relation, welche je zwei Elementen x, y die Aussage $x \leq y$ zuordnet.

Example

Für $\mathbb{Z}$ kennen wir auch die Teilbarkeitsrelation, welche zwei Elementen x, y die Aussage $\exists_{z \colon \mathbb{Z}} y = x \cdot z$ (abgekürzt: $x \mid y$) zuordnet.

Example

Eine weitere bekannte Relation in $\mathbb{Z}$ ordnet zwei Elementen $x, y \colon \mathbb{Z}$ die Aussage „x und y sind teilerfremd“ zu.

Example

Auch die Kongruenz modulo m ($\equiv_m$) ist für jedes $m \colon \mathbb{N}$ eine wichtige Relation in $\mathbb{Z}$.

Relationen: Weitere Beispiele

Example

Eine wohlbekannte Relation in der Potenzmenge einer jeden Menge ist die Teilmengen-Relation.

Example

Die Enthaltensein-Relation ordnet einem Element $x\colon X$ einer Menge X und einer Teilmenge $A\colon \mathbb{P}X$ die Aussage „x ist Element von A“ (kurz $x \in A$) zu. Sie hat also den Typ $X \to \mathbb{P}X \to \mathbb{P}$.

Bemerkung

Ist R eine (binäre) Relation, so schreibt man statt Rxy meist $x\,R\,y$ oder $x \xrightarrow{R} y$; oder einfach $x \to y$, falls R aus dem Zusammenhang ersichtlich ist. Man sagt dann auch, x und y sind in Relation. Oft werden auch diverse spezielle Symbole verwendet (z.B.: $<$, $\leq$, $\subseteq$, $\in$, $\equiv$, $\ldots$).

Tabelle

Example

Sei A die Relation, welche einem Mitarbeiter x und einer Abteilung A die Aussage „x arbeitet für die Abteilung A“ zuordnet.

Mitarbeiter	Abteilung
Gun	Al
Peter	St
Waltraud	St
Waltraud	Al
Mark	Al
Mark	St
Erich	Fz
Mark	Fz
Chris	FH
Chris	Al
Josef	St

x delegiert Arbeit an y

Als Tabelle geschrieben könnte dies etwas so aussehen:

Chef	Arbeiter
Gun	Chris
Gun	Waltraud
Chris	Mark
Waltraud	Erich
Erich	Mark
Peter	Waltraud
Peter	Mark
Peter	Josef
Josef	Waltraud
Josef	Mark

Darstellungsmöglichkeiten

- Formel;
- Tabelle;
- Graph;
- Geometrischen Kurven oder Flächen;
- Gitterpunkte.

Relationenprodukt

Definition

Gegeben seien die Relationen $R\colon X \to Y \to \mathbb{P}$ und $S\colon Y \to Z \to \mathbb{P}$. Dann wird das Relationenprodukt $(R;S)$ definiert durch

$$x \overset{R;S}{\to} z \iff \exists_{y\,:\,Y}\, x \overset{R}{\to} y \wedge y \overset{S}{\to} z.$$

Bemerkung

Vorsicht! Statt der Notation $R;S$ sind auch $R \circ S$ und $S \circ R$ sowie RS und SR gebräuchlich. Hier ist besondere Vorsicht geboten, zumal das Relationenprodukt nicht kommutativ ist.

Satz

Das Relationenprodukt ist assoziativ.

Beweis.

Übung. $\square$

Example

Seien etwa A und D die Relationen von vorhin.
Dann bedeuted die Aussage $m \stackrel{D;A}{\to} a$, daß der Mitarbeiter m an zumindest einen Mitarbeiter der Abteilung a Arbeit delegiert.

