WS 2003/04

Diskrete Strukturen I

Ernst W. Mayr

mayr@in.tum.de
Institut für Informatik
Technische Universität München

10-28-2003

Die *Groß-O-Notation* der Algorithmenanalyse von D. E. Knuth wurde von Paul Bachmann (Münster) entwickelt und von Edmund Landau (1877–1938) in seinen Arbeiten verbreitet.

Definition (Groß-O-Notation)

- $f(n)$ ist $O\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\exists c > 0,\ n_0 \in \mathbb{N}$, so dass

$$(\forall n \geq n_0) \quad \big[|f(n)| \leq c \cdot |g(n)|\big]$$

"f wächst bis auf einen konstanten Faktor nicht schneller als g"

- $f(n)$ ist $o\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\forall\ c > 0\ \exists\ n_0 \in \mathbb{N}$, so dass

$$(\forall n \geq n_0) \quad \big[|f(n)| < c \cdot |g(n)|\big]$$

"f wächst echt langsamer als g"

Die *Groß-O-Notation* der Algorithmenanalyse von D. E. Knuth wurde von Paul Bachmann (Münster) entwickelt und von Edmund Landau (1877–1938) in seinen Arbeiten verbreitet.

Definition (Groß-O-Notation)

- $f(n)$ ist $O\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\exists c > 0,\ n_0 \in \mathbb{N}$, so dass
  $$(\forall n \geq n_0) \quad \big[|f(n)| \leq c \cdot |g(n)|\big]$$
  "*f wächst bis auf einen konstanten Faktor nicht schneller als g*"
- $f(n)$ ist $o\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\forall\ c > 0\ \exists\ n_0 \in \mathbb{N}$, so dass
  $$(\forall n \geq n_0) \quad \big[|f(n)| < c \cdot |g(n)|\big]$$
  "*f wächst echt langsamer als g*"

- $f(n)$ ist $\Omega\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\exists c > 0$, $n_0 \in \mathbb{N}$, so dass

$$(\forall n \geq n_0) \quad \big[|f(n)| \geq c \cdot |g(n)|\big]$$

"*f wächst bis auf einen konstanten Faktor nicht langsamer als g*"

- $f(n)$ ist $\omega\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\forall\, c > 0\ \exists\, n_0 \in \mathbb{N}$, so dass

$$(\forall n \geq n_0) \quad \big[|f(n)| > c \cdot |g(n)|\big]$$

"*f wächst echt schneller als g*"

- $f(n)$ ist $\Theta\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn

$$f(n) \text{ ist } O\big(g(n)\big) \text{ und } f(n) \text{ ist } \Omega\big(g(n)\big)$$

"*f wächst (bis auf konstante Faktoren) genauso schnell wie g*"

- $f(n)$ ist $\Omega\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\exists c > 0,\ n_0 \in \mathbb{N}$, so dass

$$(\forall n \geq n_0) \quad \big[|f(n)| \geq c \cdot |g(n)|\big]$$

"*f wächst bis auf einen konstanten Faktor nicht langsamer als g*"

- $f(n)$ ist $\omega\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\forall\ c > 0\ \exists\ n_0 \in \mathbb{N}$, so dass

$$(\forall n \geq n_0) \quad \big[|f(n)| > c \cdot |g(n)|\big]$$

"*f wächst echt schneller als g*"

- $f(n)$ ist $\Theta\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn

$$f(n) \text{ ist } O\big(g(n)\big) \text{ und } f(n) \text{ ist } \Omega\big(g(n)\big)$$

"*f wächst (bis auf konstante Faktoren) genauso schnell wie g*"

- $f(n)$ ist $\Omega\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\exists c > 0$, $n_0 \in \mathbb{N}$, so dass

$$(\forall n \geq n_0) \quad \big[|f(n)| \geq c \cdot |g(n)|\big]$$

"*f wächst bis auf einen konstanten Faktor nicht langsamer als g*"

- $f(n)$ ist $\omega\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn $\forall\ c > 0\ \exists\ n_0 \in \mathbb{N}$, so dass

$$(\forall n \geq n_0) \quad \big[|f(n)| > c \cdot |g(n)|\big]$$

"*f wächst echt schneller als g*"

- $f(n)$ ist $\Theta\big(g(n)\big)$ (für $n \to \infty$) genau dann, wenn

$$f(n) \text{ ist } O\big(g(n)\big) \text{ und } f(n) \text{ ist } \Omega\big(g(n)\big)$$

"*f wächst (bis auf konstante Faktoren) genauso schnell wie g*"

- $f(n)$ ist $\Omega_\infty(g(n))$ genau dann, wenn $\exists\ c > 0$, so dass für unendlich viele $n \in \mathbb{N}$

$$|f(n)| \geq c \cdot |g(n)|$$

- $f(n)$ ist $\omega_\infty(g(n))$ genau dann, wenn $\forall\ c > 0$: $\exists$ unendlich viele $n \in \mathbb{N}$ mit

$$|f(n)| > c \cdot |g(n)|$$

Bemerkung: Man schreibt auch kürzer $f(n) \in O(g(n))$ oder (logisch unsauber) $f(n) = O(g(n))$. Oft werden nur Funktionen $\mathbb{N}_0 \to \mathbb{N}_0$ betrachtet (oder $\mathbb{N} \to \mathbb{N}_0$); dann sind die Absolutbeträge überflüssig. Manchmal werden auch Funktionen $\mathbb{R} \to \mathbb{R}$ oder das Verhalten für $x \to a$ betrachtet.

