

Folgen

- ▶ Objekte: unendliche Folgen

$$\mathbf{a} = (a_n)_{n \geq 0} = (a_0, a_1, a_2, \dots)$$

ganzer (oder rationaler, reeller, komplexer) Zahlen

- ▶ Ziel: wie verhalten sich die Glieder einer Folge $\mathbf{a} = (a_n)_{n \geq 0}$ in ihrem Wachstum asymptotisch, also für $n \rightarrow \infty$?
- ▶ Frage macht nur Sinn, wenn die Folge "effektiv" gegeben ist, als z.B.
 - ▶ durch einen expliziten Ausdruck ("Formel") für a_n
 - ▶ durch eine Rekursion für die a_n

- ▶ Nützlicher Standpunkt 1:
Folgen als *algebraische* Objekte ansehen!
- ▶ Nützlicher Standpunkt 2:
Folgen als *analytische* Objekte ansehen!

- ▶ Beispiele

- ▶ Fibonacci

C-rekursiv

$$f_{n+2} = f_{n+1} + f_n \quad (n \geq 0), f_0 = 0, f_1 = 1$$

- ▶ Mergesort u.a.

divide-and-conquer (statisch)

$$a_n = a_{\lfloor n/2 \rfloor} + a_{\lfloor n/2 \rfloor} + n - 1 \quad (n \geq 2), a_0 = a_1 = 0$$

- ▶ Quicksort

d&c, full-history, linear

$$b_{n+1} = \frac{2}{n+1} \sum_{k=0}^n b_k + n \quad (n \geq 0), b_0 = b_1 = 0$$

- ▶ Binäre Bäume

d&c, full-history, quadratisch und P-rekursiv

$$c_{n+1} = c_0 c_n + c_1 c_{n-1} + \dots + c_n c_0 \quad (n \geq 0), c_0 = 1$$

$$(n+1) \cdot c_n = (4n-2) \cdot c_{n-1}$$

Algebraische Sicht

- ▶ R Ring, für uns meist $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$,
 $R^{\mathbb{N}}$: Menge der Folgen $\mathbf{a} = (a_n)_{n \geq 0}$ mit $a_n \in R \quad (n \geq 0)$

- ▶ komponentenweise Addition:

sind $\mathbf{a} = (a_n)_{n \geq 0}$ und $\mathbf{b} = (b_n)_{n \geq 0}$ Folgen so ist

$$\mathbf{a} + \mathbf{b} = (a_n + b_n)_{n \geq 0}$$

- ▶ komponentenweise Skalarmultiplikation:

ist $\mathbf{a} = (a_n)_{n \geq 0}$ Folge und $\lambda \in \mathbb{C}$, so ist

$$\lambda \cdot \mathbf{a} = (\lambda a_n)_{n \geq 0}$$

- ▶ K Körper $\Rightarrow K^{\mathbb{N}}$ mit Operationen $+$ und \cdot ist Vektorraum über K .

Nullelement ist die Nullfolge $\mathbf{0} = (0, 0, 0, \dots)$.

Algebraische Sicht

- ▶ Faltungsprodukt:
sind $\mathbf{a} = (a_n)_{n \geq 0}$ und $\mathbf{b} = (b_n)_{n \geq 0}$ Folgen so ist

$$\mathbf{a} * \mathbf{b} = (c_n)_{n \geq 0} \quad \text{mit} \quad c_n = \sum_{k=0}^n a_k b_{n-k}$$

- ▶ R Ring $\Rightarrow R^{\mathbb{N}}$ mit Operationen $+$ und $*$ ist Ring.
Einselement ist die Folge $\mathbf{1} = (1, 0, 0, \dots)$.
- ▶ $\mathbf{a} = (a_n)_{n \geq 0} \in R^{\mathbb{N}} \Rightarrow$ die Gleichung $\mathbf{a} * \mathbf{b} = \mathbf{1}$ ist genau dann lösbar, wenn a_0 in R ein multiplikatives inverses Element besitzt.
- ▶ K Körper \Rightarrow alle Folgen $\mathbf{a} = (a_n)_{n \geq 0} \in K^{\mathbb{N}}$ mit $a_0 \neq 0$ sind invertierbar bezüglich $*$
(und alle Gleichungen $\mathbf{a} * \mathbf{x} = \mathbf{b}$ lösbar bei gegebenem \mathbf{b}).



