

Abschnitt i1math

29. November 1999

Inhaltsverzeichnis

1	Einführung	9
1.1	Was ist Informatik?	9
1.2	Geschichte der Programmierung	16
1.3	Problemlösen durch Algorithmen	20
2	Induktive Definitionen	24
2.1	Natürliche Zahlen	24
2.2	Wortmengen	30
2.3	Syntaktische Beschreibungsmittel	34
2.3.1	Backus-Naur-Form	35
2.3.2	Erweiterte BNF	41
2.4	Terme	46
2.5	Aufgaben	53
3	Algorithmen und Programme	55
3.1	Verifikation von Algorithmen	72
3.2	Termination und Rechenaufwand	73
3.3	Aufgaben	80
4	Abstrakte Datentypen	101
4.1	Einführung	101
4.2	Listen	103
4.3	Bäume	110
A	Mathematische Grundlagen	119
A.1	Mengen, Relationen, Abbildungen	119
A.2	Formale Logik	124
A.2.1	Aussagenlogik	124
A.2.2	Prädikatenlogik	126
A.3	Halbordnungen	128
A.4	Aufgaben	129

Anhang A

Mathematische Grundlagen

Ein gewisses mathematisches Rüstzeug muß für die Informatik vorausgesetzt werden. Dieser Anhang gibt kaum Erklärungen, sondern ist mehr als Festlegung der in diesem Buch verwendeten Begriffe und Notationen aus der Mathematik zu verstehen.

A.1 Mengen, Relationen, Abbildungen

Wir setzen voraus, daß die Grundbegriffe der Mengenlehre bekannt sind. Eine ausführliche Behandlung der Mengenlehre auf naiver, also nicht axiomatischer Basis findet sich in [Hal69].

„Unter einer Menge verstehen wir eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen“. (G. CANTOR)

Die Objekte einer Menge M heißen *Elemente* von M . Wir schreiben $x \in M$, wenn x ein Element von M ist, $x \notin M$, wenn x kein Element von M ist.

Häufig haben wir es mit Mengen von *Zahlen* zu tun. Für die wichtigsten Zahlenmengen legen wir bestimmte Bezeichnungen fest. So bezeichnet \mathbb{N} stets die Menge der *natürlichen Zahlen*; allerdings werden wir im Gegensatz zur mathematischen Tradition auch $0 \in \mathbb{N}$ annehmen. \mathbb{Z} bezeichnet die Menge der *ganzen Zahlen* und \mathbb{R} die Menge der *reellen Zahlen*.

Endliche Mengen, also Mengen mit endlich vielen Elementen schreiben wir manchmal als Aufreihung ihrer Elemente auf:

$$M = \{11, 13, 17, 19\}.$$

Häufig werden Mengen jedoch auch durch eine bestimmte Eigenschaft definiert, die man von ihren Elementen fordert:

$$M = \{x \mid x \text{ ist Primzahl}, 10 \leq x \leq 20\}.$$

Die *leere Menge* ist die Menge, die keine Elemente besitzt und wird durch \emptyset bezeichnet.

Wir sagen $A \subseteq B$ (A ist Teilmenge von B), wenn jedes Element von A auch Element von B ist. In Zeichen:

$$A \subseteq B \stackrel{\text{def}}{\iff} \forall a (a \in A \Rightarrow a \in B).^1$$

Zwei Mengen sind gleich, wenn sie die gleichen Elemente besitzen (sog. *Extensionalitätsprinzip*); dies können wir mit Hilfe der Teilmengenbeziehung auch so ausdrücken:

$$A = B \stackrel{\text{def}}{\iff} A \subseteq B \text{ und } B \subseteq A.$$

Hieraus ergibt sich für die oben erwähnte Darstellung endlicher Mengen z.B.

$$\{11, 13, 17, 19\} = \{17, 13, 19, 11\},$$

d.h. die *Reihenfolge* der Elemente ist unerheblich (bzw. es gibt gar keine ausgezeichnete Reihenfolge) und

$$\{11, 13, 17, 19\} = \{11, 13, 11, 17, 17, 11, 13, 19\},$$

d.h. es spielt keine Rolle, wie oft wir ein bestimmtes Element erwähnen; es ist trotzdem nur einmal in der Menge enthalten.