Achtung: Die Notation für Ω und Ω_∞ ist in der Literatur nicht eindeutig; im Zweifelsfall muss auf die jeweilige Definition geachtet werden!

- $f(n)$ ist $\Omega_\infty\big(g(n)\big)$ genau dann, wenn $\exists\ c > 0$, so dass für unendlich viele $n \in \mathbb{N}$

$$|f(n)| \geq c \cdot |g(n)|$$

- $f(n)$ ist $\omega_\infty\big(g(n)\big)$ genau dann, wenn $\forall\ c > 0$: $\exists$ unendlich viele $n \in \mathbb{N}$ mit

$$|f(n)| > c \cdot |g(n)|$$

Bemerkung: Man schreibt auch kürzer $f(n) \in O\big(g(n)\big)$ oder (logisch unsauber) $f(n) = O\big(g(n)\big)$. Oft werden nur Funktionen $\mathbb{N}_0 \to \mathbb{N}_0$ betrachtet (oder $\mathbb{N} \to \mathbb{N}_0$); dann sind die Absolutbeträge überflüssig. Manchmal werden auch Funktionen $\mathbb{R} \to \mathbb{R}$ oder das Verhalten für $x \to a$ betrachtet.

Achtung: Die Notation für Ω und Ω_∞ ist in der Literatur nicht eindeutig; im Zweifelsfall muss auf die jeweilige Definition geachtet werden!

- $f(n)$ ist $\Omega_\infty\big(g(n)\big)$ genau dann, wenn $\exists\ c > 0$, so dass für unendlich viele $n \in \mathbb{N}$

$$|f(n)| \geq c \cdot |g(n)|$$

- $f(n)$ ist $\omega_\infty\big(g(n)\big)$ genau dann, wenn $\forall\ c > 0$: $\exists$ unendlich viele $n \in \mathbb{N}$ mit

$$|f(n)| > c \cdot |g(n)|$$

Bemerkung: Man schreibt auch kürzer $f(n) \in O\big(g(n)\big)$ oder (logisch unsauber) $f(n) = O\big(g(n)\big)$. Oft werden nur Funktionen $\mathbb{N}_0 \to \mathbb{N}_0$ betrachtet (oder $\mathbb{N} \to \mathbb{N}_0$); dann sind die Absolutbeträge überflüssig. Manchmal werden auch Funktionen $\mathbb{R} \to \mathbb{R}$ oder das Verhalten für $x \to a$ betrachtet.

Achtung: Die Notation für Ω und Ω_∞ ist in der Literatur nicht eindeutig; im Zweifelsfall muss auf die jeweilige Definition geachtet werden!

- $f(n)$ ist $\Omega_\infty\big(g(n)\big)$ genau dann, wenn $\exists\ c > 0$, so dass für unendlich viele $n \in \mathbb{N}$

$$|f(n)| \geq c \cdot |g(n)|$$

- $f(n)$ ist $\omega_\infty\big(g(n)\big)$ genau dann, wenn $\forall\ c > 0$: $\exists$ unendlich viele $n \in \mathbb{N}$ mit

$$|f(n)| > c \cdot |g(n)|$$

Bemerkung: Man schreibt auch kürzer $f(n) \in O\big(g(n)\big)$ oder (logisch unsauber) $f(n) = O\big(g(n)\big)$. Oft werden nur Funktionen $\mathbb{N}_0 \to \mathbb{N}_0$ betrachtet (oder $\mathbb{N} \to \mathbb{N}_0$); dann sind die Absolutbeträge überflüssig. Manchmal werden auch Funktionen $\mathbb{R} \to \mathbb{R}$ oder das Verhalten für $x \to a$ betrachtet.

Achtung: Die Notation für Ω und Ω_∞ ist in der Literatur nicht eindeutig; im Zweifelsfall muss auf die jeweilige Definition geachtet werden!

Beispiel:

Behauptung: $n! \in O(n^n)$

Beweis.

$$(\forall n \in \mathbb{N})\left[n! = n(n-1)\cdots 2 \cdot 1 \le 1 \cdot n^n\right]$$

$\square$

Beispiel:

Behauptung: $\log n! \in O(n \log n)$

Beweis.

