# Formale Systeme, Automaten und Prozesse Beweise

Justin Korte

Februar 2023

## 1 Beweise

### 1.1 Sprachbeweise

#### 1.1.1 Assoziativgesetz

Für alle Sprachen $K, L, M$ gilt: $(KL)M = K(LM)$

**Beweis** :
Wir zeigen folgende Teilaussagen:

1. $(KL)M \subseteq K(LM)$
2. $K(LM) \subseteq (KL)M$

1. Sei $u \in (KL)M$.
Daraus folgt, dass ein $v \in KL$ und ein $w \in M$ existiert, sodass $u = vw$.
Da $v \in KL$ gilt, folgt $v = xy\,, x \in K, y \in L$ und damit $u = xyw$.
Definiere man nun $v' = yw$, so ergibt sich $u = xv'$, also $u \in K(LM)$.

2. Sei $u \in K(LM)$.
Daraus folgt, dass ein $v \in K$ und ein $w \in LM$ existiert, sodass $u = vw$.
Da $w \in LM$ gilt, folgt $w = xy\,, x \in L, y \in M$ und damit $u = vxy$.
Definiere man nun $w' = vx$, so ergibt sich $u = w'y$, also $u \in (KL)M$

Aus $(KL)M \subseteq K(LM)$ und $K(LM) \subseteq (KL)M$ folgt $(KL)M = K(LM)$

□

#### 1.1.2 Rechtsseitige Distributivität

Für alle Sprachen $K, L, M$ gilt: $K(L \cup M) = KL \cup KM$

**Beweis** :
Wir zeigen folgende Teilaussagen:

1. $K(L \cup M) \subseteq KL \cup KM$
2. $KL \cup KM \subseteq K(L \cup M)$

1. Sei $u \in K(L \cup M)$.
Daraus folgt, dass ein $v \in K$ und ein $w \in L \cup M$ existiert, sodass $u = vw$.
Da $w \in L \cup M$ gilt, folgt $w \in L \vee w \in M$.

**Fall 1:** $w \in L$
Dann ist $u = vw \in KL \subset KL \cup KM$

**Fall 2:** $w \in M$
Dann ist $u = vw \in KM \subset KL \cup KM$

Also gilt in beiden Fällen $u \in K(L \cup M) \Rightarrow u \in KL \cup KM \Leftrightarrow K(L \cup M) \subseteq KL \cup KM$

2. Sei $u \in KL \cup KM$.

**Fall 1:** $u \in KL$
Dann existieren $v \in K$ und $w \in L$ mit $u = vw$. Da $w \in L \Rightarrow w \in L \cup M$ gilt $u \in K(L \cup M)$

**Fall 2:** $u \in KM$ Dann existieren $v \in K$ und $w \in M$ mit $u = vw$. Da $w \in M \Rightarrow w \in L \cup M$ gilt $u \in K(L \cup M)$

Also gilt in beiden Fällen $u \in KL \cup KM \Rightarrow u \in K(L \cup M) \Leftrightarrow KL \cup KM \subseteq K(L \cup M)$

Aus $K(L \cup M) \subseteq KL \cup KM$ und $KL \cup KM \subseteq K(L \cup M)$ folgt $K(L \cup M) = KL \cup KM$

□

### 1.1.3 Kleene-Iteration

Für alle Sprachen K gilt: $K^*K = KK^*$

Wir zeigen folgende Teilaussagen:

1. $K^*K \subseteq KK^*$
2. $KK^* \subset K^*K$

1. Sei $u \in K^*K$. Dann ist $u = w_1 \dots w_n v$ mit $u, w_i \in K, \quad 1 \leq i \leq n$.
Definieren wir nun $v' = w_1, w_1' = w_2 \dots w_{n-1}' = w_n$ und $w_n' = v$.
Dann ist $w = v'w_1' \dots w_n'$, also ist $u \in KK^*$

2. Sei $u \in KK^*$. Dann ist $u = vw_1 \dots w_n$ mit $u, w_i \in K, \quad 1 \leq i \leq n$.
Definieren wir nun $w_1' = v, w_2' = w_1 \dots w_n' = w_{n-1}$ und $v' = w_n$.
Dann ist $w = w_1' \dots w_n'v'$, also ist $u \in K^*K$