Analytische Sicht

- ▶ Jede Folge $\mathbf{a} = (a_n)_{n \geq 0} \in \mathbb{C}^{\mathbb{N}}$ definiert eine unendliche Reihe (Potenzreihe):

$$\mathbf{a}(z) = \sum_{n \geq 0} a_n z^n = a_0 + a_1 z + a_2 z^2 + \dots$$

Dort, wo die Reihe für $z \in \mathbb{C}$ konvergiert, kann man sie als *Funktion* $z \mapsto \mathbf{a}(z)$ auffassen.

- ▶ $\mathbf{a}(z)$ heisst *erzeugende Funktion* der Folge \mathbf{a} .
Analogon in der Systemtheorie der E-Technik:
z-Transformierte.
- ▶ Umgekehrt: zu einer "im Nullpunkt analytischen" Funktion $z \mapsto f(z)$ liefert die Taylorentwicklung im Nullpunkt eine unendliche Folge $(f^{(n)}(0)/n!)_{n \geq 0}$.



Konvergenz und Wachstum

- ▶ Konvergenzradius $\rho \in \mathbb{R}_+ \cup \{\infty\}$:

$$\mathbf{a}(z) = \sum_{n \geq 0} a_n z^n \begin{cases} \text{konvergiert absolut für } |z| < \rho \\ \text{divergiert für } |z| > \rho \end{cases}$$

- ▶ Konvergenzkriterium von CAUCHY-HADAMARD:

$$\rho = \frac{1}{\limsup_{n \rightarrow \infty} |a_n|^{1/n}}$$

- ▶ anders formuliert: für $0 \leq r < \rho < R$ gilt

$$R^{-n} <_{i.o.} |a_n| <_{a.e.} r^{-n}$$

i.o. : für unendlich viele n , a.e. : für fast alle n



$$\mathbf{a} = (1, 1, 1, 1, 1, \dots) \quad \mathbf{a}(z) = \sum_{n \geq 0} z^n = \frac{1}{1-z}$$

$$\mathbf{b} = (1, q, q^2, q^3, \dots) \quad \mathbf{b}(z) = \sum_{n \geq 0} q^n z^n = \frac{1}{1-qz}$$

$$\mathbf{c} = (1, 2, 3, 4, 5, \dots) \quad \mathbf{c}(z) = \sum_{n \geq 0} (n+1)z^n = \frac{1}{(1-z)^2}$$

$$\mathbf{d} = \left(\binom{m+n}{m} \right)_{n \geq 0} \quad \mathbf{d}(z) = \sum_{n \geq 0} \binom{m+n}{m} z^n = \frac{1}{(1-z)^{m+1}}$$

$$\mathbf{e} = \left(\frac{1}{n!} \right)_{n \geq 0} \quad \mathbf{e}(z) = \sum_{n \geq 0} \frac{z^n}{n!} = e^z$$

$$\mathbf{f} = \left(0, \left(\frac{1}{n+1} \right)_{n > 0} \right) \quad \mathbf{f}(z) = \sum_{n > 0} \frac{z^n}{n} = -\log(1-z)$$



Einfache Rechenregeln

Die Vektorraum- bzw. Ringoperationen für Folgen sind verträglich mit den entsprechenden Operationen für Funktionen.

Für Folgen $\mathbf{a} = (a_n)_{n \geq 0}$, $\mathbf{b} = (b_n)_{n \geq 0} \in \mathbb{C}^{\mathbb{N}}$ und $\lambda \in \mathbb{C}$ gilt

- ▶ $(\mathbf{a} + \mathbf{b})(z) = \mathbf{a}(z) + \mathbf{b}(z)$
- ▶ $(\lambda \cdot \mathbf{a})(z) = \lambda \cdot \mathbf{a}(z)$
- ▶ $(\mathbf{a} * \mathbf{b})(z) = \mathbf{a}(z) \cdot \mathbf{b}(z)$
und damit auch
 $\mathbf{a} * \mathbf{b} = \mathbf{1} \Rightarrow \mathbf{a}(z)^{-1} = \mathbf{b}(z)$
- ▶ $(0^k, \mathbf{a})(z) = z^k \cdot \mathbf{a}(z)$
- ▶ $((n+1) \cdot a_{n+1})_{n \geq 0}(z) = \frac{d}{dz} a(z)$