Beweis:

$(\forall n \in \mathbb{N})\left[\log n! = \log n + \log(n-1) + \ldots + \log 1 < 1 \cdot n \cdot \log n\right]$ $\square$

Beispiel:

Behauptung: $n! \in O(n^n)$

Beweis.

$$(\forall n \in \mathbb{N})\left[n! = n(n-1)\cdots 2\cdot 1 \le 1\cdot n^n\right]$$

$\square$

Beispiel:

Behauptung: $\log n! \in O(n \log n)$

Beweis.

Beweis:

$(\forall n \in \mathbb{N})\left[\log n! = \log n + \log(n-1) + \ldots + \log 1 < 1 \cdot n \cdot \log n\right]$ $\square$

Beispiel:

Behauptung: $n! \in O(n^n)$

Beweis.

$$(\forall n \in \mathbb{N})\left[n! = n(n-1)\cdots 2 \cdot 1 \leq 1 \cdot n^n\right]$$

$\square$

Beispiel:

Behauptung: $\log n! \in O(n \log n)$

Beweis.

Beweis:

$(\forall n \in \mathbb{N})\left[\log n! = \log n + \log(n-1) + \ldots + \log 1 < 1 \cdot n \cdot \log n\right]$ $\square$

Beispiel:

Behauptung: $n! \in O(n^n)$

Beweis.

$$(\forall n \in \mathbb{N})\left[n! = n(n-1)\cdots 2 \cdot 1 \le 1 \cdot n^n\ \right]$$

$\square$

Beispiel:

Behauptung: $\log n! \in O(n \log n)$

Beweis.

Beweis:

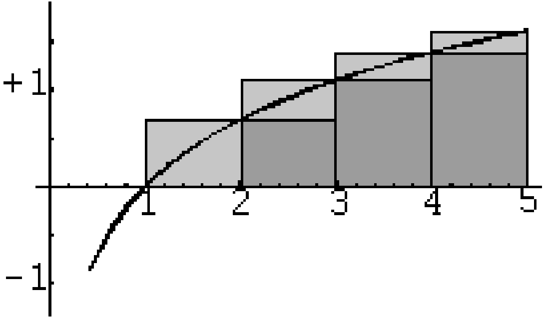
$(\forall n \in \mathbb{N})\left[\log n! = \log n + \log(n-1) + \ldots + \log 1 < 1 \cdot n \cdot \log n\right]$ $\square$

Beispiel

Behauptung: $n! = O\left((n+1) \cdot e \cdot \left(\frac{n}{e}\right)^n\right)$

Beweis:

$$(\forall n > 0)\left[\sum_{k=1}^{n-1} \ln k < \int_1^n \ln x \; dx < \sum_{k=2}^{n} \ln k < \int_1^{n+1} \ln x \; dx\right]$$

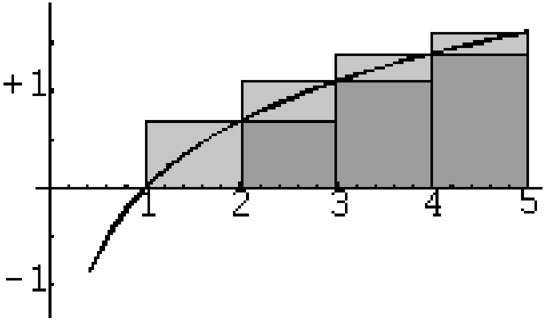


Beispiel

Behauptung: $n! = O\left((n+1)\cdot e\cdot \left(\frac{n}{e}\right)^n\right)$

Beweis:

$$(\forall n > 0)\left[\sum_{k=1}^{n-1}\ln k < \int_1^n \ln x\; dx < \sum_{k=2}^{n}\ln k < \int_1^{n+1}\ln x\; dx\right]$$



Es ist

$$\int_1^n \ln x \, dx = (x \cdot \ln x - x)\Big|_1^n = n \cdot \ln n - n + 1$$

und

$$\int_1^{n+1} \ln x \, dx = (n+1) \cdot \ln(n+1) - n$$

Also:

$$(\forall n \in \mathbb{N})\left[n \cdot \ln n - n + 1 < \ln n! < (n+1) \cdot \ln(n+1) - n\right]$$

und damit

$$\frac{n^n}{e^{n-1}} \le n! \le \frac{(n+1)^{n+1}}{e^n}$$

oder:

$$e \cdot \left(\frac{n}{e}\right)^n \le n! \le (n+1) \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{n}\right)^n \le (n+1) \cdot e \cdot \left(\frac{n}{e}\right)^n$$

q. e. d.

Es ist

$$\int_1^n \ln x \; dx = (x \cdot \ln x - x)\Big|_1^n = n \cdot \ln n - n + 1$$

und

$$\int_1^{n+1} \ln x \; dx = (n+1) \cdot \ln(n+1) - n$$

Also:

$$(\forall n \in \mathbb{N})\Big[n \cdot \ln n - n + 1 < \ln n! < (n+1) \cdot \ln(n+1) - n\Big]$$

und damit

$$\frac{n^n}{e^{n-1}} \leq n! \leq \frac{(n+1)^{n+1}}{e^n}$$

oder:

$$e \cdot \left(\frac{n}{e}\right)^n \leq n! \leq (n+1) \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{n}\right)^n \leq (n+1) \cdot e \cdot \left(\frac{n}{e}\right)^n$$

q. e. d.

