

**185.263 Theoretische Informatik
und Logik
VU 4.0**

EINFÜHRUNG

Elementare Mengentheorie

GEORG CANTOR (1845 - 1918)



„Eine Menge ist eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unseres Denkens oder unserer Anschauung (welche die Elemente der Menge genannt werden) zu einem Ganzen.“

1874: Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen.

J. reine angew. Math., 77, 258-262

Elementare Mengentheorie

Eine **Menge** ist eine Gruppe von Objekten, die als Einheit repräsentiert werden.

Mengen können beliebige Typen von Objekten beinhalten, inklusive Zahlen, Symbole, und auch andere Mengen.

Die Objekte einer Menge bezeichnet man als **Elemente**.

Um einige Konzepte zu veranschaulichen, verwenden wir Venn-Diagramme. Dabei werden Mengen als Kreise dargestellt.

Zugehörigkeit

Mengen können formal auf verschiedene Arten beschrieben werden.

Eine Möglichkeit besteht darin, die Elemente aufzulisten:

$\{7,21,57\}$ enthält die Elemente 7,21,57

Notation:

\in ... Mengen-Zugehörigkeit $7 \in \{7,21,57\}$

\notin ... Nicht-Zugehörigkeit $5 \notin \{7,21,57\}$

Mengenvorschrift

Mengen können auch durch eine Mengenvorschrift angegeben werden:

$\{ x \mid E(x) \}$ Menge der Objekte x für die $E(x)$ gilt

$\{ x \in A \mid E(x) \}$ Menge der Objekte aus der Menge A für die $E(x)$ gilt

$\{ x \in A \mid E(x) \}$ ist äquivalent zu $\{ x \mid E(x) \text{ und } x \in A \}$

Beispiel: $\{ n \mid n = m^2 \text{ für } m \in \mathbf{N} \}$

Kardinalität von Mengen

Besteht eine Menge aus den Elementen a_1, \dots, a_n für $n \geq 1$, dann schreibt man $A = \{a_1, \dots, a_n\}$ (**endliche Menge**).

Eine **unendliche Menge** enthält unendlich viele Elemente.

Beispiel:

Menge der natürlichen Zahlen: $\mathbf{N} = \{0, 1, 2, 3, \dots\}$

Menge der natürlichen Zahlen $\geq k$: $\mathbf{N}_k = \{k, k+1, k+2, \dots\}$

Die Menge, die keine Elemente enthält, wird als **leere Menge** bezeichnet und geschrieben als $\{ \}$ oder \emptyset .

Die Anzahl der Elemente einer Menge M bezeichnet man als **Kardinalität**, geschrieben als $\text{card}(M)$.

Beispiel:

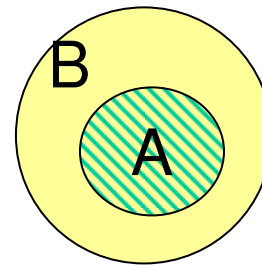
$$\text{card}(A) = n \quad \text{card}(\emptyset) = 0$$

(echte) Teilmengen

Für zwei Mengen A und B gilt:

A ist eine **Teilmenge** von B, wenn jedes Element von A auch ein Element von B ist.

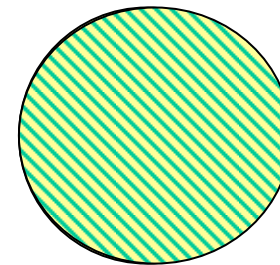
$$A \subseteq B$$



A ist eine **echte Teilmenge** von B, wenn A eine Teilmenge von B ist, die nicht gleich B ist.

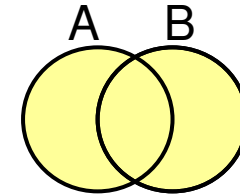
$$A \subset B$$

$A = B$ wenn $A \subseteq B$ und $B \subseteq A$



Operationen auf Mengen

Vereinigung: $A \cup B := \{ x \mid x \in A \text{ oder } x \in B \}$



Vereinigung endlich vieler Mengen M_1, \dots, M_n

$$\bigcup_{i \in \{1, \dots, n\}} M_i$$

Vereinigung abzählbar unendlich vieler Mengen M_1, M_2, \dots

$$\bigcup_{i \in \mathbf{N}_1} M_i \quad \text{bzw.} \quad \bigcup_{i \in \mathbf{N}_1} M_i$$

$$\bigcup_{i \in \mathbf{N}_1} M_i = \{ x \mid x \in M_i \text{ für ein } i \in \mathbf{N}_1 \}$$