Alternative Formulierung

$$(1+z)^\alpha = \sum_{n \geq 0} \binom{\alpha}{n} z^n$$

Folgerung: für $k \in \mathbb{N}$ und $\gamma \in \mathbb{C}$

$$\begin{aligned} \frac{z^k}{(1-\gamma \cdot z)^{k+1}} &= z^k \cdot \sum_{n \geq 0} \binom{n+k}{n} (\gamma \cdot z)^n = \sum_{n \geq 0} \binom{n+k}{k} \gamma^n \cdot z^{n+k} \\ &= \sum_{n \geq 0} \binom{n}{k} \gamma^{n-k} \cdot z^n \end{aligned}$$

Diese Reihenentwicklung konvergiert für $|z| < |\gamma|^{-1}$.

Newtons Binomialformel

Ist $\alpha \in \mathbb{C}$, so gilt die für $|z| < 1$ konvergierende Potenzreihenentwicklung (Taylorreihe):

$$(1-z)^{-\alpha} = \sum_{n \geq 0} \alpha \cdot (\alpha+1) \cdot (\alpha+n-1) \frac{z^n}{n!} = \sum_{n \geq 0} \binom{\alpha+n-1}{n} z^n$$

Beweis:

$$\frac{d}{dz} (1-z)^{-\alpha} = \alpha \cdot (1-z)^{-\alpha-1}$$

$$\left(\frac{d}{dz}\right)^n (1-z)^{-\alpha} = \alpha \cdot (\alpha+1) \cdots (\alpha+n-1) \cdot (1-z)^{-\alpha-n}$$

Folgerung aus Newtons Formel

- ▶ Gegeben $\gamma \in \mathbb{C}, \gamma \neq 0$ und $k \in \mathbb{N}$
Für eine Folge $\mathbf{a} = (a_n)_{n \geq 0} = (a_0, a_1, a_2, \dots)$ sind die beiden folgenden Aussagen äquivalent:

1. Es gibt ein Polynom $P(X) \in \mathbb{C}[X]_{\leq k}$ mit

$$(1) \quad \sum_{n \geq 0} a_n z^n = \frac{P(z)}{(1-\gamma \cdot z)^{k+1}}$$

2. Es gibt ein Polynom $R(X) \in \mathbb{C}[X]_{\leq k}$ mit

$$(2) \quad a_n = R(n) \cdot \gamma^n \quad (n \geq 0)$$

NB: Der folgende Beweis zeigt auch, wie man $R(X)$ aus $P(X)$ und umgekehrt berechnet

Beweis:

- ▶ Der Vektorraum $\mathbb{C}[X]_{\leq k}$ hat
 1. die Polynome $\{1, X, X^2, \dots, X^j, \dots, X^k\}$ als Basis
 2. die Polynome $\{1, \binom{X}{1}, \binom{X}{2}, \dots, \binom{X}{j}, \dots, \binom{X}{k}\}$ als Basis
- ▶ Die Menge der Folgen $\mathbf{a} = (a_n)_{n \geq 0} = (a_0, a_1, a_2, \dots)$ mit
 1. Eigenschaft (1) bilden einen Vektorraum V_1 über \mathbb{C}

$$\Phi_1 : \mathbb{C}[X]_{\leq k} \rightarrow V_1 : P(X) \mapsto \sum_{n \geq 0} a_n z^n = \frac{P(z)}{(1 - \gamma \cdot z)^{k+1}}$$

ist linear und injektiv,

d.h. die $\Phi_1(X^j)$ ($0 \leq j \leq k$) bilden eine Basis von V_1

2. Eigenschaft (2) bilden einen Vektorraum V_2 über \mathbb{C}

$$\Phi_2 : \mathbb{C}[X]_{\leq k} \rightarrow V_2 : R(X) \mapsto (a_n)_{n \geq 0} = (R(n) \cdot \gamma^n)_{n \geq 0}$$

ist linear und injektiv,

d.h. die $\Phi_2(\binom{X}{j})$ ($0 \leq j \leq k$) bilden eine Basis von V_1

Fortsetzung des Beweises:

