4.9 Das Wachstumsverhalten von Funktionen

Die Groß-O-Notation wurde von D. E. Knuth in der Algorithmenanalyse eingeführt. Sie wurde ursprünglich von Paul Bachmann (1837–1920) entwickelt und von Edmund Landau (1877–1938) in seinen Arbeiten verbreitet.

Definition 39 (Groß-O-Notation)

- $f(n) \in \mathcal{O}\big(g(n)\big)$ (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“

- $f(n) \in o\big(g(n)\big)$ (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“

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

$$(\forall n \geq n_0)\ \big[|f(n)| \geq c \cdot g(n) \geq 0\big]$$

„f wächst bis auf einen konstanten Faktor nicht langsamer als g“

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

$$(\forall n \geq n_0)\ \big[|f(n)| > c \cdot g(n) \geq 0\big]$$

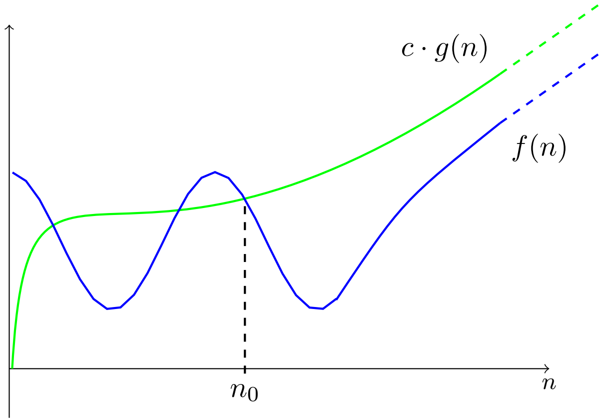
„f wächst echt schneller als g“

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

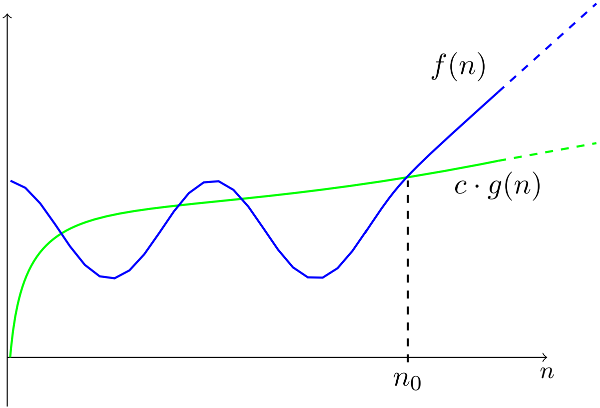
$$f(n) \in \mathcal{O}\big(g(n)\big) \text{ und } f(n) \in \Omega\big(g(n)\big)$$

„f wächst (bis auf konstante Faktoren) genauso schnell wie g“

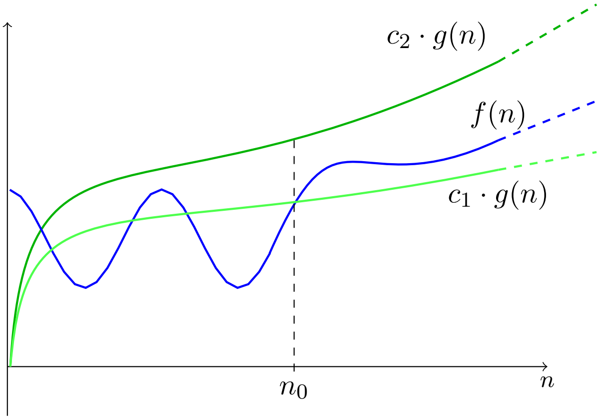
Graphische Darstellung von $\mathcal{O}$



Graphische Darstellung von ω



Graphische Darstellung von Θ



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

$$|f(n)| \geq c \cdot g(n) \geq 0\,.$$

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

$$|f(n)| > c \cdot g(n) \geq 0\,.$$

Bemerkungen:

1. Man schreibt oft, aber logisch unsauber $f(n) = \mathcal{O}(g(n))$.
2. Oft werden nur Funktionen $\mathbb{N}_0 \to \mathbb{N}_0$ betrachtet (oder $\mathbb{N} \to \mathbb{N}_0$); dann sind die Absolutbeträge überflüssig.
3. Manchmal werden auch Funktionen $\mathbb{R} \to \mathbb{R}$ oder das Verhalten für $x \to a$ betrachtet.
4. Achtung: Die Notation für Ω und Ω_∞ ist in der Literatur nicht eindeutig; im Zweifelsfall muss auf die jeweilige Definition geachtet werden!