Aus $K^*K \subseteq KK^*$ und $KK^* \subset K^*K$ folgt $K^*K = KK^*$

□

### 1.1.4 Schnitt von Sprachen unter Kleene-Iteration

Für alle Sprachen K,L gilt: $(K \cap L)^* \subseteq K^* \cap L^*$, aber es gilt nicht $K^* \cap L^* \subseteq (K \cap L)^*$ und damit insbesondere nicht $(K \cap L)^* = K^* \cap L^*$

Wir zeigen folgende Teilaussagen:

1. $(K \cap L)^* \subseteq K^* \cap L^*$
2. $K^* \cap L^* \nsubseteq (K \cap L)^*$

1. Sei $w \in (K \cap L)^*$.

**Fall 1:** $w = \varepsilon$
$\varepsilon \in (K \cap L)^*$. Da $\varepsilon \in K^* \wedge \varepsilon \in L^* \Rightarrow \varepsilon \in K^* \cap L^* \Leftrightarrow (K \cap L)^* \subseteq K^* \cap L^*$

**Fall 2:** $w \neq \varepsilon$
Dann existiert ein $n \geq 1$, dass $w = w_1 \dots w_n$ gilt mit $w_i \in (K \cap L) \forall i \in \{1 \dots n\}$
Also ist $w_i \in K$ und $w_i \in L \ \forall i \in \{1 \dots n\}$
Daraus folgt $w \in K^*$ und $w \in L^* \Rightarrow w \in K^* \cap L^*$.

2. Wir zeigen per Widerspruchsbeweis $K^* \cap L^* \nsubseteq (K \cap L)^*$. Wir nehmen an, dass $K^* \cap L^* \subseteq (K \cap L)^*$ gilt.
Daraus folgt: $\forall w \in K^* \cap L^* \Rightarrow w \in (K \cap L)^*$.

Sei nun $K := \{a\}$ und $L := \{aa\}$. Dann folgt:
$K^* \cap L^* = \{a^{2n} | n \in \mathbb{N}\}$ und $(K \cap L)^* = \{\varepsilon\}$. Aus oberer Definition ergibt sich $K^* \cap L^* \nsubseteq (K \cap L)^*$, was aber einen Widerspruch zur Annahme ergibt. Somit muss $K^* \cap L^* \nsubseteq (K \cap L)^*$ gelten.

Aus $(K \cap L)^* \subseteq K^* \cap L^*$ und $K^* \cap L^* \nsubseteq (K \cap L)^*$ folgt $K^* \cap L^* \neq (K \cap L)^*$.

□

## 1.2 Hilfsbeweise

### 1.2.1 Darstellung eines Wortes im b-adischen System

Sei $w \in \{0, \dots, b\}^*$ und $a \in \{0, \dots, b\}$ Zahlendarstellungen zur Basis b.
Dann gilt $k(wa) = b \cdot k(w) + a$ mit $k(w) = \sum_{i=1}^{n} w_i \cdot b^{n-i}$
**Beweis** :
Sei $z = z_1 \dots z_{n+1}$ mit $w = z_1 \dots z_n$ und $a = z_{n+1}$.
Daraus folgt:

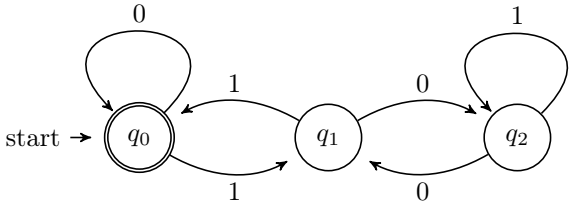
$$\begin{aligned} k(z) &= \sum_{i=1}^{n+1} z_i \cdot b^{n+1-i} \\ &= \sum_{i=1}^{n} (z_i \cdot b^{n+1-i}) + z_{n+1} \cdot b^0 \\ &= b \cdot \sum_{i=1}^{n} (z_i \cdot b^{n-i}) + z_{n+1} \\ &= b \cdot k(z_1 \dots z_n) + z_{n+1} \\ &= b \cdot k(w) + a \end{aligned}$$