- ▶ Es gilt
 1. $V_1 \subseteq V_2$, denn $\Phi_2(X^j) \in V_2$ für $0 \leq j \leq k$:

$$\begin{aligned} \frac{z^j}{(1 - \gamma \cdot z)^{k+1}} &= \sum_{n \geq 0} \binom{n+k}{k} \gamma^j z^{n+j} \\ &= \sum_{n \geq 0} \underbrace{\left[\binom{n-j+k}{k} \gamma^{-j} \right]}_{\text{Pol. in } n \text{ vom Grad } k} \gamma^n z^n \end{aligned}$$

2. $V_2 \subseteq V_1$, denn $\Phi_1(\binom{X}{j}) \in V_1$ für $0 \leq j \leq k$:

$$\sum_{n \geq 0} \binom{n}{j} \gamma^n z^n = \frac{\gamma^j}{(1 - \gamma z)^{j+1}} = \frac{\gamma^j (1 - \gamma z)^{k-j}}{(1 - \gamma z)^{k+1}}$$

3. Daher: $V_1 = V_2$

Anwendung: reguläre/rationale Sprachen

- ▶ $L \subseteq \Sigma^*$ formale Sprache, $\#\Sigma = k$
 $L_n := L \cap \Sigma^n$ Wörter der Länge n von L
- ▶ Problem: (Code-)Rate einer formalen Sprache (SHANNON)

$$\lim_{n \rightarrow \infty} \frac{\log_k \#L_n}{n} = ?$$

- ▶ Erzeugende Funktion der Wortlängen $(\#L_n)_{n \geq 0}$ von L :

$$L(z) = \sum_{n \geq 0} \#L_n z^n$$

- ▶ THEOREM: Ist L eine reguläre (= Typ-3)-Sprache, so ist $L(z)$ eine rationale Funktion, d.h. es gibt Polynome $P(X), Q(X)$ mit $Q(0) \neq 0$ und

$$L(z) = \frac{P(z)}{Q(z)}$$

Eindeutige Vereinigung

- ▶ Sind $L, M \subseteq \Sigma^*$ formale Sprachen und ist die Vereinigung $L \cup M$ eindeutig, d.h. $L \cap M = \emptyset$, so gilt

$$\#(L \cup M)_n = \#L_n + \#M_n \quad (n \geq 0)$$

und somit

$$(L \cup M)(z) = L(z) + M(z)$$

- ▶ Folgerung, falls $L \cup M$ eindeutig und $L(z), M(z)$ rational:

$$\left. \begin{aligned} L(z) &= \frac{P(z)}{Q(z)} \\ M(z) &= \frac{R(z)}{S(z)} \end{aligned} \right\} \Rightarrow (L \cup M)(z) = \frac{P(z) \cdot S(z) + Q(z) \cdot R(z)}{Q(z) \cdot S(z)}$$

d.h. auch $(L \cup M)(z)$ rational

Eindeutiges Produkt

- ▶ Sind $L, M \subseteq \Sigma^*$ formale Sprachen und ist das Produkt $L \cdot M$ eindeutig, d.h. für jedes $w \in L \cdot M$ gibt es genau ein Paar $(u, v) \in L \times M$ mit $w = u \cdot v$, so gilt

$$\#(L \cdot M)_n = \sum_{0 \leq k \leq n} \#L_k \cdot \#M_{n-k} \quad (n \geq 0)$$

und somit

$$(L \cdot M)(z) = L(z) \cdot M(z)$$

- ▶ Folgerung, falls $L \cdot M$ eindeutig und $L(z), M(z)$ rational:

$$\left. \begin{array}{l} L(z) = \frac{P(z)}{Q(z)} \\ M(z) = \frac{R(z)}{S(z)} \end{array} \right\} \Rightarrow (L \cdot M)(z) = \frac{P(z) \cdot R(z)}{Q(z) \cdot S(z)}$$