Wir sagen $A \not\subseteq B$, wenn $A \subseteq B$ nicht gilt, $A \neq B$, wenn $A = B$ nicht gilt. A heißt *echte Teilmenge* von B , wenn $A \subseteq B$, aber $A \neq B$. Wir schreiben dann $A \subset B$. Wir schreiben $B \supseteq A$, wenn $A \subseteq B$ gilt, ebenso für $B \supset A$.

Die *Vereinigung* $A \cup B$ zweier Mengen A und B ist definiert durch

$$A \cup B \stackrel{\text{def}}{=} \{a \mid a \in A \text{ oder } a \in B\}.$$

Dabei ist das „oder“ kein ausschließliches „oder“ („entweder–oder“); es darf durchaus auch $a \in A$ und $a \in B$ sein.

Der *Durchschnitt* $A \cap B$ zweier Mengen A und B ist definiert durch

$$A \cap B \stackrel{\text{def}}{=} \{a \mid a \in A \text{ und } a \in B\}.$$

Die *Differenz* $A \setminus B$ zweier Mengen A und B ist definiert durch

$$A \setminus B \stackrel{\text{def}}{=} \{a \mid a \in A, a \notin B\}.$$

Die mengentheoretische Differenz hat durch diese Definition etwas andere Eigenschaften als die arithmetische Differenz. Es gilt z.B.

$$\{11, 13, 17, 19\} \setminus \{11, 31, 41\} = \{13, 17, 19\};$$

die Tatsache, daß 31 und 41 in der ersten Menge gar nicht vorkommen, spielt keine Rolle.

¹Die logischen Zeichen werden in Abschnitt A.2 behandelt.

Definition A.1 Das *cartesische Produkt* $A \times B$ zweier Mengen A und B ist definiert durch

$$A \times B \stackrel{\text{def}}{=} \{(a, b) \mid a \in A, b \in B\}.$$

Für $n \geq 2$ Mengen A_1, \dots, A_n definieren wir:

$$A_1 \times \dots \times A_n \stackrel{\text{def}}{=} \{(a_1, \dots, a_n) \mid a_i \in A_i\}.$$

Für eine Menge A und eine natürliche Zahl $n \geq 2$ definieren wir

$$A^n \stackrel{\text{def}}{=} A \times \overset{n}{\dots} \times A.$$

Damit wir die Fälle $n = 0$ und $n = 1$ nicht immer ausschließen müssen, definieren wir außerdem

$$\begin{aligned} A^1 &\stackrel{\text{def}}{=} A \\ A^0 &\stackrel{\text{def}}{=} \{()\}. \end{aligned}$$

A^0 ist also eine einelementige Menge, deren einziges Element wir in Übereinstimmung mit der Tupelschreibweise (a_1, \dots, a_n) mit $()$ bezeichnen.

Für eine Menge A bezeichnen wir die Anzahl ihrer Elemente („Mächtigkeit“) mit $|A|$. Für unendliche Mengen vereinbaren wir $|A| = \infty$.

Für eine Menge A heißt

$$\mathcal{P}(A) \stackrel{\text{def}}{=} \{T \mid T \subseteq A\}$$

die *Potenzmenge* von A . Für endliche Mengen gilt $|\mathcal{P}(A)| = 2^{|A|}$.

Nach diesen Vorbereitungen kommen wir nun zum eigentlichen Thema dieses Abschnitts:

Definition A.2 Eine (*binäre*) *Relation* ist eine Teilmenge $\rho \subseteq A \times B$. ρ heißt

- *rechtseindeutig* $\stackrel{\text{def}}{\iff}$ für alle $a \in A$ gibt es höchstens ein $b \in B$ mit $(a, b) \in \rho$,
- *linkseindeutig* $\stackrel{\text{def}}{\iff}$ für alle $b \in B$ gibt es höchstens ein $a \in A$ mit $(a, b) \in \rho$.