Es ist

$$\int_1^n \ln x \; dx = (x \cdot \ln x - x)\Big|_1^n = n \cdot \ln n - n + 1$$

und

$$\int_1^{n+1} \ln x \; dx = (n+1) \cdot \ln(n+1) - n$$

Also:

$$(\forall n \in \mathbb{N})\Big[n \cdot \ln n - n + 1 < \ln n! < (n+1) \cdot \ln(n+1) - n\Big]$$

und damit

$$\frac{n^n}{e^{n-1}} \leq n! \leq \frac{(n+1)^{n+1}}{e^n}$$

oder:

$$e \cdot \left(\frac{n}{e}\right)^n \leq n! \leq (n+1) \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{n}\right)^n \leq (n+1) \cdot e \cdot \left(\frac{n}{e}\right)^n$$

q. e. d.

Die Stirling'sche Formel

$$\lim_{n\to\infty}\left(n!\Big/\sqrt{n}\cdot\left(\frac{n}{e}\right)^n\right)=\sqrt{2\pi}$$

oder mit anderen Worten:

$$n! = \sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^n\cdot(1+o(1))$$

Beispiel: Polynome: Sei

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0;\, a_i \in \mathbb{R},\ a_n \neq 0\,.$$

Behauptung: $f(x) = O(x^n)$

Die Stirling'sche Formel

$$\lim_{n\to\infty}\left(n!\Big/\sqrt{n}\cdot\left(\frac{n}{e}\right)^n\right)=\sqrt{2\pi}$$

oder mit anderen Worten:

$$n! = \sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^n\cdot(1+o(1))$$

Beispiel: Polynome: Sei

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0; a_i\in\mathbb{R},\ a_n\neq 0\ .$$

Behauptung: $f(x)=O(x^n)$

Die Stirling'sche Formel

Behauptung: $f(x) = O(x^n)$

Beweis.

$$\begin{aligned}\forall x \geq 1: \quad |f(x)| \quad &\leq \left|\sum_{i=0}^{n} a_i \cdot x^i\right| \leq \sum_{i=0}^{n} |a_i| \cdot x^i \\ &\leq x^n \cdot \left(\sum_{i=0}^{n} |a_i|\, x^{i-n}\right) \leq x^n \cdot \underbrace{\sum |a_i|}_{=:c}\end{aligned}$$

$\square$

Die Stirling'sche Formel

Behauptung: $f(x) = O(x^n)$

Beweis.

$$
\begin{aligned}
\forall x \geq 1: \quad |f(x)| &\leq \left| \sum_{i=0}^{n} a_i \cdot x^i \right| \leq \sum_{i=0}^{n} |a_i| \cdot x^i \\
&\leq x^n \cdot \left(\sum_{i=0}^{n} |a_i| \, x^{i-n} \right) \leq x^n \cdot \underbrace{\sum |a_i|}_{=:c}
\end{aligned}
$$

$\square$

Kapitel 2. Algebraische Grundlagen

Definition

Eine Algebra besteht aus einer Trägermenge S und einer Menge Φ von Operationen auf S (der Operatorenmenge). Dabei gilt: Jeder Operator ist eine (totale) Abbildung

$$S^m \to S$$

der Stelligkeit (Arität, arity) $m \in \mathbb{N}_0$.

Nullstellige Operatoren sind Konstanten, z. B. 0, 47, $\perp$.
Einstellige Operatoren sind unäre Operatoren, z. B. $x \mapsto 2^x$, $x \mapsto \neg x$, $A \mapsto 2^A$.
Zweistellige Operatoren sind binäre Operatoren, z. B. $(x, y) \mapsto \max\{x, y\}$, $(x, y) \mapsto \mathrm{ggT}(x, y)$, $(x, y) \mapsto x + y$.
Dreistellige Operatoren sind ternäre Operatoren, z. B. $(x, y, z) \mapsto$ **if** x **then** y **else** z **fi**

Kapitel 2. Algebraische Grundlagen

Definition

Eine Algebra besteht aus einer Trägermenge S und einer Menge Φ von Operationen auf S (der Operatorenmenge). Dabei gilt: Jeder Operator ist eine (totale) Abbildung

$$S^m \to S$$

der Stelligkeit (Arität, arity) $m \in \mathbb{N}_0$.