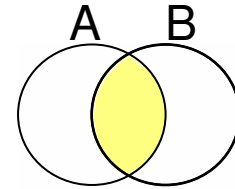
Für beliebige Mengen A , sodass M_a für jedes $x \in A$ eine Menge ist, definiert man

$$\bigcup_{a \in A} M_a = \{ x \mid x \in M_a \text{ für ein } a \in A \}$$

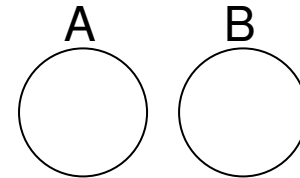
Operationen auf Mengen

Durchschnitt: $A \cap B := \{ x \mid x \in A \text{ und } x \in B \}$

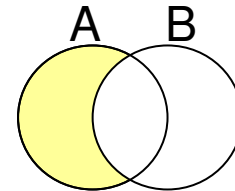
analog $\cap_{i \in \{1, \dots, n\}} M_i$, $\cap_{i \in \mathbb{N}_1} M_i$, $\cap_{a \in A} M_a$



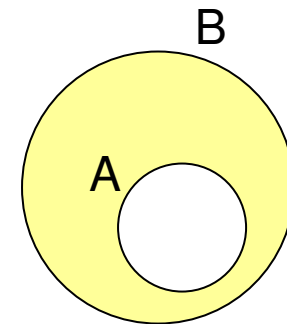
A und B sind **disjunkt** wenn $A \cap B = \emptyset$



Differenzmenge: $A - B := \{ x \mid x \in A \text{ und } x \notin B \}$



Gilt $A \subseteq B$, so nennt man $B - A$ das
Komplement von A (bezüglich B),
geschrieben \bar{A}



Operationen auf Mengen - Eigenschaften

Seien A, B, C Mengen, dann gilt:

$$A \cup A = A$$

Idempotenz

$$A \cup B = B \cup A$$

Kommutativität

$$(A \cup B) \cup C = A \cup (B \cup C)$$

Assoziativität

$$A \cup (A \cap B) = A$$

Absorption

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Distributivität

$$A - (B \cup C) = (A - B) \cap (A - C)$$

De Morgan'sches Gesetz

Duale Versionen: Vertauschen von \cap und \cup

(Multi-) Mengen

Die Reihenfolge der Elemente und auch deren Wiederholung in einer Menge ist nicht von Bedeutung.

$$\{7,7,57,7,21\} = \{7,21,57\}$$

Bemerkung:

$\{7\}$ und $\{7,7\}$ sind identische Mengen, aber unterschiedliche Multimengen (multisets).

Sequenzen (Tupel)

Eine Sequenz von Objekten ist eine geordnete Liste von Objekten.

Beispiel: $(7,21,57)$ ist eine andere Sequenz als $(7,57,21)$ oder auch $(7,7,21,57)$

Endliche Sequenzen werden auch **Tupel** genannt.

Eine Sequenz mit k Elementen wird **k-Tupel** genannt.

$((7,21,57))$ ist also ein 3-Tupel oder Tripel; ein 2-Tupel wird auch **Paar** genannt)

Mengen und Tupel können auch Elemente von anderen Mengen und Tupeln sein.

Operationen auf Mengen

Potenzmenge von A:

Menge aller Teilmengen von A 2^A bzw. $\mathcal{P}(A)$

Beispiel:

$$A = \{ 0, 1 \} \quad 2^A = \{ \{ \}, \{0\}, \{1\}, \{0,1\} \}$$

Kartesisches Produkt (Kreuzprodukt):

$$A \times B := \{ x \mid x = (a,b) \text{ mit } a \in A \text{ und } b \in B \}$$

$$M_1 \times \dots \times M_n := \{ x \mid x = (x_1, \dots, x_n) \text{ mit } x_i \in M_i \text{ f\"ur } 1 \leq i \leq n \}$$

$$\text{card}(A) = n, \text{ card}(B) = m$$

$$\text{card}(2^A) = 2^n \quad \text{card}(A \times B) = nm$$

Relationen und Funktionen

Relation R auf S: $R \subseteq S \times S$

(Definitionsbereich (domain) \times Wertebereich (range))

Menge von Paaren (a,b), wobei eine Beziehung zwischen a und b aus S besteht oder nicht besteht.