Statt $(a, b) \in \rho$ schreiben wir in der Regel $a\rho b$. Für eine Relation ρ heißt

$$\rho^{-1} \stackrel{\text{def}}{=} \{(b, a) \mid (a, b) \in \rho\}$$

die *Umkehrrelation* von ρ .

In der Praxis werden Relationen häufig durch *Tabellen* oder *Pfeildiagramme* dargestellt.

Definition A.3 Eine Relation $\rho \subseteq A \times A$ heißt

- *reflexiv* $\stackrel{\text{def}}{\iff}$ für alle $a \in A$ gilt $a\rho a$,
- *irreflexiv* $\stackrel{\text{def}}{\iff}$ für kein $a \in A$ gilt $a\rho a$,
- *symmetrisch* $\stackrel{\text{def}}{\iff}$ aus $a\rho b$ folgt $b\rho a$,
- *antisymmetrisch* $\stackrel{\text{def}}{\iff}$ aus $a\rho b$ und $b\rho a$ folgt $a = b$,
- *transitiv* $\stackrel{\text{def}}{\iff}$ aus $a\rho b$ und $b\rho c$ folgt $a\rho c$,
- *Äquivalenzrelation* $\stackrel{\text{def}}{\iff}$ ρ ist reflexiv, symmetrisch und transitiv.

Definition A.4 Eine *Abbildung* ist ein Tripel $f = (A, \rho_f, B)$, wobei A und B Mengen sind und $\rho_f \subseteq A \times B$ eine rechtseindeutige Relation. A heißt *Vorbereich* von f , B heißt *Nachbereich* und ρ_f der *Graph* von f . Statt $f = (A, \rho_f, B)$ schreiben wir auch $f : A \rightarrow B$ oder $A \xrightarrow{f} B$. Statt $(a, b) \in \rho_f$ schreiben wir normalerweise $f(a) = b$. Die Teilmenge

$$\text{Def}(f) \stackrel{\text{def}}{=} \{a \in A \mid \text{es gibt } b \in B \text{ mit } f(a) = b\}$$

von A heißt *Definitionsbereich* von f , die Teilmenge

$$\text{Im}(f) \stackrel{\text{def}}{=} \{b \in B \mid \text{es gibt } a \in A \text{ mit } f(a) = b\}$$

von B heißt *Bildbereich* von f .

Nach dieser Definition sind zwei Abbildungen $f = (A, \rho_f, B)$ und $g = (C, \rho_g, D)$ *gleich* genau dann, wenn $A = C$, $B = D$ und $\rho_f = \rho_g$. Beachte, daß die Gleichheit der Graphen auch die Gleichheit von Definitionsbereich und Bildbereich mit sich bringt.

Definition A.5 Für eine Menge A ist die *Identitätsabbildung* definiert durch $\text{id}_A \stackrel{\text{def}}{=} (A, \rho_{\text{id}_A}, A)$ mit $\rho_{\text{id}_A} \stackrel{\text{def}}{=} \{(a, a) \mid a \in A\}$.

Definition A.6 Die Abbildungen nach Definition A.4 sind sogenannte *partielle Abbildungen*, d.h. wir können nicht sicher sein, daß $\text{Def}(f) = A$ gilt. Eine Abbildung $A \xrightarrow{f} B$ heißt

- *total* $\stackrel{\text{def}}{\iff} \text{Def}(f) = A$,
- *surjektiv* $\stackrel{\text{def}}{\iff} \text{Im}(f) = B$,
- *injektiv* $\stackrel{\text{def}}{\iff}$ aus $f(a_1) = f(a_2)$ folgt $a_1 = a_2$ für beliebige $a_1, a_2 \in A$,

- *bijektiv* $\stackrel{\text{def}}{\iff} A \xrightarrow{f} B$ ist injektiv, total und surjektiv.

Ist $A \xrightarrow{f} B$ bijektiv, so heißen A und B *isomorph*, in Zeichen $A \cong B$.

