René Maseli
Prof. Dr. Roland Meyer

Theoretische Informatik 1
Große Übung 3

TU Braunschweig
Wintersemester 2022/23

Korrektheit von Arden's Lemma

Seien $L, U, V \subseteq \Sigma^*$ Sprachen mit $L = U^*.V$. Es gilt $L = U.L \cup V$.

$$\begin{aligned} L &= U^*.V \\ &= (U^+ \cup \{\varepsilon\}).V \\ &= U^+.V \cup V \\ &= U.U^*.V \cup V \\ &= U.L \cup V \end{aligned}$$

Korrektheit der Potenzmengen-Konstruktion nach Rabin & Scott

Seien $A = \langle Q, q_0, \to, Q_F\rangle$ ein NFA und $A' = \langle \mathcal{P}(Q), \{q_0\}, \to', Q'_F\rangle$ dessen Potenzmengen-Automat. Es gilt $\mathcal{L}(A') = \mathcal{L}(A)$:

Sei $w \in \mathcal{L}(A)$. Es gibt die Berechnung $q_0 \xrightarrow{w_1} q_1 \cdots \xrightarrow{w_n} q_n \in Q_F$. Es gibt die eindeutige Berechnung $\{q_0\} = Q_0 \xrightarrow{w_1} Q_1 \cdots \xrightarrow{w_n} Q_n$. Induktiv wissen wir $q_i \in Q_i$, denn $q_0 \in Q_0$ und $q_i \in Q_i \Rightarrow q_{i+1} \in Q_{i+1}$. Es folgt $Q_n \in Q_F$, also $w \in \mathcal{L}(A')$.

Sei $w \in \mathcal{L}(A')$. Die Berechnung dazu sei $\{q_0\} = Q_0 \xrightarrow{w_1} Q_1 \cdots \xrightarrow{w_n} Q_n \in Q_F$. Es gibt $q_n \in Q_n \cap Q_F$. Induktiv gibt es stets mindestens einen Vorgänger $q_i \in Q_i$. Betrachte also die Berechnung $q_0 \xrightarrow{w_1} q_1 \cdots \xrightarrow{w_n} q_n \in Q_F$. Daraus folgt $w \in \mathcal{L}(A)$.

Produktautomat

Theorem
Seien Σ ein endliches Alphabet und $L, K \subseteq \Sigma^*$ regulär. Der Durchschnitt $L \cap K$ ist regulär.

Beweis
Klar mit deMorgan'schen Regeln und der bereits bekannten Abgeschlossenheit unter Komplement: $L \cap K = \overline{\overline{L} \cup \overline{K}}$. □

Dennoch gibt es einen praktischeren Ansatz. Seien $A = \langle Q_A, q_{0A}, \to_A, Q_{FA}\rangle$ und $B = \langle Q_B, q_{0B}, \to_B, Q_{FB}\rangle$ endliche Automaten mit $\mathcal{L}(A) = L$ und $\mathcal{L}(B) = K$ Der Produktautomat $A \cap B = \langle Q_A \times Q_B, \langle q_{0A}, q_{0B}\rangle, \to', Q_{FA} \times Q_{FB}\rangle$ enthält genau dann eine Transition $\langle p_A, p_B\rangle \xrightarrow{s} \langle q_A, q_B\rangle$, wenn gleichzeitig $p_A \xrightarrow{s}_A q_A$ und $p_B \xrightarrow{s}_B q_B$ existieren. Man sagt, $A \cap B$ simuliert gleichzeitig A und B und akzeptiert genau dann, wenn beide Simulationen akzeptieren.

Es gilt $\mathcal{L}(A \cap B) = \mathcal{L}(A) \cap \mathcal{L}(B)$.

Beweis
Sei $w = w_1 w_2 \ldots w_n \in \Sigma^*$. Wir zeigen beide Teilmengen-Beziehungen gleichzeitig.

$$\begin{aligned}
&\quad w \in \mathcal{L}(A) \cap \mathcal{L}(B) \\
&\text{gdw. } q_{0A} \xrightarrow{w}_A q_{nA} \in Q_{FA} \text{ und } q_{0B} \xrightarrow{w}_B q_{nB} \in Q_{FB} \\
&\text{gdw. es } q_{0A} \xrightarrow{w_1}_A q_{1A} \xrightarrow{w_2}_A \cdots \xrightarrow{w_n}_A q_{nA} \in Q_{FA} \text{ und } q_{0B} \xrightarrow{w_1}_B q_{1B} \xrightarrow{w_2}_B \cdots \xrightarrow{w_n}_B q_{nB} \in Q_{FB} \text{ gibt} \\
&\text{gdw. es } \langle q_{0A}, q_{0B} \rangle \xrightarrow{w_1} \langle q_{1A}, q_{1B} \rangle \xrightarrow{w_2} \cdots \xrightarrow{w_n} \langle q_{nA}, q_{nB} \rangle \in Q_{FA} \times Q_{FB} \text{ gibt} \\
&\text{gdw. } \langle q_{0A}, q_{0B} \rangle \xrightarrow{w} \langle q_{nA}, q_{nB} \rangle \in Q_{FA} \times Q_{FB} \\
&\text{gdw. } w \in \mathcal{L}(A \cap B)
\end{aligned}$$