□

## 1.3 Automatenbeweise

### 1.3.1 Binärautomat mit Teilbarkeit 3

Sei $A_2$ der folgende Automat:



Dann gilt $A_2$ akzeptiert $w \in \{0,1\}^* \Leftrightarrow b(w) \equiv 0 \, mod \, 3$

**Beweis** :

Wir zeigen per vollständiger Induktion über $n \in \mathbb{N}_0$, dass für alle Wörter $w = a_1 \dots a_n \in \Sigma^*$ gilt:
Ist $(r_0, r_1, \dots, r_n)$ ein Lauf von $A_2$ auf $w \Rightarrow r_n \equiv bin(w) \, mod \, 3$

**Induktionsanfang** :

Sei n = 0. Dann ist der Lauf von $A_2$ auf $w = \varepsilon$ demnach (0), und $bin(\varepsilon) = 0 \Rightarrow r_0 \equiv bin(\varepsilon) \, mod \, 3$.

**Induktionsvoraussetzung** :

Für ein beliebiges, festes $n \in \mathbb{N}_0$ gilt $r_n \equiv bin(a_1 \dots a_n) \, mod \, 3$

**Induktionsschritt** :

Sei $(r_0, \dots, r_{n+1})$ der Lauf von $A_2$ auf $w = a_1 \dots a_{n+1}$.
Aus (1.2.1) gilt : $bin(w) = bin(a_1 \dots a_n a_{n+1}) = 2 \cdot bin(a_1 \dots a_n) + a_{n+1}$
Nun gilt mithilfe der Voraussetzung $b(w) = 2 \cdot bin(a_1 \dots a_n) + a_{n+1} \overset{IV}{\equiv} 2 \cdot r_n + a_{n+1} \, mod \, 3$

Nun betrachten wir alle Belegungen von $r_n$ und $a_{n+1}$ :

**Fall 1:** $r_n = 0, a_{n+1} = 0$

Dann gilt $bin(w) \equiv 2 \cdot r_n + a_{n+1} \, mod \, 3 \equiv 0 \, mod \, 3$ und $\delta(r_n, a_{n+1}) = r_{n+1} \Rightarrow \delta(0,0) = 0$

**Fall 2:** $r_n = 0, a_{n+1} = 1$

Dann gilt $bin(w) \equiv 2 \cdot r_n + a_{n+1} \, mod \, 3 \equiv 1 \, mod \, 3$ und $\delta(r_n, a_{n+1}) = r_{n+1} \Rightarrow \delta(0,1) = 1$

**Fall 3:** $r_n = 1, a_{n+1} = 0$

Dann gilt $bin(w) \equiv 2 \cdot r_n + a_{n+1} \, mod \, 3 \equiv 2 \, mod \, 3$ und $\delta(r_n, a_{n+1}) = r_{n+1} \Rightarrow \delta(1,0) = 2$

**Fall 4:** $r_n = 1, a_{n+1} = 1$

Dann gilt $bin(w) \equiv 2 \cdot r_n + a_{n+1} \, mod \, 3 \equiv 0 \, mod \, 3$ und $\delta(r_n, a_{n+1}) = r_{n+1} \Rightarrow \delta(1,1) = 0$

**Fall 5:** $r_n = 2, a_{n+1} = 0$

Dann gilt $bin(w) \equiv 2 \cdot r_n + a_{n+1} \, mod \, 3 \equiv 1 \, mod \, 3$ und $\delta(r_n, a_{n+1}) = r_{n+1} \Rightarrow \delta(2,0) = 1$

**Fall 6:** $r_n = 2, a_{n+1} = 1$

Dann gilt $bin(w) \equiv 2 \cdot r_n + a_{n+1} \, mod \, 3 \equiv 2 \, mod \, 3$ und $\delta(r_n, a_{n+1}) = r_{n+1} \Rightarrow \delta(2,1) = 2$

Damit wurde die Behauptung der Induktion bewiesen. Wenn nun $r_n = 0$ gilt, so befindet sich der Automat in $q_0$ und akzeptiert. Aus der bewiesenen Induktion folgt nun:

$$A_2 \text{ akzeptiert } w \in \{0,1\}^* \Leftrightarrow r_n = 0 \overset{Ind.}{\Leftrightarrow} bin(w) \equiv 0 \, mod \, 3$$

Damit wurde die Behauptung bewiesen.