Schreibweise: aRb

Eigenschaften von Relationen

1. **Reflexiv** wenn aRa für alle a aus S gilt
2. **Irreflexiv** wenn aRa für alle a aus S falsch ist
3. **Transitiv** wenn aRc aus aRb und bRc folgt
4. **Symmetrisch** wenn bRa aus aRb folgt
5. **Asymmetrisch** wenn aRb impliziert, dass bRa nicht gilt.

Beispiel:

Ordnungsrelation $<$ auf der Menge der ganzen Zahlen ist transitiv und asymmetrisch (und daher irreflexiv)

Relationen und Funktionen

Äquivalenzrelation:

Relation, die reflexiv, symmetrisch und transitiv ist.

Wichtige Eigenschaft einer Äquivalenzrelation R auf S :

S wird durch R in disjunkte, nichtleere Äquivalenzklassen unterteilt.

$S = S_1 \cup S_2 \cup \dots$, wobei für i und j mit $i \neq j$ gilt:

1. $S_i \cap S_j = \{\}$
2. Für jedes a und b aus S_i ist aRb wahr
3. Für jedes a aus S_i und b aus S_j ist aRb falsch

Beispiel: Kongruenz modulo einer ganzen Zahl m

$i \equiv j \pmod{m}$ falls i und j ganze Zahlen sind mit der Eigenschaft, dass $i - j$ durch m teilbar ist.

Relationen und Funktionen

Hüllen von Relationen

E..Menge von Eigenschaften von Relationen über S.

E-Hülle von R ist die kleinste Relation R' , die alle Paare von R enthält und die Eigenschaften aus E besitzt

Transitive Hülle von R, geschrieben R^+ :

1. Falls (a,b) in R ist, so ist (a,b) auch in R^+
2. Falls (a,b) und (b,c) in R^+ sind, so ist (a,c) auch in R^+
3. Nichts ist in R^+ , außer es folgt aus 1. und 2.

Reflexive und Transitive Hülle von R, geschrieben R^* :

$$R^+ \cup \{(a,a) \mid a \in S\}$$

Beispiel: Sei $R = \{ (1,2), (2,2), (2,3) \}$ Relation auf $\{1,2,3\}$

$$R^+ = \{ (1,2), (2,2), (2,3), (1,3) \}$$

$$R^* = \{ (1,1), (1,2), (1,3), (2,2), (2,3), (3,3) \}$$

Relationen und Funktionen

Unter einer **Funktion** oder Abbildung $f: X \rightarrow Y$ einer Menge X in eine Menge Y (festgelegt durch $f \subseteq X \times Y$) versteht man eine Vorschrift, die jedem Element x von X ein eindeutig bestimmtes Element y aus Y zuordnet: $f(x)=y$
($f(x)$ ist der Funktionswert von f an Stelle x)

Funktionswerte von f (*range*):

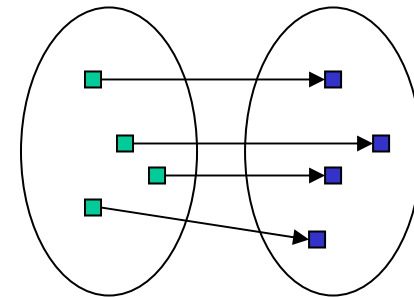
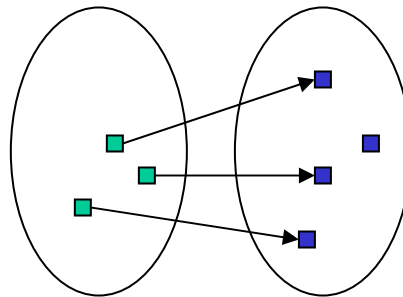
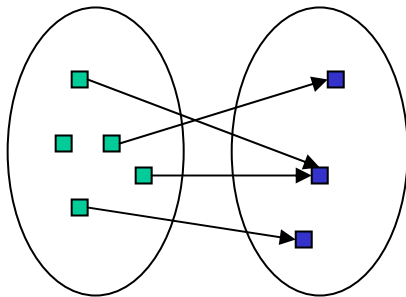
$$\text{rng}(f) = \{ y \mid (x,y) \in f \text{ für ein } x \in X \}$$

$f: X \rightarrow Y$ und $g: X \rightarrow Y$ heißen **gleich**, symbolisch $f \equiv g$, wenn $f(x) = g(x)$ für alle $x \in X$.