Diagonale

Definition

In jeder Menge X definiert die Gleichheit eine als Diagonale Δ_X bezeichnete Relation, durch

$$x \; \Delta_X \; y \iff x = y.$$

Satz

Für jede Relation $R\colon X \to Y$ gilt

$$R; \Delta_Y = R = \Delta_X; R.$$

Inverse Relation

Definition

Zu jeder Relation R von X nach Y definiert man die zu R inverse Relation durch

$$x \overset{R^{-1}}{\to} y \iff y \overset{R}{\to} x.$$

Example

Die zur Kleiner-Relation inverse Relation ist die Größer-Relation (d.h. $<^{-1} = >$), denn $x < y$ gilt genau dann wenn $y > x$.
Ähnliches gilt z.B. für die Teilmengenbeziehung. Gleichheitsrelation und die Kongruenz modulo m sind zu sich selbst invers.
Für die inverse Relation eines Graphen: alle Pfeile umdrehen.
Tabelle der inversen Relation: Spalten vertauschen.
Geometrische Darstellung der inversen Relation in der x-y-Ebene: Koordinaten vertauschen, d.h. die geometrische Figur wird an der Hauptdiagonalen gespiegelt.

Relationen als Monoid

Satz

Die Menge der Relationen in einer Menge X, d.h. die Menge $X \to X \to \mathbb{P}$, bildet zusammen mit dem Relationenprodukt und der Diagonale Δ_X als neutralem Element ein Monoid.

Bemerkung

Es ergibt sich jedoch keine Gruppe, weil im allgemeinen $R; R^{-1} = \Delta_X$ nicht gilt.

Definition

Notation mit Potenzen:

$$\begin{aligned}
R^1 &= R \\
R^2 &= R; R \\
R^{n+1} &= R^n; R = R; R^n \\
R^0 &= \Delta_X \\
R^{-n} &= (R^{-1})^n
\end{aligned}$$

Rechnen mit Potenzen

Satz

Sei R eine Relation von X nach Y. Es gelten für alle $n, m\colon \mathbb{N}$:

$$R^n; R^m = R^{n+m} = R^m; R^n,$$
$$(R^n)^m = R^{n \cdot m} = (R^m)^n.$$

Und für Relationen R, S in X gilt

$$(R; S)^{-1} = S^{-1}; R^{-1}$$

Die Relationen R, S sind genau dann vertauschbar (d.h. $R; S = S; R$) wenn für alle $n\colon \mathbb{Z}$ gilt

$$(R; S)^n = R^n; S^n,$$

Äquivalenzrelationen

Definition

Sei X ein Datentyp. Dann heißt eine Relation R in X

reflexiv	falls	$\forall_{x\colon X}\, x \overset{R}{\to} x;$
symmetrisch	falls	$\forall_{x,y\colon X}\big(x \overset{R}{\to} y \iff y \overset{R}{\to} x\big);$
transitiv	falls	$\forall_{x,y,z\colon X}\big(x \overset{R}{\to} y \wedge y \overset{R}{\to} z \implies x \overset{R}{\to} z\big).$

Sie heißt eine Äquivalenzrelation, wenn sie reflexiv, symmetrisch und transitiv ist.

Bemerkung

Für Äquivalenzrelationen verwendet man gerne Symbole wie $=, \equiv, \cong, \sim, \simeq, \triangleq, \doteq$.

Bemerkung

Auf jeder Menge ist die Diagonale Δ_X *eine Äquivalenzrelationen.*

Äquivalenzrelation via Funktion

Satz

Ist $\equiv$ *eine Äquivalenzrelation in* Y *und* $f\colon X \to Y$, *dann wird durch*

$$x \equiv_f y \iff f(x) \equiv f(y)$$

eine Äquivalenzrelation in X *definiert.*

Hüllen

Satz

Eine Relation R in einer Menge X ist

$$\begin{aligned} \textit{reflexiv} &\iff R \supseteq R^0; \\ \textit{symmetrisch} &\iff R = R^{-1}; \\ \textit{transitiv} &\iff R \supseteq R^2. \end{aligned}$$

Definition

Unter der reflexiven, symmetrischen oder transitiven Hülle einer Relation R in X versteht man die kleinste R umfassende Relation in X, welche die entsprechende Eigenschaft hat.

Satz

Sei R eine Relation in einer Menge X. Dann gelten

$$\begin{aligned} \textit{reflexive Hülle von } R &= R^0 \cup R; \\ \textit{symmetrische Hülle von } R &= R \cup R^{-1}; \\ \textit{transitive Hülle von } R &= \bigcup_{k=1}^{n} R^k =: R^+ \end{aligned}$$

Ordnungsrelationen

Definition

Eine Relation in X heißt Quasi-Ordung falls sie reflexiv und transitiv ist.