Vielfach verwendet man auch die Bezeichnung „Funktion“ für eine totale Abbildung. Für partielle Abbildungen verwenden wir in der Regel die Schreibweise $f : A \rightsquigarrow B$, um so nicht eigens auf die Partialität hinweisen zu müssen. Wenn wir $f : A \rightarrow B$ schreiben, so heißt dies, daß f total ist.

Definition A.7 Für zwei Mengen A, B bezeichnet man die Menge der partiellen Abbildungen von A nach B mit $[A \rightarrow B]$, die Menge der totalen Abbildungen von A nach B mit B^A . Beachte, daß die Menge der partiellen Abbildungen die der totalen beinhaltet.

Definition A.8 Für zwei Abbildungen $A \xrightarrow{f} B$ und $B \xrightarrow{g} C$ definiert man die *Komposition* $g \circ f$ durch

$$g \circ f \stackrel{\text{def}}{=} (A, \rho_{g \circ f}, C)$$

mit

$$\rho_{g \circ f} \stackrel{\text{def}}{=} \{(a, c) \mid \text{es gibt } b \in B \text{ mit } (a, b) \in \rho_f \text{ und } (b, c) \in \rho_g\}.$$

Lemma A.9 Die Komposition von Abbildungen ist assoziativ, das heißt für $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ und $C \xrightarrow{h} D$ gilt

$$(h \circ g) \circ f = h \circ (g \circ f).$$

Man läßt deshalb oft die Klammern ganz weg und schreibt $h \circ g \circ f$. Eine ähnliche Aussage gilt für partielle Abbildungen, wobei allerdings auf die Definitionsbereiche zu achten ist.

Lemma A.10 Für eine bijektive Abbildung $A \xrightarrow{f} B$ mit $f = (A, \rho_f, B)$ existiert eine Umkehrabbildung $B \xrightarrow{f^{-1}} A$ mit $f^{-1} \stackrel{\text{def}}{=} (B, \rho_{f^{-1}}, A)$, wobei $\rho_{f^{-1}} \stackrel{\text{def}}{=} \rho_f^{-1}$. Es gilt $f^{-1} \circ f = \text{id}_A$ und $f \circ f^{-1} = \text{id}_B$.

Kommen wir nun noch einmal zurück zu den Potenzmengen. Es ist üblich, Teilmengen $T \subseteq \mathcal{P}(A)$ durch sog. *charakteristische Funktionen* darzustellen:

Definition A.11 Sei A eine Menge, $T \in \mathcal{P}(A)$. Die *charakteristische Funktion* von T ist definiert durch

$$\chi_T : A \rightarrow \{0, 1\}$$

$$\chi_T(x) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{falls } x \in T \\ 0 & \text{falls } x \notin T \end{cases}$$

Ist umgekehrt $f : A \rightarrow \{0, 1\}$ eine (totale) Abbildung, so kann man hieraus eine Menge $T_f \in \mathcal{P}(A)$ ableiten durch

$$T_f \stackrel{\text{def}}{=} \{x \in A \mid f(x) = 1\}.$$

Die Zuordnung $T \rightarrow \chi_T$ ist bijektiv.

Definition A.12 Für $T \in \mathcal{P}(A)$ ist das *Komplement* (von T in A) definiert durch

$$\bar{T} \stackrel{\text{def}}{=} A \setminus T.$$

Lemma A.13 Für $A, B \in \mathcal{P}(M)$ gelten die (sog. de Morgan'schen) Gesetze:

$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

A.2 Formale Logik

Wie in dem vorangehenden Abschnitt wollen wir auch hier nicht übertrieben formal vorgehen, sondern eher intuitiv.

A.2.1 Aussagenlogik

Eine *Aussage* ist ein Satz, dem man prinzipiell einen *Wahrheitswert* zuordnen kann. Unerheblich ist dabei, ob man diesen Wahrheitswert auch ermitteln kann. Wir verwenden eine *zweiwertige Logik* mit den Wahrheitswerten W (wahr) und F (falsch).²

Beispiele für Aussagen und ihre Wahrheitswerte:

1. 6 ist eine Primzahl (F).
2. 1024 ist eine Zweierpotenz (W).
3. Es gab früher Leben auf der Venus (unbekannt, aber jedenfalls W oder F).