Rechenzeit in Abhängigkeit von der Problemgröße

Problemgröße	Zeitbedarf					
n	$\log n$	n	$n \log n$	n^2	2^n	$n!$
10	3×10^{-9} s	10^{-8} s	3×10^{-8} s	10^{-7} s	10^{-6} s	3×10^{-3} s
10^2	7×10^{-9} s	10^{-7} s	7×10^{-7} s	10^{-5} s	4×10^{13} yr	*
10^3	$1,0 \times 10^{-8}$ s	10^{-6} s	1×10^{-5} s	10^{-3} s	*	*
10^4	$1,3 \times 10^{-8}$ s	10^{-5} s	1×10^{-4} s	10^{-1} s	*	*
10^5	$1,7 \times 10^{-8}$ s	10^{-4} s	2×10^{-3} s	10 s	*	*
10^6	2×10^{-8} s	10^{-3} s	2×10^{-2} s	17 min	*	*

Annahme: eine Operation dauert 10^{-9} Sekunden, $\log n = \log_2 n$

Bezeichnung von Wachstums-Größenordnungen

$o(1)$	konvergiert gegen 0
$\mathcal{O}(1)$	beschränkt durch Konstante
$\mathcal{O}(\log n)$	logarithmische Funktion
$\mathcal{O}(\log^k n)$	polylogarithmische Funktion
$\mathcal{O}(n)$	linear beschränkte Funktion
$\bigcup_{k\geq 0} \mathcal{O}(n^k)$	polynomiell beschränkte Funktion
$\bigcup_{c\geq 0} \Omega(2^{cn})$	(mindestens) exponentielle Funktion

Beispiel 40

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 41

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

Beweis:

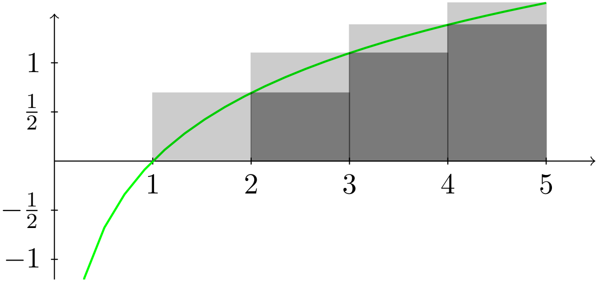
$(\forall n \in \mathbb{N})\left[\log n! = \log n + \log(n-1) + \ldots + \log 1 < 1 \cdot n \cdot \log n\right]$ $\square$

Beispiel 42

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

Beweis:

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



$\square$

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:

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

□

Die Stirling'sche Formel

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

oder mit anderen Worten:

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

Kapitel II Algebraische Grundlagen

1. Algebren

1.1 Grundbegriffe

Definition 43

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 44

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 45

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

1.2 Eigenschaften

Signatur einer Algebra

Definition 46

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

Beispiel 47

$\langle \mathbb{B}, \{t, f, \neg, \wedge, \vee\}\rangle$ (Boolesche Algebra, $\mathbb{B} = \{t, f\}$): 0, 0, 1, 2, 2

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

Beispiel 48

$\langle 2^U, \{U, \emptyset, \bar{}, \cap, \cup\}\rangle$: 0, 0, 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.

Einselement, Nullelement, Inverses

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

Definition 49

- 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 50

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 51

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

$$c = d\ .$$

Beweis:

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

$\square$

Satz 52

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

$$c = d\ .$$

Beweis:

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

$\square$

Beispiel 53

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.