Satz

Sei $\sqsubseteq$ eine Quasiordnung in X. Dann wird durch

$$x \equiv y \iff x \sqsubseteq y \wedge y \sqsubseteq x$$

eine Äquivalenzrelation definiert.

Definition

Eine Relation R in einer Menge X heißt antisymmetrisch falls

$$\forall_{x,y\colon X}\big(x \stackrel{R}{\to} y \wedge y \stackrel{R}{\to} x \implies x = y\big).$$

Eine antisymmetrische Quasiordnung heißt partielle Ordnung oder einfach Ordnung.

Satz

Jede Quasiordnung $\sqsubseteq$ in X kann als Ordnung in $X/_{\equiv}$ aufgefaßt werden.

Lineare Ordnung

Definition

Ein Ordnung $\sqsubseteq$ in X heißt linear falls

$$\forall_{x,y\colon X} x \sqsubseteq y \vee y \sqsubseteq x.$$

Im allgemeinen gibt es zu einer partiellen Ordnung mehrere lineare Ordnungen, welche sie umfassen. Das Problem, zu einer partiellen Ordung $\sqsubseteq$ irgendeine diese umfassende lineare Ordnung $\leq$ mit $(\sqsubseteq) \subseteq (\leq)$ zu finden, heißt topologisches Sortieren.

Funktionale Relationen

Definition

Eine Relation p von X nach Y heißt deterministisch, wohldefiniert, funktional oder eine partielle Funktion falls gilt

$$\forall_{x\colon X}\forall_{y,z\colon Y}\bigl(x \xrightarrow{p} y \wedge x \xrightarrow{p} z \implies y = z\bigr).$$

Sie heißt terminierend oder total, falls gilt

$$\forall_{x\colon X}\exists_{y\colon Y}\, x \xrightarrow{p} y.$$

Erfüllt sie beide Eigenschaften, so nennt man sie eine (totale) Funktion.

Injektiv und Surjektiv

Definition

Eine Funktion $f\colon X \to Y$ heißt injektiv falls

$$\forall_{x,y\colon X} f(x) = f(y) \implies x = y;$$

sie heißt surjektiv falls

$$\forall_{y\colon Y} \exists_{x\colon X} fx = y;$$

und bijektiv falls sie injektiv und surjektiv ist.

Bemerkung

Diese Eigenschaften sind dual zu den definierenden Eigenschaften für Funktionen. Die Injektivität bedeutet gerade, daß auch f^{-1} deterministisch ist, die Surjektivität bedeutet daß f^{-1} terminiert, und die Bijektivität, daß auch f^{-1} wieder eine Funktion ist. Insbesondere gilt für bijektive Funktionen

$$f^{-1} \circ f = \mathrm{id}_X \qquad \textit{und} \qquad f \circ f^{-1} = \mathrm{id}_Y .$$

Relationenalgebra

Definition

Sei U eine Menge von Spaltenüberschriften. Ein Relationenschema σ ordnet jeder Überschrift $u\colon U$ einen Datentyp zu. Ein zu σ passendes Tupel ordnet jedem $u\colon U$ ein Element vom Typ $\sigma(u)$ zu. Eine zu σ passende Relation (im Sinne der Relationenalgebra) besteht dann aus einer (üblicherweise endlichen) Menge von derartigen Tupeln.

Bemerkung

In praktischen Anwendungen kann ein Relationenschema mehr als nur die Datentypen der verschiedenen Spalten festlegen (z.B. Beziehungen zwischen den Spalten und zu anderen Relationen). Darauf wollen wir hier allerdings nicht näher eingehen.

Bemerkung

Da Relationen gemäß Definition eine Menge von Tupeln sind, ist klar, wie Durchschnitt, Vereinigung und Mengendifferenz von Relationen (vom selben Schema!) zu bilden sind.

Grundoperationen für Relationen

Definition

Eine Restriktion (auch Selektion) wählt gewisse Tupel aus einer Relation (d.h. Zeilen einer Tabelle) aufgrund eines Kriteriums aus. Bezeichnungsweise: σ_K, wobei K das Kriterium ist.