d.h. auch $(L \cdot M)(z)$ rational



Beweis des Theorems

- ▶ Fakt: jede reguläre Sprache kann aus \emptyset und den einelementigen Sprachen $\{\lambda\}, \{a\}$ für $a \in \Sigma$ durch eindeutige Vereinigung, Produkt und Iteration gewonnen werden. Das ist nicht offensichtlich! Man muss im Beweis des Theorems von KLEENE die Konstruktion von einem DFA zu einem äquivalenten regulären Ausdruck untersuchen.
- ▶ Induktionsbeweis
 - ▶ Die Basissprachen haben rationale erzeugende Funktionen

$$\emptyset(z) = 0, \{\lambda\}(z) = 1, \{a\}(z) = z \quad (a \in \Sigma)$$
 - ▶ Die Eigenschaft, eine rationale erzeugende Funktion zu haben, bleibt unter *eindeutigen* Vereinigungen, Produkten und Iterationen erhalten.



Eindeutige Iteration

- ▶ Ist $L \subseteq \Sigma^*$ eine formale Sprache und ist die Iteration L^* eindeutig, d.h. für jedes $w \in L^*$ gibt es genau ein $m \geq 0$ mit $w \in L^m$ und sind alle Potenzen L^m eindeutig, so gilt

$$\#(L^*)_n = \#(L^0)_n + \#(L^1)_n + \#(L^2)_n + \dots + \#(L^m)_n + \dots$$

und somit

$$L^*(z) = L^0(z) + L^1(z) + L^2(z) + \dots = \frac{1}{1 - L(z)}$$

- ▶ Wichtig: L^* eindeutig $\rightarrow \lambda \notin L$, also $\#(L^m)_n = 0$ für $n < m$.
- ▶ Folgerung, falls L^* eindeutig und $L(z)$ rational:

$$L(z) = \frac{P(z)}{Q(z)} \Rightarrow L^*(z) = \frac{1}{1 - \frac{P(z)}{Q(z)}} = \frac{Q(z)}{Q(z) - P(z)}$$

d.h. auch $(L^*)(z)$ rational, da $Q(0) - P(0) = Q(0) \neq 0$.



Ergänzung

Die *Komplementierung* zählt nicht zu den rationalen Operationen. Aber sie lässt sich gut behandeln:

- ▶ Σ Alphabet mit $\#\Sigma = k$
- ▶ $L \subseteq \Sigma^*$ formale Sprache, $\bar{L} = \Sigma^* \setminus L$ komplementäre Sprache
- ▶ die Vereinigung $L \cup \bar{L} = \Sigma^*$ ist eindeutig, also

$$L(z) + \bar{L}(z) = \Sigma^*(z) = \sum_{n \geq 0} k^n z^n = \frac{1}{1 - kz}$$

(ganz unabhängig davon, ob L regulär ist oder nicht).



Beispiel

- ▶ $\Sigma = \{a, b, c\}$
- ▶ $L \subseteq \Sigma^*$: Wörter, die keinen Faktor aa enthalten
- ▶ $(\#L_n)_{n \geq 0} = (1, 3, 8, 22, 60, 164, 448, \dots)$
- ▶ regulärer Ausdruck $(\lambda + a)(b + c + ba + ca)^*$
- ▶ alle Operationen sind eindeutig!
- ▶ erzeugende Funktion

$$L(z) = (1 + z) \cdot \frac{1}{1 - (2z + 2z^2)} = \frac{1 + z}{1 - 2z - 2z^2}$$



Ergänzende Bemerkungen

- ▶ Man nennt die drei Operationen auf Sprachen:
 - ▶ Vereinigung
 - ▶ Produkt
 - ▶ Iteration (Kleene-*)

rationale Operationen, in Anlehnung an die rationalen Operationen der Arithmetik: Summe, Produkt, Reziproke (Division!).
- ▶ Die Typ-3 Sprachen heißen auch *Rationale Sprachen* wegen der Generierung mittels rationaler Operationen. Die sog. *regulären* Ausdrücke sollten eigentlich *rationale* Ausdrücke heißen.



Beispiel (Forts.)