Relationen und Funktionen

Man nennt f

- **surjektiv** von X auf Y , wenn $\text{rng}(f) = Y$
- **injektiv** wenn für beliebige $x_1, x_2 \in X$ aus $f(x_1) = f(x_2)$ auch $x_1 = x_2$ folgt.
- **bijektiv** wenn f sowohl surjektiv als auch injektiv ist.



Grundbegriffe der Algebra

Sei M eine nicht-leere Menge; unter einer **binären Operation** (Abbildung) $\circ : M \times M \rightarrow M$ versteht man eine Vorschrift, die jedem geordneten Paar von Elementen aus M ein eindeutig bestimmtes Element von M zuordnet.

Anmerkung: Eine Abbildung $f: M^n \rightarrow M$ (für $n \in \mathbf{N}$) heißt **n-stellige Operation** auf M .

Beispiele:

Aus zwei reellen Zahlen a, b kann man die Summe $a+b$ oder das Produkt ab erzeugen.

Aus zwei Elementen M, N der Potenzmenge einer Menge X kann man ihre Vereinigung $M \cup N$ oder ihren Durchschnitt $M \cap N$ erzeugen.

Assoziativgesetz

Gegeben sei (M, \circ) , also eine nichtleere Menge M mit einer binären Operation \circ .

(AG) Assoziativgesetz

(M, \circ) heißt **assoziativ**, wenn für alle $a, b, c \in M$ gilt:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

(d.h., es kommt nicht auf das Setzen der Klammern an)

Beispiel: In $(\mathbf{N}, +)$ gilt das Assoziativgesetz:

$$(1 + 4) + 3 = 1 + (4 + 3)$$

Kommutativgesetz

Gegeben sei (M, \circ) , also eine nichtleere Menge M mit einer binären Operation \circ .

(KG) **Kommutativgesetz**

(M, \circ) heißt **kommutativ**, wenn für alle $a, b \in M$ gilt:

$$a \circ b = b \circ a$$

(d.h., es kommt nicht auf die Reihenfolge an)

Beispiel: In $(\mathbf{N}, +)$ gilt das Kommutativgesetz:

$$1 + 3 = 1 + 3$$

Neutrales Element

Gegeben sei (M, \circ) , also eine nichtleere Menge M mit einer binären Operation \circ .

(NE) Neutrales Element

Ein Element $e \in M$ mit

$$e \circ a = a \circ e = a \quad \text{für alle } a \in M$$

heißt **neutrales Element**.

Beispiel: Das neutrale Element von $(\mathbf{N}, +)$ ist 0.

Inverses Element

Gegeben sei (M, \circ) , also eine nichtleere Menge M mit einer binären Operation \circ .

(IE) Inverses Element

Gibt es in (M, \circ) mit neutralem Element zu jedem $a \in M$ (mindestens) ein $b \in M$ mit

$$a \circ b = b \circ a = e,$$

so heißt b ein **inverses Element** zu a
(man sagt auch: a ist **invertierbar**).

Beispiel: In (\mathbf{Z}, \cdot) sind genau 1 und -1 invertierbar,
in (\mathbf{Q}, \cdot) alle Elemente.

Distributivgesetz

(DG) Distributivgesetz

Seien $+$ und \circ binäre Operationen auf M , $M \neq \{\}$.

Gilt in $(M, +, \circ)$ für alle $a, b, c \in M$

$$a \circ (b + c) = (a \circ b) + (a \circ c) \text{ und}$$

$$(b + c) \circ a = (b \circ a) + (c \circ a),$$

so heißt \circ **distributiv** bezüglich $+$.

Beispiel: In $(\mathbf{N}, +, \cdot)$ ist die gewöhnliche Multiplikation distributiv bezüglich der gewöhnlichen Addition:

$$2 \cdot (3+4) = (2 \cdot 3) + (2 \cdot 4) \text{ bzw.}$$

$$(3+4) \cdot 2 = (3 \cdot 2) + (4 \cdot 2)$$

Algebraische Strukturen: Gruppen

Gegeben sei (M, \circ) , also eine nichtleere Menge M mit einer binären Operation \circ ; (M, \circ) mit genau einer binären Operation \circ nennt man auch **Gruppoid**.