Nullstellige Operatoren sind Konstanten, z. B. 0, 47, $\perp$.
Einstellige Operatoren sind unäre Operatoren, z. B. $x \mapsto 2^x$, $x \mapsto \neg x$, $A \mapsto 2^A$.
Zweistellige Operatoren sind binäre Operatoren, z. B. $(x, y) \mapsto \max\{x, y\}$, $(x, y) \mapsto \mathrm{ggT}(x, y)$, $(x, y) \mapsto x + y$.
Dreistellige Operatoren sind ternäre Operatoren, z. B. $(x, y, z) \mapsto$ **if** x **then** y **else** z **fi**

Kapitel 2. Algebraische Grundlagen

Definition

Eine Algebra besteht aus einer Trägermenge S und einer Menge Φ von Operationen auf S (der Operatorenmenge). Dabei gilt: Jeder Operator ist eine (totale) Abbildung

$$S^m \to S$$

der Stelligkeit (Arität, arity) $m \in \mathbb{N}_0$.

Nullstellige Operatoren sind Konstanten, z. B. 0, 47, $\perp$.
Einstellige Operatoren sind unäre Operatoren, z. B. $x \mapsto 2^x$, $x \mapsto \neg x$, $A \mapsto 2^A$.
Zweistellige Operatoren sind binäre Operatoren, z. B. $(x, y) \mapsto \max\{x, y\}$, $(x, y) \mapsto \mathrm{ggT}(x, y)$, $(x, y) \mapsto x + y$.
Dreistellige Operatoren sind ternäre Operatoren, z. B. $(x, y, z) \mapsto$ **if** x **then** y **else** z **fi**

Kapitel 2. Algebraische Grundlagen

Definition

Eine Algebra besteht aus einer Trägermenge S und einer Menge Φ von Operationen auf S (der Operatorenmenge). Dabei gilt: Jeder Operator ist eine (totale) Abbildung

$$S^m \to S$$

der Stelligkeit (Arität, arity) $m \in \mathbb{N}_0$.

Nullstellige Operatoren sind Konstanten, z. B. 0, 47, $\perp$.
Einstellige Operatoren sind unäre Operatoren, z. B. $x \mapsto 2^x$, $x \mapsto \neg x$, $A \mapsto 2^A$.
Zweistellige Operatoren sind binäre Operatoren, z. B.
$(x, y) \mapsto \max\{x, y\}$, $(x, y) \mapsto \mathrm{ggT}(x, y)$, $(x, y) \mapsto x + y$.
Dreistellige Operatoren sind ternäre Operatoren, z. B.
$(x, y, z) \mapsto$ **if** x **then** y **else** z **fi**

Kapitel 2. Algebraische Grundlagen

Definition

Eine Algebra besteht aus einer Trägermenge S und einer Menge Φ von Operationen auf S (der Operatorenmenge). Dabei gilt: Jeder Operator ist eine (totale) Abbildung

$$S^m \to S$$

der Stelligkeit (Arität, arity) $m \in \mathbb{N}_0$.

Nullstellige Operatoren sind Konstanten, z. B. 0, 47, $\perp$.
Einstellige Operatoren sind unäre Operatoren, z. B. $x \mapsto 2^x$, $x \mapsto \neg x$, $A \mapsto 2^A$.
Zweistellige Operatoren sind binäre Operatoren, z. B. $(x, y) \mapsto \max\{x, y\}$, $(x, y) \mapsto \mathrm{ggT}(x, y)$, $(x, y) \mapsto x + y$.
Dreistellige Operatoren sind ternäre Operatoren, z. B.
$(x, y, z) \mapsto$ **if** x **then** y **else** z **fi**

Beispiel:

Sei U eine Menge, F die Menge der Funktionen von $U \to U$.
$(F, \circ)$ ist eine Algebra mit $\circ$ als Komposition von Funktionen.

Beispiel:

Boolesche Algebra:
$\langle\{T, F\}, \{\neg, \wedge, \vee\}\rangle$ ist eine (endliche) Algebra.

Beispiel:

Sei U eine Menge, F die Menge der Funktionen von $U \rightarrow U$.
$(F, \circ)$ ist eine Algebra mit $\circ$ als Komposition von Funktionen.

Beispiel:

Boolesche Algebra:
$\langle \{T, F\}, \{\neg, \wedge, \vee\} \rangle$ ist eine (endliche) Algebra.

Definition

Die Signatur einer Algebra besteht aus der Liste der Stelligkeiten der Operatoren.

Beispiel: $\langle \mathbb{B}, \{\neg, \wedge, \vee\}\rangle$ (Boolesche Algebra): 1, 2, 2

$$\begin{array}{lcccc} \neg & : & \mathbb{B} & \to & \mathbb{B} \\ \wedge & : & \mathbb{B}\times\mathbb{B} & \to & \mathbb{B} \\ \vee & : & \mathbb{B}\times\mathbb{B} & \to & \mathbb{B} \end{array}$$

$\langle 2^U, \{\bar{\ }, \cap, \cup\}\rangle$ (2^U: Potenzmenge von U): 1, 2, 2

$$\begin{array}{lccl} \bar{\ } & : & 2^U & \to 2^U \\ \cap & : & 2^U \times 2^U & \to 2^U \\ \cup & : & 2^U \times 2^U & \to 2^U \end{array}$$

Diese beiden Algebren haben dieselbe Signatur; die Trägermenge ist unwesentlich, es kommt nur auf die Reihenfolge der Stelligkeiten an.