□

## 1.4 Abschlusseigenschaften von DFA-erkennbaren Sprachen

### 1.4.1 Abschluss des Komplements

Sei $L \subseteq \Sigma^*$ DFA-erkennbar. Dann ist auch $\overline{L}$ DFA-erkennbar

**Beweis** :

Sei $A = (Q, \Sigma, \delta, q_0, F)$ ein DFA mit $L(A) = L$.
Sei $\overline{A}$ der DFA, der aus A durch Vertauschen von Endzuständen und Nicht-Endzuständen entsteht, also $\overline{A} = (Q, \Sigma, \delta, q_0, Q \setminus F)$

Wir zeigen nun $L(\overline{A}) = \overline{L}$, also dass $\overline{L}$ DFA-erkennbar ist.

Sei nun $w = a_1 \dots a_n \in \Sigma^*$. Wir zeigen

$$A \text{ akzeptiert } w \Leftrightarrow \overline{A} \text{ akzeptiert w nicht}$$

$A$ und $\overline{A}$ haben den gleichen Lauf $(r_0 \dots r_n)$ auf $w$. Es gilt:

$$\begin{aligned} \text{A akzeptiert w} &\Leftrightarrow r_n \in F \\ &\Leftrightarrow r_n \notin Q \setminus F \\ &\Leftrightarrow \overline{A} \text{ akzeptiert w nicht} \end{aligned}$$

Daraus folgt, dass $\overline{A}$ genau alle Wörter w verwirft, wenn A diese akzeptiert.
Negiert bedeutet das, dass $\overline{A}$ genau alle Wörter w akzeptiert, wenn A diese verwirft.
Damit akzeptiert $\overline{A}$ alle Wörter aus $\overline{L}$, also gilt $L(\overline{A}) = \overline{L}$. Damit ist $\overline{L}$ DFA-erkennbar.

□

### 1.4.2 Abschluss des Schnittes

Seien $L_1, L_2 \subseteq \Sigma^*$ DFA-erkennbar. Dann ist $L_1 \cap L_2$ DFA-erkennbar.

**Beweis** :

Sei $A_1 = (Q_1, \Sigma, \delta_1, q_{01}, F_1)$ ein DFA mit $L(A_1) = L_1$ und
sei $A_2 = (Q_2, \Sigma, \delta_2, q_{02}, F_2)$ ein DFA mit $L(A_2) = L_2$.

Wir konstruieren einen Produktautomaten $A = (Q_1 \times Q_2, \Sigma, \delta, (q_{01}, q_{02}), F)$ mit
$\delta((r_1, r_2), a) := (\delta_1(r_1, a), \delta_2(r_2, a))$ und $F = F_1 \times F_2$

Wir zeigen nun:

$$\text{A akzeptiert w} \Leftrightarrow A_1 \text{ akzeptiert w und } A_2 \text{ akzeptiert w}$$

woraus $L(A) = L(A_1) \cap L(A_2)$ folgt.

Sei $w = a_1 \dots a_n$ und der Lauf von $A_1 = (r_0, a_1, r_1, \dots, a_n, r_n)$ und von $A_2 = (s_0, a_1, s_1, \dots, a_n, s_n)$.
Daraus folgt der Lauf von A als $((r_0, s_0), a_1, (r_1, s_1), \dots, a_n, (r_n, s_n))$
Gleichermaßen gilt dadurch:

$$A_1 \text{ akzeptiert } w \Leftrightarrow r_n \in F_1$$

$$A_2 \text{ akzeptiert } w \Leftrightarrow s_n \in F_2$$

Desweiteren folgt:

$$\begin{aligned} A \text{ akzeptiert } w &\Leftrightarrow (r_n, s_n) \in F = F_1 \times F_2 \\ &\Leftrightarrow r_n \in F_1 \text{ und } s_n \in F_2 \\ &\Leftrightarrow A_1 \text{ akzeptiert } w \text{ und } A_2 \text{ akzeptiert } w \end{aligned}$$

Damit ist $L(A) = L_1 \cap L2$, also ist $L_1 \cap L_2$ DFA-erkennbar.