(M, \circ) heißt

- **Halbgruppe**, wenn (M, \circ) assoziativ ist;
- **kommutative Halbgruppe**, wenn (M, \circ) assoziativ und kommutativ ist;
- **Monoid**, wenn (M, \circ) assoziativ ist und ein neutrales Element hat;
- **Gruppe**, wenn (M, \circ) assoziativ ist, ein neutrales Element hat und jedes Element invertierbar ist;
- **kommutative Gruppe**, wenn (M, \circ) eine Gruppe und überdies kommutativ ist.

Algebraische Strukturen: Ring, Körper

Eine nichtleere Menge M ($M \neq \{\}$) mit zwei binären Operationen $+$ und \cdot ($M, +, \cdot$) heißt **Ring**, wenn gilt:

- $(M, +)$ ist eine **kommutative Gruppe**,
- (M, \cdot) ist eine **Halbgruppe**,
- \cdot ist **distributiv** bezüglich $+$.

Ist (M, \cdot) sogar eine kommutative Halbgruppe, so heißt auch der Ring $(M, +, \cdot)$ **kommutativ**.

Ein kommutativer Ring $(M, +, \cdot)$ mit Einheitselement heißt **Körper**, wenn zusätzlich gilt, dass jedes Element aus $M \setminus \{0\}$ invertierbar bezüglich \cdot ist.

$(M \setminus \{0\}, \cdot)$ ist also eine Gruppe, wobei 0 das neutrale Element bezüglich $+$ in $(M, +, \cdot)$ bezeichnet).

Algebraische Strukturen: Semiring

$(M, +, \cdot, 0, 1)$ heißt **Halbring** (oder **Semiring**), wenn gilt:

- $(M, +, 0)$ ist ein **kommutatives Monoid** (das neutrale Element bezeichnen wir mit 0);
- $(M, \cdot, 1)$ ist ein **Monoid** (mit Einheitsselement $1 \neq 0$);
- \cdot ist **distributiv** bezüglich $+$;
- $a \cdot 0 = 0 \cdot a = 0$ für alle $a \in M$.

Beweise

Ein Beweis ist ein überzeugendes logisches Argument, dass eine Aussage wahr ist.

Beweis durch Konstruktion

Viele Sätze behaupten die Existenz von bestimmten Typen von Objekten. Ein Weg, solche Sätze zu beweisen, besteht darin, zu zeigen, wie man diese Objekte konstruiert.

Indirekter Beweis (Beweis durch Widerspruch)

Wir nehmen an, dass der Satz wahr ist, und zeigen dann, dass diese Annahme zu einer offensichtlich falschen Konsequenz, einem Widerspruch, führt.

Beweise

CARL FRIEDRICH GAUSS (1777-1855)



Die Lehrer von Gauss waren sehr erstaunt, als dieser bereits im Alter von sieben Jahren die Zahlen von 1 bis 100 im Handumdrehen summieren konnte.

Er erkannte nämlich sofort, dass diese Summe aus 50 Zahlenpaaren bestand, die jeweils 101 ergaben.

Beweise: Induktion

Um eine Aussage $A(n)$ für alle $n \in \mathbf{N}$ (bzw. für alle $n \in \mathbf{N}_k$) zu beweisen: ($A(n)$ hängt von der ganzen Zahl $n \geq k$ ab.)

Induktionsbasis:

$A(m)$ ist für $m = k$ richtig.

Induktionshypothese:

Nehme an, $A(m)$ gilt für $m = n$.

Induktionsbehauptung:

Zeige, $A(m)$ gilt dann auch für $m = n+1$.

Induktionsprinzip:

Dann ist die Aussage $A(m)$ für alle $m \geq k$ richtig.

Beweise: Induktion

Beispiel:

Aussage: für alle positiven natürlichen Zahlen gilt

$$1+2+\dots+n = (n(n+1))/2$$

Induktionsbasis:

A(n) ist offensichtlich für $n = 1$ richtig: $1 = (1 \cdot 2)/2$

Induktionshypothese:

$1 + 2 + \dots + n = (n(n+1))/2$ Umformen ergibt:

Induktionsbehauptung:

$$1 + 2 + \dots + n + n + 1 = ((n + 1)(n + 1 + 1))/2$$

Einsetzen und Umformen ergibt:

$$\begin{aligned} 1 + 2 + \dots + n + n + 1 &= (n(n+1))/2 + n + 1 = \\ (n+1)((n/2)+1) &= (n+1)((n+2)/2) = ((n + 1)(n + 1 + 1))/2 \end{aligned}$$

Somit haben wir mittels **Induktion** bewiesen:

$1+2+\dots+n = (n(n+1))/2$ gilt für alle natürlichen Zahlen $n \geq 1$.