Definition

Eine Projektion wählt aus jedem Tupel einer Relation gewisse Komponenten aus (d.h. Spalten einer Tabelle). Bezeichnungsweise: π_U, wobei U eine Liste von Spaltenüberschriften ist.

Definition

Beim kartesischen Produkt zweier Relationen R, S wird jedes Tupel der einen Relation mit jedem Tupel der anderen Relation kombiniert und aus diesen eine neue Relation $R \times S$ gebildet.

Definition

Umbenennung der Überschriften.

Example

Wir bilden das kartesischen Produkt $R \times S$ der folgende Relationen R und S:

A	B
a	1
a	2
b	1

$\times$

C	D
2	x
1	y

$=$

A	B	C	D
a	1	2	x
a	2	2	x
b	1	2	x
a	1	1	y
a	2	1	y
b	1	1	y

In Forsetzung des vorigen Beispiels wählen wir nun all jene Zeilen aus, bei denen die Spalten B und C übereinstimmen (Restriktion mit B=C). Dies ergibt zuerst:

$$\sigma_{B=C}(R \times S) \;=\; \begin{array}{c|c|c|c} A & B & C & D \\ \hline a & 2 & 2 & x \\ a & 1 & 1 & y \\ b & 1 & 1 & y \end{array}$$

Klarerweise ist es unnötig beide Spalten (B und C), die ohnehin gleich sind, zu verwenden. Wir können etwa die Spalte C weglassen, mit einer Projektion auf A,B,D. Dies ergibt:

$$\pi_{A,B,D}(\sigma_{B=C}(R \times S)) \;=\; \begin{array}{c|c|c} A & B & D \\ \hline a & 2 & x \\ a & 1 & y \\ b & 1 & y \end{array}$$

Relationenprodukt

Oft ist man in solchen Fällen an der vermittelnden Spalte gar nicht interessiert und führt eine Projektion auf A,D durch. Dies führt zum ganz normalen Relationenprodukt $(R;S)$:

$$\pi_{A,D}(\sigma_{B=C}(R \times S)) \; = \; \begin{array}{c|c} \text{A} & \text{D} \\ \hline \text{a} & \text{x} \\ \text{a} & \text{y} \\ \text{b} & \text{y} \end{array} \; = \; R;S$$

SQL

$$R = \begin{array}{c|c} A & B \\ \hline a & 1 \\ a & 2 \\ b & 1 \end{array} \quad S = \begin{array}{c|c} C & D \\ \hline 2 & x \\ 1 & y \end{array} \qquad R;S = \begin{array}{c|c} A & D \\ \hline a & x \\ a & y \\ b & y \end{array}$$

Das Relationenprodukt $R;S = \pi_{A,D}(\sigma_{B=C}(R \times S))$ im obigen Beispiel läßt sich folgendermaßen mit SQL realisieren :

```
 select distinct A, D
from R, S
where B = C
```

Vorgängerrelation in $\mathbb{N}$

Example

Vorgängerrelation: $\prec\colon \mathbb{N} \to \mathbb{N} \to \mathbb{P}$

$$m \prec n :\Longleftrightarrow \; Sm = n.$$

Sei weiters $P\colon \mathbb{N} \to \mathbb{P}$. Dann ist

$$\begin{aligned} \big(\forall_{m \prec Sn} P(m)\big) \; &\Longleftrightarrow \; P(n) \\ \big(\forall_{m \prec 0} P(m) \; &\Longleftrightarrow \; \top \end{aligned}$$

Das Induktionsprinzip (Peano-Induktion):

$$\frac{P(0) \quad \forall_{n\,:\,\mathbb{N}}\big(P(n) \implies P(Sn))\big)}{\forall_{n\,:\,\mathbb{N}} P(n)}$$

$$\frac{\forall_{n\,:\,\mathbb{N}}\big(\forall_{m \prec n} P(m)\big) \implies P(n)}{\forall_{n\,:\,\mathbb{N}} P(n)}$$

Vorgängerfunktion für Listen

Example

Vorgängerrelation für Listen: $\prec : A^* \to A^* \to \mathbb{P}$

$$t \prec \ell :\Longleftrightarrow \exists_{h\,:\,A}\; h \triangleleft t = \ell.$$