- ▶ $\bar{L} \subseteq \Sigma^*$: Wörter, die mindestens einen Faktor aa enthalten
- ▶ $(\#\bar{L}_n)_{n \geq 0} = (0, 0, 1, 5, 21, 79, 281, \dots)$
- ▶ erzeugende Funktion

$$\begin{aligned} \bar{L}(z) &= \Sigma^*(z) - L(z) \\ &= \frac{1}{1 - 3z} - \frac{1 + z}{1 - 2z - 2z^2} = \frac{z^2}{1 - 5z + 4z^2 + 6z^3} \end{aligned}$$

- ▶ Vorsicht: zwar ist $\Sigma^*aa\Sigma^*$ ein regulärer Ausdruck für \bar{L} , aber diese Darstellung ist nicht eindeutig! Klarerweise ist

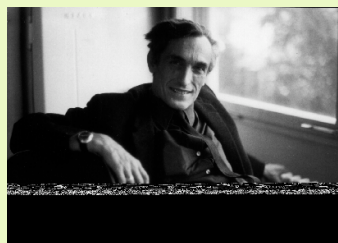
$$\frac{1}{1 - 3z} \cdot z^2 \cdot \frac{1}{1 - 3z} = \frac{z^2}{1 - 6z + 9z^2} \neq \frac{z^2}{1 - 5z + 4z^2 + 6z^3}$$



Historische Bemerkung

- ▶ Für *eindeutige* kontextfreie Sprachen gilt ein analoges Theorem: die erzeugenden Funktionen solcher Sprachen sind immer *algebraisch* (d.h. Lösungen eines *polynomialen* Gleichungssystems).
- ▶ Beide Theoreme sind wesentlicher Bestandteil einer Arbeit, die für die Entwicklung einer mathematischen Theorie der kontextfreien Sprachen eine fundamentale Bedeutung hatte: N. Chomsky, M.-P. Schützenberger: *The algebraic theory of context-free languages*. In: Computer Programming and Formal Languages, P. Brafford and D. Hirschberg, eds., North Holland, 1963.





Marcel-Paul Schützenberger (1920-1996)

Mediziner, Mathematiker, Begründer der Theoretischen Informatik in Frankreich
 insbesondere: Theorie der kontextfreien Sprachen (mit Noam Chomsky)

Photo: Konrad Jacobs, Oberwolfach, 1972

Anwendung: Beweis von CATALANS Formel

- ▶ $c_n =$ Anzahl der Binärbäume mit n inneren Knoten
 = Anzahl der korrekten Klammerungen mit n Klammerpaaren
- ▶ $\mathbf{c} = (c_n)_{n \geq 0} = (1, 1, 2, 5, 14, 42, 132, \dots)$
- ▶ Rekursion (aus strukturellem Aufbau der Objekte)
 [J.A. VON SEGNER, 1758]

$$c_{n+1} = c_0 \cdot c_n + c_1 \cdot c_{n-1} + c_2 \cdot c_{n-2} + \dots + c_n \cdot c_0$$

mit Startwert $c_0 = 1$

Diese Rekursion ist "full-history" und nicht linear!

- ▶ Explizite Formel [E. CH. CATALAN, 1838]

$$c_n = \frac{1}{n+1} \binom{2n}{n}$$

- ▶ erzeugende Funktion

$$\mathbf{c}(z) = \sum_{n \geq 0} c_n z^n = 1 + z + 2z^2 + 5z^3 + 14z^4 + \dots$$

- ▶ Übersetzung der Rekursion in quadratische Gleichung für $\mathbf{c}(z)$:

$$\mathbf{c}(z) = 1 + z \cdot \mathbf{c}(z)^2$$

- ▶ Lösung der quadratischen Gleichung

$$\mathbf{c}(z) = \frac{1 \pm \sqrt{1 - 4z}}{2z}$$

- ▶ NEWTONS Formel

$$\sqrt{1 - 4z} = \sum_{n \geq 0} \binom{1/2}{n} (-4z)^n$$

- ▶ Umrechnen der Binomialkoeffizienten:

$$\binom{1/2}{n} (-4)^n = \begin{cases} 1 & n = 0 \\ -\frac{2}{n} \binom{2n-2}{n-1} & n > 0 \end{cases}$$

- ▶ Einsetzen und Auswählen des richtigen Vorzeichens:

$$\mathbf{c}(z) = \sum_{n \geq 0} c_n z^n = \sum_{n \geq 0} \frac{1}{n+1} \binom{2n}{n} z^n$$

- ▶ Folgerung mittels Koeffizientenvergleich:

$$c_n = \frac{1}{n+1} \binom{2n}{n} \quad (n \geq 0).$$