Keine Aussage in diesem Sinne ist der Satz: „Der Wahrheitswert dieses Satzes ist F “, denn es ist offensichtlich unmöglich, diesem Satz einen Wahrheitswert W oder F zuzuordnen.

Aus *primitiven (elementaren) Aussagen* werden mit Hilfe sog. aussagenlogischer *Junktoren* zusammengesetzte Aussagen aufgebaut; die wichtigsten Junktoren sind:

„**und**“ (\wedge): $a \wedge b$ hat den Wahrheitswert W genau dann, wenn a und b beide den Wert W haben.

„**oder**“ (\vee): $a \vee b$ hat den Wahrheitswert W genau dann, wenn von a und b mindestens eins den Wert W hat.

²Für den Wahrheitswert W sind in der Informatik auch die Bezeichnungen true, 1 oder H (= high) gebräuchlich, für F auch false, 0 oder L (= low).

„nicht“ (\neg): $\neg a$ hat den Wahrheitswert W genau dann, wenn a den Wert F hat.

In der Aussagenlogik gilt demnach das Prinzip, daß man den Wahrheitswert einer zusammengesetzten Aussage allein aus den Wahrheitswerten der Bestandteile bestimmen kann (Extensionalitätsprinzip). Wir haben dieses Prinzip schon bei den Mengen kennengelernt: Zwei Mengen sind gleich, wenn alle ihre Elemente gleich sind. Das Extensionalitätsprinzip ist auch sonst in der Informatik von großer Wichtigkeit; so wird z.B. die Bedeutung eines *Programms* einer strukturierten Programmiersprache allein durch die Bedeutung seiner Bestandteile erklärt.

Statt $\neg a$ wird gelegentlich auch \bar{a} geschrieben, was besonders in Formeln wie $\neg(a \vee b) = \bar{a} \wedge \bar{b}$ die Lesbarkeit verbessert.

Meistens werden logische Junktoren durch sogenannte *Wahrheitstafeln* definiert:

\wedge	W	F
W	W	F
F	F	F

\vee	W	F
W	W	W
F	W	F

\neg	
W	F
F	W

Andere Junktoren, die ebenfalls häufig verwendet werden, sind:

„impliziert“ (\Rightarrow):

\Rightarrow	W	F
W	W	F
F	W	W

$a \Rightarrow b$ liest man auch als „wenn a , dann b “ oder „aus a folgt b “. Beachte, daß $F \Rightarrow W$ ebenso wie $F \Rightarrow F$ beide den Wahrheitswert W besitzen! In der formalen Aussagenlogik kann man aus einer falschen Voraussetzung jede Folgerung ziehen. Zum Ableiten wahrer Aussagen aus anderen wahren Aussagen verwendet man deshalb den *Modus ponens*: Wenn a und $a \Rightarrow b$ beide den Wahrheitswert W haben, dann kann man den Wahrheitswert W für b folgern.

„äquivalent“ (\Leftrightarrow):

\Leftrightarrow	W	F
W	W	F
F	F	W

Häufig sieht man die Wahrheitstafeln auch in einer etwas ausführlicheren Form, wie im folgenden gezeigt. Dabei haben wir die Wahrheitstafeln für alle vorgestellten Junktoren in einer Tabelle zusammengefaßt:

a	b	$a \wedge b$	$a \vee b$	$\neg a$	$a \Rightarrow b$	$a \Leftrightarrow b$
W	W	W	W	F	W	W
W	F	F	W	F	F	F
F	W	F	W	W	W	F
F	F	F	F	W	W	W

Zur Einsparung von Klammern vereinbaren wir, daß \neg am stärksten bindet, gefolgt von \wedge , dann \vee , dann \Rightarrow und zum Schluß \Leftrightarrow .

Eine zusammengesetzte Aussage heißt *allgemeingültig* oder eine *Tautologie*, wenn sie stets den Wahrheitswert W besitzt, unabhängig vom Wahrheitswert ihrer elementaren Aussagen. Beispiele für Tautologien sind etwa $a \vee \bar{a}$ („Satz vom ausgeschlossenen Dritten“) und $\overline{a \wedge \bar{a}}$ („Satz vom Widerspruch“). Zwei Aussagen a und b heißen *äquivalent*, wenn $a \Leftrightarrow b$ eine Tautologie ist.