Definition

Die Signatur einer Algebra besteht aus der Liste der Stelligkeiten der Operatoren.

Beispiel: $\langle \mathbb{B}, \{\neg, \wedge, \vee\}\rangle$ (Boolesche Algebra): 1, 2, 2

$$\begin{array}{ccccc} \neg & : & \mathbb{B} & \to & \mathbb{B} \\ \wedge & : & \mathbb{B}\times\mathbb{B} & \to & \mathbb{B} \\ \vee & : & \mathbb{B}\times\mathbb{B} & \to & \mathbb{B} \end{array}$$

$\langle 2^U, \{\bar{~}, \cap, \cup\}\rangle$ (2^U: Potenzmenge von U): 1, 2, 2

$$\begin{array}{ccccc} \bar{~} & : & 2^U & \to & 2^U \\ \cap & : & 2^U\times 2^U & \to & 2^U \\ \cup & : & 2^U\times 2^U & \to & 2^U \end{array}$$

Diese beiden Algebren haben dieselbe Signatur; die Trägermenge ist unwesentlich, es kommt nur auf die Reihenfolge der Stelligkeiten an.

Definition

Die Signatur einer Algebra besteht aus der Liste der Stelligkeiten der Operatoren.

Beispiel: $\langle \mathbb{B}, \{\neg, \wedge, \vee\} \rangle$ (Boolesche Algebra): 1, 2, 2

$$\begin{array}{ccccc} \neg & : & \mathbb{B} & \to & \mathbb{B} \\ \wedge & : & \mathbb{B} \times \mathbb{B} & \to & \mathbb{B} \\ \vee & : & \mathbb{B} \times \mathbb{B} & \to & \mathbb{B} \end{array}$$

$\langle 2^U, \{\bar{\ }, \cap, \cup\} \rangle$ (2^U: Potenzmenge von U): 1, 2, 2

$$\begin{array}{cccc} \bar{\ } & : & 2^U & \to 2^U \\ \cap & : & 2^U \times 2^U & \to 2^U \\ \cup & : & 2^U \times 2^U & \to 2^U \end{array}$$

Diese beiden Algebren haben dieselbe Signatur; die Trägermenge ist unwesentlich, es kommt nur auf die Reihenfolge der Stelligkeiten an.

Definition

Die Signatur einer Algebra besteht aus der Liste der Stelligkeiten der Operatoren.

Beispiel: $\langle\mathbb{B}, \{\neg, \wedge, \vee\}\rangle$ (Boolesche Algebra): 1, 2, 2

$$\begin{array}{ccccc} \neg & : & \mathbb{B} & \rightarrow & \mathbb{B} \\ \wedge & : & \mathbb{B}\times\mathbb{B} & \rightarrow & \mathbb{B} \\ \vee & : & \mathbb{B}\times\mathbb{B} & \rightarrow & \mathbb{B} \end{array}$$

$\langle 2^U, \{^-, \cap, \cup\}\rangle$ (2^U: Potenzmenge von U): 1, 2, 2

$$\begin{array}{ccccc} ^- & : & 2^U & \rightarrow & 2^U \\ \cap & : & 2^U\times 2^U & \rightarrow & 2^U \\ \cup & : & 2^U\times 2^U & \rightarrow & 2^U \end{array}$$

Diese beiden Algebren haben dieselbe Signatur; die Trägermenge ist unwesentlich, es kommt nur auf die Reihenfolge der Stelligkeiten an.

Sei $\langle S, \circ \rangle$ eine Algebra, $\circ$ beliebiger zweistelliger Operator.

Definition

- Ein Element $1 \in S$ heißt linkes (bzw. rechtes) Einselement für den Operator $\circ$, falls

$$(\forall a \in S) \quad 1 \circ a = a \text{ (bzw. } a \circ 1 = a)$$

  1 heißt Einselement, falls es linkes und rechtes Einselement ist.

- Ein Element $0 \in S$ heißt linkes (bzw. rechtes) Nullelement für den Operator $\circ$, falls

$$(\forall a \in S) \quad 0 \circ a = 0 \text{ (bzw. } a \circ 0 = 0)$$

  0 heißt Nullelement, falls es linkes und rechtes Nullelement ist.

- Sei 1 Einselement. Für $a \in S$ heißt $a^{-1} \in S$ Rechtsinverses von a, falls

$$a \circ a^{-1} = 1$$

  Analog: Linksinverses

Sei $\langle S, \circ \rangle$ eine Algebra, $\circ$ beliebiger zweistelliger Operator.