Beweise: Generalisierung

Kann man für eine beliebige natürlich Zahl $n (\geq k)$ zeigen, dass die Aussage $A(n)$ gilt, dann gilt sie für alle natürlichen Zahlen $n (\geq k)$.

Beispiel: Es gibt beliebig große Primzahlücken.

Wir nehmen eine beliebige natürlich Zahl $n \geq 1$ und zeigen, dass es $n-1$ aufeinanderfolgende Zahlen gibt, die alle keine Primzahlen sind: Betrachte

$n! + k$ für $k = 2, \dots, n$

Klarerweise gilt $k/(n!+k)$, da k ein Faktor von $n!$ ist. q.e.d.

Mächtigkeit von Mengen

Zwei Mengen A und B heißen **gleichmächtig**, wenn es eine bijektive Abbildung von A nach B gibt.

Jede Menge, die gleichmächtig mit **N** ist, heißt eine **abzählbare** Menge.

Jede unendliche, nicht abzählbare Menge heißt **überabzählbar**.

Beispiel:

Die Menge aller reellen Zahlen ist gleichmächtig mit der Menge der reellen Zahlen in jedem beliebigen Intervall $(a,b) = \{ x \mid x \text{ reell und } a < x < b \}$.

Beide Mengen sind nicht abzählbar.

Diagonalverfahren

Sei $M = \{0,1\}^{\mathbf{N}}$ die Menge aller Funktionen $f: \mathbf{N} \rightarrow \{0,1\}$.
Dann ist M nicht abzählbar.

Cantorsches Diagonalverfahren

Angenommen, es gibt eine bijektive Funktion $g: \mathbf{N} \rightarrow M$.
Sei dann die Funktion $h: \mathbf{N} \rightarrow \{0,1\}$ folgendermaßen
definiert: $h(n) = ([g(n)](n) + 1 \pmod{2})$, i.e.,

$$h(n) = \begin{cases} 1 & \text{falls } [g(n)](n) = 0 \\ 0 & \text{falls } [g(n)](n) = 1 \end{cases}$$

Dann ist h eine Funktion von \mathbf{N} in $\{0,1\}$, die somit in M
sein müsste, allerdings wurde h so definiert, dass für kein
 $n \in \mathbf{N}$ $h = g(n)$ sein kann, denn für jedes $n \in \mathbf{N}$ gilt
 $h(n) \neq [g(n)](n)$, was aber $h \notin M$ bedeutet.

Somit ergibt sich aber ein Widerspruch zur Annahme,
dass die Menge M abgezählt werden kann.

Cantorsches Diagonalverfahren

	$g(1)$ $\neq h$	$g(2)$ $\neq h$...	$g(n)$ $\neq h$...
1	$[g(1)](1)$ $\neq h(1)$	$[g(2)](1)$...	$[g(n)](1)$...
2	$[g(1)](2)$	$[g(2)](2)$ $\neq h(2)$...	$[g(n)](2)$...
...
n	$[g(1)](n)$	$[g(2)](n)$...	$[g(n)](n)$ $\neq h(n)$...
...

Folgerung

Sei A eine abzählbar unendliche Menge. Dann ist 2^A überabzählbar.

Sei $A = \{x_n \mid n \in \mathbf{N}\}$ und für jede Teilmenge $M \subseteq A$ die Funktion $\chi_M: \mathbf{N} \rightarrow \{0,1\}$ durch
 $\chi_M = 0$, falls $x_n \notin M$ und
 $\chi_M = 1$, falls $x_n \in M$,
definiert; χ_M ist die *charakteristische Funktion* von M bezüglich A . Dann ist durch $g: 2^A \rightarrow \{0,1\}^{\mathbf{N}}$ mit $g(m) = \chi_M$ eine bijektive Abbildung zwischen 2^A und $\{0,1\}^{\mathbf{N}}$ definiert und 2^A nach dem vorigen Satz somit ebenfalls überabzählbar. \square

Formale Sprachen

AXEL THUE (1863 - 1922)



„The further removed from usefulness or practical application the more important“

1906: Über unendliche Zeichenreihen.