Man kann zeigen, daß man nur die Junktoren \wedge , \vee , \neg braucht, um jede aussagenlogische Aussage formulieren zu können. So ist etwa die Aussage $a \Rightarrow b$ äquivalent zu $\neg a \vee b$, wie man leicht anhand der Wahrheitstafeln verifiziert. In Wirklichkeit kommt man sogar mit nur je einem von zwei Junktoren aus, die man „nor“ und „nand“ nennt und die definiert sind durch:

$$a \text{ nor } b \stackrel{\text{def}}{\Leftrightarrow} \neg(a \vee b)$$

$$a \text{ nand } b \stackrel{\text{def}}{\Leftrightarrow} \neg(a \wedge b).$$

Im Prinzip könnte man jede aussagenlogische Aussage durch Wahrheitstafeln auf ihre Allgemeingültigkeit hin überprüfen. Auch die Äquivalenz von Ausdrücken kann man durch Wahrheitstafeln überprüfen. In der Regel ist es jedoch zweckmäßiger, mit diesen Ausdrücken formal zu rechnen. Die folgenden Tautologien stellen *Rechenregeln* für die Aussagenlogik dar:

Lemma A.14 Für Aussagen a, b, c gilt:

$$\begin{array}{ll} a \wedge a \Leftrightarrow a & a \vee a \Leftrightarrow a \\ (a \wedge b) \wedge c \Leftrightarrow a \wedge (b \wedge c) & (a \vee b) \vee c \Leftrightarrow a \vee (b \vee c) \\ a \wedge b \Leftrightarrow b \wedge a & a \vee b \Leftrightarrow b \vee a \\ a \wedge (a \vee b) \Leftrightarrow a & a \vee (a \wedge b) \Leftrightarrow a \\ a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c) & a \vee (b \wedge c) \Leftrightarrow (a \vee b) \wedge (a \vee c) \\ \overline{a \wedge b} \Leftrightarrow \bar{a} \vee \bar{b} & \overline{a \vee b} \Leftrightarrow \bar{a} \wedge \bar{b} \\ \bar{\bar{a}} \Leftrightarrow a & \end{array}$$

Diese Gesetze heißen (in der angegebenen Reihenfolge) *Idempotenzgesetz*, *Assoziativgesetz*, *Kommutativgesetz*, *Absorptivgesetz* und *Distributivgesetz*. Das *de-Morgan'sche Gesetz* kennen wir bereits aus der Mengenlehre.³

A.2.2 Prädikatenlogik

Häufig macht man in der Mathematik Aussagen der Gestalt, daß es mindestens ein Objekt (Individuum) mit einer bestimmten Eigenschaft („Prädikat“) gibt oder daß ein bestimmtes Prädikat für alle Objekte aus einem bestimmten

³Ersetzt man \wedge durch \cap , \vee durch \cup und \Leftrightarrow durch $=$, so gelten alle diese Gesetze auch in der Mengenlehre.

Bereich gilt. Dazu werden sogenannte *Quantoren* eingeführt, und zwar der *Allquantor* (Universalquantor) \forall und der *Existenzquantor* \exists . Im folgenden bezeichnen wir Prädikate mit Großbuchstaben und Individuen mit Kleinbuchstaben. Die *Stelligkeit* eines Prädikats ist die Anzahl der Individuen, über die hier eine Aussage gemacht wird.