Definition

- Ein Element $1 \in S$ heißt linkes (bzw. rechtes) Einselement für den Operator $\circ$, falls

$$(\forall a \in S) \quad 1 \circ a = a \text{ (bzw. } a \circ 1 = a)$$

  1 heißt Einselement, falls es linkes und rechtes Einselement ist.

- Ein Element $0 \in S$ heißt linkes (bzw. rechtes) Nullelement für den Operator $\circ$, falls

$$(\forall a \in S) \quad 0 \circ a = 0 \text{ (bzw. } a \circ 0 = 0)$$

  0 heißt Nullelement, falls es linkes und rechtes Nullelement ist.

- Sei 1 Einselement. Für $a \in S$ heißt $a^{-1} \in S$ Rechtsinverses von a, falls

$$a \circ a^{-1} = 1$$

  Analog: Linksinverses

Sei $\langle S, \circ \rangle$ eine Algebra, $\circ$ beliebiger zweistelliger Operator.

Definition

- Ein Element $1 \in S$ heißt linkes (bzw. rechtes) Einselement für den Operator $\circ$, falls

$$(\forall a \in S) \quad 1 \circ a = a \text{ (bzw. } a \circ 1 = a)$$

  1 heißt Einselement, falls es linkes und rechtes Einselement ist.

- Ein Element $0 \in S$ heißt linkes (bzw. rechtes) Nullelement für den Operator $\circ$, falls

$$(\forall a \in S) \quad 0 \circ a = 0 \text{ (bzw. } a \circ 0 = 0)$$

  0 heißt Nullelement, falls es linkes und rechtes Nullelement ist.

- Sei 1 Einselement. Für $a \in S$ heißt $a^{-1} \in S$ Rechtsinverses von a, falls

$$a \circ a^{-1} = 1$$

  Analog: Linksinverses

Beispiel

Betrachte $F(U)$, d. h. die Menge aller Abbildungen $U \to U$. Dann gilt (mit der Komposition als Operator):

- $f \in F(U)$ hat genau dann ein Rechtsinverses, wenn f surjektiv ist.

  $$f \circ f^{-1} = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so daß gilt: $g(x)$ wird von f auf x abgebildet.)

- $f \in F(U)$ hat genau dann ein Linksinverses, wenn f injektiv ist.

  $$f^{-1} \circ f = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so dass gilt: $f(x)$ wird von g auf x abgebildet.)

Ist f bijektiv, dann stimmen die beiden f^{-1} aus (1) und (2) überein.

Beispiel

Betrachte $F(U)$, d. h. die Menge aller Abbildungen $U \to U$. Dann gilt (mit der Komposition als Operator):

- $f \in F(U)$ hat genau dann ein Rechtsinverses, wenn f surjektiv ist.

  $$f \circ f^{-1} = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so daß gilt: $g(x)$ wird von f auf x abgebildet.)

- $f \in F(U)$ hat genau dann ein Linksinverses, wenn f injektiv ist.

  $$f^{-1} \circ f = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so dass gilt: $f(x)$ wird von g auf x abgebildet.)

Ist f bijektiv, dann stimmen die beiden f^{-1} aus (1) und (2) überein.

Beispiel

Betrachte $F(U)$, d. h. die Menge aller Abbildungen $U \rightarrow U$. Dann gilt (mit der Komposition als Operator):

- $f \in F(U)$ hat genau dann ein Rechtsinverses, wenn f surjektiv ist.

  $$f \circ f^{-1} = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so daß gilt: $g(x)$ wird von f auf x abgebildet.)

- $f \in F(U)$ hat genau dann ein Linksinverses, wenn f injektiv ist.

  $$f^{-1} \circ f = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so dass gilt: $f(x)$ wird von g auf x abgebildet.)

Ist f bijektiv, dann stimmen die beiden f^{-1} aus (1) und (2) überein.

Beispiel

Betrachte $F(U)$, d. h. die Menge aller Abbildungen $U \to U$. Dann gilt (mit der Komposition als Operator):

- $f \in F(U)$ hat genau dann ein Rechtsinverses, wenn f surjektiv ist.

  $$f \circ f^{-1} = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so daß gilt: $g(x)$ wird von f auf x abgebildet.)

- $f \in F(U)$ hat genau dann ein Linksinverses, wenn f injektiv ist.

  $$f^{-1} \circ f = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so dass gilt: $f(x)$ wird von g auf x abgebildet.)

Ist f bijektiv, dann stimmen die beiden f^{-1} aus (1) und (2) überein.