Das bekannte Induktionsprinzip für Listen ist dasselbe wie

$$\frac{\forall_{\ell\,:\,A^*}\big(\forall_{m \prec \ell} P(m)\big) \implies P(\ell)}{\forall_{\ell\,:\,A^*} P(\ell)}$$

Definition

Eine Relation $\prec : X \to X \to \mathbb{P}$ in einer Menge X heißt wohlfundiert wenn gilt:

$$\frac{\forall_{x\,:\,X}\big(\forall_{y \prec x} P(y)\big) \implies P(x)}{\forall_{x\,:\,X} P(x)}$$

Vollständige Induktion

Example

Die Relation $<: \mathbb{N} \to \mathbb{N} \to \mathbb{P}$ in den natürlichen Zahlen ist wohlfundiert. Dies bedeutet, daß auch das Prinzip der vollständigen Induktion gultig ist:

$$\frac{\forall_{n\,:\,\mathbb{N}}\big(\forall_{m\,:\,\mathbb{N}} m < n \implies P(m)\big) \implies P(n)}{\forall_{n\,:\,\mathbb{N}} P(n)}$$

Beispiel: Euklidscher Algorithmus.
Man beachte: $\prec^+ = <$.

Satz

Sei $\prec: X \to X$ eine wohlfundierte Relation in X, dann ist auch dessen transitive Hülle $\prec^+$ wohlfundiert.

Wohlfundiertheit durch eine Funktion

Satz

Sei $f : X \to Y$
und $\prec : Y \to Y \to \mathbb{P}$ *wohlfundiert.*
Dann ist auch die durch

$$x \prec_f y :\iff f(x) \prec f(y)$$

definierte Relation $\prec_f : X \to X \to \mathbb{P}$ *wohlfundiert.*

Example

Für Listen A^* ist die Länge eine Funktion in die natürlichen Zahlen.
Da in $\mathbb{N}$ die Relation $<$ wohlfundiert ist, ist auch die durch

$$m <_{|.|} \ell :\iff |m| < |\ell|$$

definierte Relation in A^* wohlfundiert.

Kürzere Listen

Dies erlaubt es uns, Induktion über die Länge von Listen zu führen:

$$\frac{\forall_{\ell\colon A^*}\big(\forall_{|m|<|\ell|} P(m)\big) \implies P(\ell)}{\forall_{\ell\colon A^*} P(\ell)}$$

Sortieren

Example

Sei A eine Menge, in der eine lineare Ordnung $\preceq$ definiert ist. Sei $\text{sort}\colon A^* \to A^*$ die Funktion, welche jeder Liste dessen sortierte Version zuordnet. Man kann eine solche Funktion etwa folgendermaßend rekursiv definieren:

$$\begin{aligned}
\text{sort}\,[] &= [] \\
\text{sort}(\ell) &= \text{sort}[x \leftarrow \ell \mid x \prec a] \mathbin{+\!\!+} [x \leftarrow \ell \mid x = a] \mathbin{+\!\!+} \text{sort}[x \leftarrow \ell \mid x \succ a]
\end{aligned}$$

wobei für das a in der zweiten Gleichung irgendein Element aus der Liste ℓ gewählt wird (am besten zufällig).

Anmerkung: Damit der Algorithmus wirklich funktioniert muß man die Alternativen $x \prec y$, $x = y$, $x \succ y$ effektiv entscheiden können.

Direktes Produkt

Satz

In den Mengen A und B seien die wohlfundierten Relation $\prec_A$ bzw. $\prec_B$ gegeben. Dann erhalten wir durch

$$(a,b) \prec (c,d) :\iff a \prec_A c \wedge b \prec_B d$$

eine wohlfundierte Relation.
Alternativ erhalten wir auch durch

$$(a,b) \prec (c,d) :\iff a \prec_A c \vee (a = b \wedge b \prec_B d)$$

eine wohlfundierte Relation (lexikographische Ordnung).

Example

Die Ackermann-Funktion

Bemerkung

Die lexikographische Ordnung läßt sich auch für Listen formulieren.