□

### 1.4.3 Abschluss der Vereinigung

Seien $L_1, L_2 \subseteq \Sigma^*$ DFA-erkennbar. Dann ist $L_1 \cup L_2$ DFA-erkennbar.

**Beweis 1** :

Aus den de-Morganschen Gesetzen folgt $L_1 \cup L_2 = \overline{L_1} \cap \overline{L_2}$.
Da sowohl $L_1$ als auch $L_2$ DFA-erkennbar sind, folgt aus (1.4.1), dass $\overline{L_1}$ und $\overline{L_2}$ DFA-erkennbar sind.
Aus (1.4.2) folgt, dass auch $\overline{L_1} \cap \overline{L_2}$ DFA-erkennbar ist. Da $\overline{L_1} \cap \overline{L_2} + L_1 \cup L_2$ gilt, muss auch $L_1 \cup L_2$ DFA-erkennbar sein.

□

## 1.5 Erreichbarkeitsbeweise

### 1.5.1 Äquivalenz von Akzeptanz und Erreichbarkeit

Sei $A = (Q, \Sigma, \Delta, q_0, F)$ ein NFA und $w \in \Sigma^*$. Dann gilt :

$$w \in L(A) \Leftrightarrow E(A, w) \cap F \neq \emptyset$$

**Beweis** :

$$\begin{aligned} w \in L(A) &\Leftrightarrow A \text{ akzeptiert } w \\ &\Leftrightarrow \exists q \in F : q \in E(A, w) \\ &\Leftrightarrow E(A, w) \cap F \neq \emptyset \end{aligned}$$

□

### 1.5.2 Strukturelle Erreichbarkeit

Sei $A = (Q, \Sigma, \Delta, q_0, F)$ ein NFA. Dann gilt:

1. $E(A, \varepsilon) = \{q_0\}$
2. Für alle $w \in \Sigma^*$ und $a \in \Sigma$ gilt:

$$E(A, wa) = \bigcup_{q \in E(a,w)} \{q' \in Q | (q, a, q') \in \Delta\}$$

**Beweis** :

1. $\forall q \in Q$ gilt:

$$q \in E(A, \varepsilon) \Leftrightarrow q_0 \xrightarrow{\varepsilon} q \Leftrightarrow q = q_0$$

2. Sei $w \in \Sigma^*$ und $a \in \Sigma$. Dann gilt $\forall q \in Q$:

$$\begin{aligned} q \in E(A, wa) &\Leftrightarrow q_0 \xrightarrow{wa} q \\ &\Leftrightarrow \exists\, q' \in Q: \quad q_0 \xrightarrow{w} q' \text{ und } (q', a, q) \in \Delta \\ &\Leftrightarrow \exists\, q' \in Q: \quad q' \in E(A, w) \text{ und } (q', a, q) \in \Delta \\ &\Leftrightarrow q \in \bigcup_{q' \in E(A,w)} \{q'' \in Q | (q', a, q'') \in \Delta\} \end{aligned}$$

□

## 1.6 Äquivalenz von Automaten

### 1.6.1 Äquivalenz von DFA und NFA

DFA und NFA sind zueinander äquivalent .

**Beweis** :

Wir zeigen 2 Teilaussagen:

1. Zu jedem DFA gibt es einen äquivalenten NFA
2. Zu jedem NFA gibt es einen äquivalenten DFA

1. Sei $A = (Q, \Sigma, \delta, q_0, F)$ ein DFA. Wir definieren $\Delta \subseteq Q \times \Sigma \times Q$ mit $\Delta = \{(q, a, q') | \delta(q, a) = q'\}$.

Wir zeigen, dass der NFA $A' = (Q, \Sigma, \Delta, q_0, F)$ äquivalent zu $A$ ist.