Satz

1 Falls c linkes Einselement ist und d rechtes Einselement (bezüglich des binären Operator $\circ$), dann ist

$$c = d\ .$$

Beweis.

$$d = c \circ d = c\ .$$

$\square$

Satz

1 Falls c linkes Einselement ist und d rechtes Einselement (bezüglich des binären Operator $\circ$), dann ist

$$c = d \, .$$

Beweis.

$$d = c \circ d = c \, .$$

$\square$

Satz

2 Falls c linkes Nullelement und d rechtes Nullelement (bezüglich $\circ$), dann ist

$$c = d\ .$$

Beweis.

$$c = c \circ d = d\ .$$

$\square$

Satz

2 Falls c linkes Nullelement und d rechtes Nullelement (bezüglich $\circ$), dann ist

$$c = d\,.$$

Beweis.

$$c = c \circ d = d\,.$$

$\square$

Beispiel

Betrachte $\langle\{b, c\}, \{\bullet\}\rangle$ mit

$\bullet$	b	c
b	b	b
c	c	c

Es gilt: b und c sind linke Nullelemente, und b und c sind rechte Einselemente.

2.1.2.3 Abgeschlossenheit

Definition

Sei $\langle S, \Phi \rangle$ eine Algebra, T eine Teilmenge von S.

- T ist unter den Operatoren in Φ abgeschlossen (stabil), falls ihre Anwendung auf Elemente aus T wieder Elemente aus T ergibt.
- $\langle T, \Phi \rangle$ heißt Unteralgebra von $\langle S, \Phi \rangle$, falls $T \neq \emptyset$ und T unter den Operatoren $\in \Phi$ abgeschlossen ist.

Beispiele:

- $\langle \mathbb{N}_0, + \rangle$ ist Unteralgebra von $\langle \mathbb{Z}, + \rangle$
- $\langle \{0, 1\}, \cdot \rangle$ ist Unteralgebra von $\langle \mathbb{N}_0, \cdot \rangle$
- $\langle \{0, 1\}, + \rangle$ ist keine Unteralgebra von $\langle \mathbb{Z}, + \rangle$, da sie nicht abgeschlossen ist $(1 + 1 = 2)$.

2.1.2.3 Abgeschlossenheit

Definition

Sei $\langle S, \Phi \rangle$ eine Algebra, T eine Teilmenge von S.

- T ist unter den Operatoren in Φ abgeschlossen (stabil), falls ihre Anwendung auf Elemente aus T wieder Elemente aus T ergibt.
- $\langle T, \Phi \rangle$ heißt Unteralgebra von $\langle S, \Phi \rangle$, falls $T \neq \emptyset$ und T unter den Operatoren $\in \Phi$ abgeschlossen ist.

Beispiele:

- $\langle \mathbb{N}_0, + \rangle$ ist Unteralgebra von $\langle \mathbb{Z}, + \rangle$
- $\langle \{0, 1\}, \cdot \rangle$ ist Unteralgebra von $\langle \mathbb{N}_0, \cdot \rangle$
- $\langle \{0, 1\}, + \rangle$ ist keine Unteralgebra von $\langle \mathbb{Z}, + \rangle$, da sie nicht abgeschlossen ist $(1 + 1 = 2)$.

2.1.2.3 Abgeschlossenheit

Definition

Sei $\langle S, \Phi \rangle$ eine Algebra, T eine Teilmenge von S.

- T ist unter den Operatoren in Φ abgeschlossen (stabil), falls ihre Anwendung auf Elemente aus T wieder Elemente aus T ergibt.
- $\langle T, \Phi \rangle$ heißt Unteralgebra von $\langle S, \Phi \rangle$, falls $T \neq \emptyset$ und T unter den Operatoren $\in \Phi$ abgeschlossen ist.

Beispiele:

- $\langle \mathbb{N}_0, + \rangle$ ist Unteralgebra von $\langle \mathbb{Z}, + \rangle$
- $\langle \{0, 1\}, \cdot \rangle$ ist Unteralgebra von $\langle \mathbb{N}_0, \cdot \rangle$
- $\langle \{0, 1\}, + \rangle$ ist keine Unteralgebra von $\langle \mathbb{Z}, + \rangle$, da sie nicht abgeschlossen ist $(1 + 1 = 2)$.

2.1.2.3 Abgeschlossenheit

Definition

Sei $\langle S, \Phi \rangle$ eine Algebra, T eine Teilmenge von S.

- T ist unter den Operatoren in Φ abgeschlossen (stabil), falls ihre Anwendung auf Elemente aus T wieder Elemente aus T ergibt.
- $\langle T, \Phi \rangle$ heißt Unteralgebra von $\langle S, \Phi \rangle$, falls $T \neq \emptyset$ und T unter den Operatoren $\in \Phi$ abgeschlossen ist.

Beispiele:

- $\langle \mathbb{N}_0, + \rangle$ ist Unteralgebra von $\langle \mathbb{Z}, + \rangle$
- $\langle \{0, 1\}, \ \cdot \ \rangle$ ist Unteralgebra von $\langle \mathbb{N}_0, \ \cdot \ \rangle$
- $\langle \{0, 1\}, + \rangle$ ist keine Unteralgebra von $\langle \mathbb{Z}, + \rangle$, da sie nicht abgeschlossen ist $(1 + 1 = 2)$.