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:

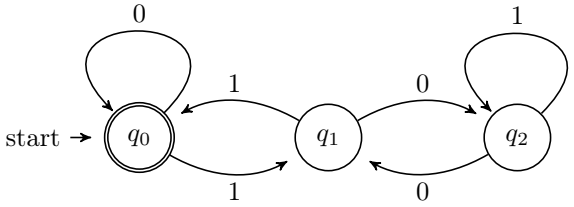
$$\begin{aligned} k(z) &= \sum_{i=1}^{n+1} z_i \cdot b^{n+1-i} \\ &= \sum_{i=1}^{n} (z_i \cdot b^{n+1-i}) + z_{n+1} \cdot b^0 \\ &= b \cdot \sum_{i=1}^{n} (z_i \cdot b^{n-i}) + z_{n+1} \\ &= b \cdot k(z_1 \dots z_n) + z_{n+1} \\ &= b \cdot k(w) + a \end{aligned}$$

□

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 $r_n \equiv bin(a_1 \dots a_n) \, mod \, 3$

Induktionsvoraussetzung :

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.

□