Norske Vid. Selsk. Skr., I Mat. Nat. Kl., Kristiana 7, 1-22

Symbole und Wörter

Ein **Alphabet** ist eine endliche Menge von **Symbolen**.

z.B.: $\Sigma_1 = \{0,1\}$
 $\Sigma_2 = \{a,\dots,z\}$
 $\Sigma_3 = \{0,1,a,b,c\}$

Ein **Wort** über einem Alphabet ist eine endliche Folge von Symbolen über diesem Alphabet.

z.B.: 01001 ist ein Wort über Σ_1
abbab ist ein Wort über Σ_2

Wörter

Ist w ein Wort über Σ , dann ist die **Länge von w** , in Zeichen $|w|$, die Anzahl der Symbole, die w enthält.

z.B.: $\Sigma = \{0,1\}$ $w = 0101$ $|w| = 4$

Hat ein Wort w über Σ die Länge n , dann schreiben wir $w = a_1a_2\dots a_n$ wobei jedes $a_i \in \Sigma$.

Das Wort mit der Länge 0 heißt **Leerwort**, geschrieben ε d.h. $|\varepsilon| = 0$.

Konkatenation, Potenzbildung - Wörter

Haben wir ein Wort x der Länge n und ein Wort y der Länge m , dann ist die **Konkatenation** von x und y das Wort, das man durch Hintereinanderschreiben von x und y erhält:

$$x \cdot y = xy \quad |xy| = n+m$$

Achtung: $x \cdot y \neq y \cdot x$

Um ein Wort mit sich selbst mehrere Male zu verketteten, benützen wir folgende Notation (**Potenzbildung**):

$$w^k = \underbrace{w \cdot w \cdot \dots \cdot w}_k$$
$$w^0 = \varepsilon \quad w^n = w \cdot w^{n-1}$$

Formale Sprache

Σ^* ist die Menge aller Wörter (inklusive ε) über Σ

$$\Sigma^+ = \Sigma^* - \{\varepsilon\}$$

Eine **formale Sprache** ist eine beliebige Teilmenge L von Σ^* .

$$L \subseteq \Sigma^*$$

Es gilt:

$$\Sigma^* = \bigcup_{n \in \mathbf{N}} \Sigma^n \quad \text{wobei} \quad \Sigma^n = \{x_1 x_2 \dots x_n \mid x_i \in \Sigma \text{ und } 0 \leq i \leq n\}$$

$$\Sigma^+ = \bigcup_{n \in \mathbf{N}_1} \Sigma^n$$

Präfix, Teilwort, Suffix

Sei $w \in \Sigma^*$ und $w = xuy$ für Wörter $x, u, y \in \Sigma^*$.
Dann heißt x **Präfix**, u **Teilwort** und y **Suffix** von w .

Für $w \in \Sigma^*$ und $a \in \Sigma$ bezeichnen wir mit $|w|_a$ die **Anzahl** der Symbole a in w .

Sei $w = a_1a_2 \dots a_{n-1}a_n$ aus Σ^* . Dann ist $w^r = a_n a_{n-1} \dots a_2a_1$ das **Spiegelbild** von w .

Ein Wort $w \in \Sigma^*$ heißt **Palindrom**, wenn $w = w^r$ gilt.

Operationen auf Sprachen

Erweiterung der Konkatenation und Potenzbildung auf Sprachen:

Konkatenation von Sprachen A, B:

$$A \cdot B = \{ x \cdot y \mid x \in A, y \in B \}$$

Achtung: Konkatenation ist nicht kommutativ!

Potenzbildung einer Sprache A:

$$A^0 = \{ \varepsilon \} \qquad A^n = A \cdot A^{n-1} \quad \text{für } n \geq 1$$

$$A^* = \bigcup_{n \in \mathbf{N}} A^n$$

$$A^+ = \bigcup_{n \in \mathbf{N}_1} A^n$$

Operationen auf Sprachen - Beispiel

Seien A und B Sprachen.

Vereinigung: $A \cup B = \{ x \mid x \in A \text{ oder } x \in B \}$

Konkatenation: $A \cdot B = \{ x \cdot y \mid x \in A \text{ und } y \in B \}$

Stern: $A^* = \{ x_1 x_2 \dots x_k \mid x_i \in A \text{ und } 0 \leq i \leq k \}$

Beispiel:

$\Sigma = \{a, b, \dots, z\}$.