Ist Q ein n -stelliges Prädikat und sind x_1, \dots, x_n Individuen eines Individuenbereichs, so ist die Behauptung, daß Q auf x_1, \dots, x_n zutrifft (abgekürzt $Qx_1 \dots x_n$) eine prädikatenlogische Aussage. Wir verwenden auch aussagenlogische Aussagen und andere mathematische Ausdrücke wie $x \in M$ oder $n < m$ zur Formulierung prädikatenlogischer Aussagen. Dies ist nur eine Vereinfachung der Notation, da in Wirklichkeit $x \in M$, $n < m$ und ähnliche Ausdrücke auch zweistellige Prädikate sind. Statt der Individuen selbst kommen in den Quantorenausdrücken *Individuenvariablen* vor; diese sind Platzhalter für die Individuen selbst. Die prädikatenlogische Aussage

$$(\forall x)Qx$$

bedeutet dann: Für alle Individuen a gilt die Aussage (das Prädikat) Q , wobei für die Variable x das Individuum a eingesetzt wird. Dementsprechend heißt

$$(\exists x)Qx :$$

Es gibt mindestens ein Individuum a , so daß die Aussage Qa wahr ist. Die Variable x heißt in beiden Fällen eine *gebundene Variable* des Prädikatsausdrucks. Variablen, die nicht gebunden sind, heißen *freie Variablen*.

Eine wichtige Eigenschaft der Quantoren enthält der folgende Satz:

Satz A.15 *Ist Q ein einstelliges Prädikat, so ist die Aussage $\neg(\forall x)Qx$ genau dann wahr, wenn $(\exists x)\neg Qx$ wahr ist. Umgekehrt ist die Aussage $\neg(\exists x)Qx$ genau dann wahr, wenn $(\forall x)\neg Qx$ wahr ist.*

Im Prinzip ist es daher möglich, mit nur einem der beiden Quantoren auszukommen. Im Interesse der Verständlichkeit von Aussagen behält man jedoch beide Quantoren bei.

Häufig machen wir Einschränkungen an den Individuenbereich, indem wir z.B. schreiben

$$(\forall x \in M)(\exists y \in N) Pxy .$$

Dies kann man als Abkürzung für die kompliziertere Aussage

$$(\forall x)(x \in M \Rightarrow (\exists y \in N)Pxy)$$

oder die noch kompliziertere Aussage

$$(\forall x)(x \in M \Rightarrow (\exists y)(y \in N \wedge Pxy))$$

verstehen.

A.3 Halbordnungen

Definition A.16 Sei M eine Menge. Eine Relation $\rho \subseteq M \times M$ heißt *Halbordnung* auf M $\stackrel{\text{def}}{\iff} \rho$ ist

1. *reflexiv*, d.h. $(\forall x \in M) x\rho x$,
2. *transitiv*, d.h. $(\forall x, y, z \in M) (x\rho y \wedge y\rho z) \Rightarrow x\rho z$ und
3. *antisymmetrisch*, d.h. $(\forall x, y \in M) (x\rho y \wedge y\rho x) \Rightarrow x = y$.

Ein Beispiel für eine Halbordnung ist etwa die Relation „ \subseteq “ zwischen Mengen. Unter einer *halbgeordneten Menge* $(M; \rho)$ wollen wir eine Menge M mit einer Halbordnung ρ verstehen. Normalerweise gibt es in einer halbgeordneten Menge *unvergleichbare Elemente*, d.h. Elemente $x, y \in M$, für die weder $x\rho y$ noch $y\rho x$ gilt. In der halbgeordneten Menge $(M; \subseteq)$ mit

$$M = \{\{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$$

sind z.B. die Elemente $\{1, 2\}$ und $\{2, 3\}$ unvergleichbar. Daher definieren wir

Definition A.17 Eine *totale Ordnung* auf einer Menge M ist eine Halbordnung ρ , bei der zusätzlich gilt

$$(\forall x, y \in M) x\rho y \vee y\rho x.$$

Definition A.18 Sei $(M; \rho)$ eine halbgeordnete Menge. Ein Element $x \in M$ heißt

minimales Element: $\stackrel{\text{def}}{\iff} (\forall y \in M) y\rho x \Rightarrow y = x$

kleinstes Element: $\stackrel{\text{def}}{\iff} (\forall y \in M) x\rho y$

Erfahrungsgemäß werden die Begriffe „minimales“ und „kleinstes Element“ gerne verwechselt. Das liegt vielleicht daran, daß die Relation „ \leq “ auf Zahlen, die man gerne als „Modell“ für eine Halbordnung betrachtet, in Wirklichkeit eine totale Ordnung ist. Bei totalen Ordnungen fallen die Begriffe „minimales“ und „kleinstes Element“ jedoch zusammen. Deshalb hier noch einmal eine verbale Definition:

minimales Element heißt, daß es kein Element gibt, das kleiner ist. Es kann aber Elemente geben, die unvergleichbar mit einem minimalen Element sind. (In der oben angegebenen Menge M sind $\{1, 2\}$ und $\{2, 3\}$ beide minimal.)