Dazu betrachten wir die Folge $\rho = (r_0, a_1, r_1, \ldots, a_n, r_n)$ mit $r_0 \ldots r_n \in Q$ und $a_1 \ldots a_n \in \Sigma$.
Dann gilt mit $1 \leq in$ :

$$\delta(r_{-1}, a_i) = r_i \Leftrightarrow (r_{i-1}, a_i, r_i) \in \Delta$$

Da A und $A'$ beide in $q_0$ anfangen, folgt daraus:

$$\rho \text{ ist Lauf von } A \Leftrightarrow \rho \text{ ist Lauf von } A'$$

Und da sowohl $A$ als auch $A'$ die gleichen Endzustände besitzen , so folgt daraus:

$$\rho \text{ ist akzeptierender Lauf von } A \Leftrightarrow \rho \text{ ist akzeptierender Lauf von } A'$$

Daraus folgt schließlich

$$A \text{ akzeptiert } a_1 \ldots a_n \Leftrightarrow A;\ \text{akzeptiert } a_1 \ldots a_n \Rightarrow L(A) = L(A')$$

Also sind A und A' äquivalent .

2. Sei $A = (Q, \Sigma, \Delta, q_0, F)$ ein NFA und $A' = Q', \Sigma, \delta, q_0', F'$ der **Potenzmengenautomat** von A mit :

$Q' := Pot(Q), \quad \delta(q', a) := \{q \in Q \mid \exists\, p \in q' : (p, a, q) \in \Delta\}$ mit
$q' \in Q, a \in \Sigma, \quad q'_0 := \{q_0\}, \quad F' = \{q' \in Q' | q' \cap F \neq \emptyset\}$

Wir zeigen, dass jeder NFA zum oben gebauten Potenzmengenautomat äquivalent sind, also $L(A) = L(A')$.

Dazu zeigen wir erst, dass bei $w \in \Sigma^*$ und $q' \in Q'$ gilt: $A' : q'_0 \overset{w}{\to} q' \Leftrightarrow q' = E(A, w)$

**1.6.* <u>Beweis mit Induktion über</u>** $n := |w|$ :

**<u>Induktionsanfang</u>** :

Sei n = 0. Dann ist $w = \varepsilon$ und $q' = q'_0 = \{q'_0\} \overset{(1.5.2)}{=} E(A, \varepsilon)$.

**<u>Induktionsvoraussetzung</u>** :

Es gibt ein $q' \in Q'$ mit $A' : q'_0 \overset{w}{\to} q'$

**<u>Induktionsschritt</u>** :

Sei $w = w'a$ mit $w' \in \Sigma^*$ und $|w'| = n$ sowie $a \in \Sigma /$
Sei $q'' \in Q'$ mit $A' : q'_0 \overset{w}{\to} q''$. Dann folgt:

$$\begin{aligned} q' &= \delta(q'', a) \\ &= \{q \in Q \mid \exists\, p \in q'' : (p, a, q) \in \Delta\} \\ &= \bigcup_{p \in E(A, w')} \{q \in Q | (p, a, q) \in \Delta\} \\ &\overset{(1.5.2)}{=} E(A, w) \end{aligned}$$

Damit wurde die Induktionsbehauptung bewiesen

□

*Sei* w $\in \Sigma^*$ und sei $q' \in Q'$ mit $A' : q'_0 \overset{w}{\to} q'$, dann gilt:

$$\begin{aligned} w \in L(A) &\overset{(1.5.1)}{\Longleftrightarrow} E(A, w) \cap F \neq \emptyset \\ &\overset{(1.6.*)}{\Longleftrightarrow} q' \cap F\emptyset \\ &\Longleftrightarrow q' \in F \\ &\Longleftrightarrow A' \text{ akzeptiert } w \\ &\Longleftrightarrow w \in L(A') \end{aligned}$$

Aus 1. und 2. folgt, dass DFA und NFA zueinander äquivalent sind, also ist eine Sprache genau dann DFA-erkennbar, wenn sie NFA-erkennbar ist. Somit Ist die Menge der DFA-erkennbaren Sprachen gleich der Menge der NFA-erkennbaren Sprachen.

□