Wenn $A = \{ \text{good, bad} \}$ und $B = \{ \text{girl, boy} \}$ dann ist

$A \cup B = \{ \text{good, bad, boy, girl} \}$

$A \cdot B = \{ \text{goodgirl, goodboy, badgirl, badboy} \}$

$A^* = \{ \epsilon, \text{good, bad, goodgood, goodbad, badgood, badbad, goodgoodgood, goodgoodbad, goodbadgood, goodbadbad, ...} \}$

Eigenschaften von Sprachoperationen

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \quad \text{Assoziativität von } \cdot$$

$$A \cdot (B \cup C) = A \cdot B \cup A \cdot C \quad \text{Distributivität von } \cdot$$

$$(B \cup C) \cdot A = B \cdot A \cup C \cdot A \quad \text{Distributivität von } \cdot$$

$$\{\epsilon\} \cdot A = A$$

$$\{\} \cdot A = \{\}$$

$$A \cdot \{\epsilon\} = A$$

$$A \cdot \{\} = \{\}$$

$$(A \cup \{\epsilon\})^* = A^*$$

$$(A^*)^* = A^*$$

$$A \cdot A^* = A^+$$

$$A^* \cdot A = A^+$$

$$A^+ \cup \{\epsilon\} = A^*$$

Eigenschaften von Sprachoperationen

Die Menge der formalen Sprachen über einem Alphabet bildet daher einen nicht-kommutativen Semiring mit der Vereinigung als Addition und dem neutralen Element $\{ \}$ sowie mit der Konkatenation als Multiplikation und dem Einheitselement $\{\varepsilon\}$.

Abgeschlossenheit

Sind eine Menge B und Operatoren auf Teilmengen von B gegeben, so kann man sich natürlich fragen, ob die Anwendung der Operatoren auf diese Teilmengen von B wieder Teilmengen von B ergibt.

Sei B eine Menge und $f: B^n \rightarrow B$ eine Funktion. Eine Menge $A \subseteq B$ heißt **abgeschlossen** unter f , wenn gilt: aus $x_1, \dots, x_n \in A$ folgt $f(x_1, \dots, x_n) \in A$

Beispiel:

\mathbf{N} ist abgeschlossen unter Addition, aber nicht unter Subtraktion.

Induktive Definition

Schema der **induktiven Definition**:

A ist die kleinste Menge für die gilt:

(1) $A_0 \in A$

(2) Wenn $x_1, \dots, x_n \in A$, dann $f(x_1, \dots, x_n) \in A$.

Komponenten: **Grundmenge**, **Abschlusseigenschaft**,
Minimalitätsbedingung

Induktive Definition: Beispiel

Beispiel:

Die Menge der Palindrome ist die kleinste Menge, für die gilt:

- (1) ε ist ein Palindrom.
- (2) Für jedes Symbol a ist a ein Palindrom.
- (3) Ist a ein Symbol und x ein Palindrom dann ist auch axa ein Palindrom.

Beispiel:

Die Menge der wohlgeformten Klammerausdrücke (WKA) über dem Alphabet $\{ [,] \}$ ist die kleinste Menge, für die gilt:

- (1) ε ist ein WKA.
- (2) Ist w ein WKA, dann ist auch $[w]$ ein WKA.
- (3) Sind w und v WKA, dann ist auch wv ein WKA.

Induktive Definition: Reguläre Mengen

Die Menge $L_{\text{reg}}(\Sigma)$ **regulärer Mengen** über Σ ist die kleinste Menge, sodass

- (1) $\emptyset, \{a\} \in L_{\text{reg}}(\Sigma)$ für alle $a \in \Sigma$.
- (2) Wenn A und $B \in L_{\text{reg}}(\Sigma)$, dann sind auch
 $A \cup B, AB, A^* \in L_{\text{reg}}(\Sigma)$.

Möglichkeiten und Grenzen

Sei Σ ein beliebiges Alphabet.

Σ^* ist abzählbar.

2^{Σ^*} ist überabzählbar.

Es bleibt nur zu zeigen, dass Σ^* abzählbar ist.

Aber Σ^n ist für jedes $n \in \mathbf{N}$ endlich:

$\text{card}(\Sigma^0) = \text{card}(\epsilon) = 1$; für $n > 0$ gilt: $\text{card}(\Sigma^n) = (\text{card}(\Sigma))^n$

Folgerung

Die Menge aller formaler Sprachen $L \subseteq \Sigma^*$ ist also überabzählbar, die Menge $L_{\text{reg}}(\Sigma)$ regulärer Mengen (Sprachen) hingegen ist abzählbar.

(D.h., „fast alle“ Sprachen sind nicht regulär!)