kleinstes Element heißt, daß alle anderen Elemente größer sind. Damit ist auch die Vergleichbarkeit gegeben. Es gibt in einer Menge höchstens ein kleinstes Element. (In der oben angegebenen Menge M gibt es kein kleinstes Element.)

Definition A.19 Für eine halbgeordnete Menge $(M; \rho)$ werden die Begriffe *maximales Element* und *größtes Element* dual zu den Begriffen *minimales* und *kleinstes Element* definiert.

A.4 Aufgaben

Aufgabe A.1 $A \xrightarrow{f} A$ sei eine injektive Abbildung. Zeige, daß f total ist genau dann, wenn f bijektiv ist.

Aufgabe A.2 $A \xrightarrow{f} B \xrightarrow{g} C$ sei injektiv (surjektiv). Was kann man dann über $A \xrightarrow{f} B$ bzw. $B \xrightarrow{g} C$ mit Bestimmtheit sagen?

Aufgabe A.3 Zeige, daß die Umkehrfunktion $B \xrightarrow{f^{-1}} A$ einer bijektiven Funktion $A \xrightarrow{f} B$ stets injektiv ist.

Aufgabe A.4 Für eine endliche Menge A beweise man

$$|\mathcal{P}(A)| = 2^{|A|}$$

Aufgabe A.5 Sei A eine endliche Menge. Man beweise, daß für $T \in \mathcal{P}(A)$ gilt

$$|T| + |\bar{T}| = |A|$$

Aufgabe A.6 Herr Meier, ein ausgezeichneter Logiker, macht die folgende wahre Aussage: „Wenn es draußen regnet, regnet es draußen nicht“. Regnet es nun oder nicht?

Aufgabe A.7 Stellen Sie den folgenden aussagenlogischen Ausdruck durch ausschließliche Verwendung von *nor* dar:

$$(a \wedge b) \wedge (c \vee \bar{d})$$

Literaturverzeichnis

- [Bau68] BAUMANN, RICHARD: *Algol-Manual der Alcor-Gruppe*. R. Oldenbourg, München/Wien, 3. Auflage, 1968.
- [Bau89] BAUER, F. L.: *100 Jahre Peano-Zahlen*. Informatik-Spektrum, 12:340–341, 1989.
- [End72] ENDERTON, H. B.: *A Mathematical Introduction to Logic*. Academic Press, 1972.
- [GKP89] GRAHAM, R. L., D. E. KNUTH und O. PATASHNIK: *Concrete Mathematics*. Addison-Wesley, 1989.
- [Hal69] HALMOS, P: *Naive Mengenlehre*. Vandenhoeck & Ruprecht, Göttingen, 1969.
- [Kla83] KLAEREN, HERBERT: *Algebraische Spezifikation — Eine Einführung*. Springer Verlag, Berlin-Heidelberg-New York, 1983.
- [Knu73] KNUTH, D. E.: *The Art of Computer Programming*, volume 3. Addison-Wesley, 1973. Sorting and Searching.
- [Mes71] MESCHKOWSKI, H.: *Einführung in die moderne Mathematik*, Band 75/75a der Reihe *Hochschultaschenbücher*. BI, 1971.
- [MHR80] METROPOLIS, N., J. HOWLETT, and GIAN-CARLO ROTA (editors): *A History of Computing in the Twentieth Century*. Academic Press, 1980.
- [Wex81] WEXELBLAT, RICHARD L. (editor): *History of Programming Languages*, New York, 1981. Academic Press.
- [Wir85] WIRTH, NIKLAUS: *Programming in Modula-2*. Springer, 3rd edition, 1985.