□

Shuffle

Definition
Seien Σ ein Alphabet und $v, w \in \Sigma^*$. Der Shuffle $v \shuffle w$ ist die Menge der Worte, die durch eine beliebige abwechslung der Buchstaben von v und w hervorgehen. Dabei soll die Reihenfolge der Buchstaben aus demselben Wort erhalten bleiben.

$$v \shuffle w := \begin{cases} a.(x \shuffle w) \cup b(v \shuffle y) & \text{falls } v = a.x \text{ und } w = b.y \\ \{v.w\} & \text{falls } v = \varepsilon \text{ oder } w = \varepsilon \end{cases}$$

Der Shuffle zweier Sprachen $L \subseteq \Sigma^*$ und $M \subseteq \Sigma^*$ ist die Sprache

$$L \shuffle M := \bigcup \{ \, v \shuffle w \mid v \in L \text{ und } w \in M \, \}$$

Beispiel
$aab \shuffle ba = \{\underline{aab}ba, \underline{aa}b\underline{b}a, \underline{aa}ba\underline{b}, \underline{a}b\underline{ab}a, \underline{a}b\underline{a}a\underline{b}, \underline{a}ba\underline{ab}, b\underline{aab}a, b\underline{aa}a\underline{b}, b\underline{a}a\underline{ab}, ba\underline{aab}\}$

Beispiele für reguläre Sprachen sind

$$(aa)^* \shuffle b^* = b^*\left(ab^*ab^*\right)^* \qquad (ab)^* \shuffle (ba)^* = (ab \cup ba)^*$$

$$a^* \shuffle b^* = \{a, b\}^* \qquad a \shuffle a^*.b.a^* = a^*.(ab \cup ba).a^*$$

Proposition
Falls L und M regulär sind, dann ist es auch $L \sqcup\!\sqcup M$.

Versuch 1
Veranschaulicht, wie Beweise mittels NFA-Konstruktion strukturiert sind. Der Beweis weist allerdings einige Lücken auf.

Seien $A = \langle Q_A, i_A, \to_A, F_A \rangle$ und $B = \langle Q_B, i_B, \to_B, F_B \rangle$ NFAs auf dem Alphabet Σ. Wir konstruieren einen neuen NFA $A \sqcup\!\sqcup B = \langle Q, i, \to, F \rangle$ mit $\mathcal{L}(A \sqcup\!\sqcup B) = \mathcal{L}(A) \sqcup\!\sqcup \mathcal{L}(B)$.

$$Q = Q_A \times Q_B \qquad i = \langle i_A, i_B \rangle \qquad F = F_A \times F_B$$

$$\langle p_A, p_B \rangle \xrightarrow{s} \langle q_A, q_B \rangle \text{ gdw. } \left(p_A \xrightarrow{s}_A p_A \wedge p_B = q_B\right) \vee \left(p_A = q_A \wedge p_B \xrightarrow{s}_B q_B\right)$$

Nun gilt es, die Korrektheit dieser Konstruktion zu zeigen.

Sei $x = x_1 \ldots x_k \in \mathcal{L}(A \sqcup\!\sqcup B)$. Dann gibt es einen akzeptierenden Lauf $i \xrightarrow{x_1} \langle a_1, b_1 \rangle \xrightarrow{x_2} \cdots \xrightarrow{x_k} \langle a_k, b_k \rangle \in F$. Dabei simuliert gemäß der obigen Konstruktion jede dieser Transitionen entweder eine A-Transition oder eine B-Transition, während der simulierte Zustand des jeweils anderen Automaten unverändert bleibt. Die Aneinanderreihung der A-Transitionen liefert nun ein *Subwort* $v \in \Sigma^*$ mit einen akzeptierenden Lauf $i_A \xrightarrow{v}{}^*_A a_k \in F_A$. Analog erhalten wir über den B-Transitionen das andere Subwort $w \in \Sigma^*$ und einen akzeptierenden Lauf $i_B \xrightarrow{w}{}^*_B b_k \in F_B$. [...] Jetzt beobachten wir $x \in v \sqcup\!\sqcup w \subseteq \mathcal{L}(A) \sqcup\!\sqcup \mathcal{L}(B)$.

Sei $x = x_1 \ldots x_k \in \mathcal{L}(A) \sqcup\!\sqcup \mathcal{L}(B)$, insbesondere $x \in v \sqcup\!\sqcup w$ mit $v = v_1 \ldots v_n \in \mathcal{L}(A)$ und $w = w_1 \ldots w_m \in \mathcal{L}(B)$ mit $n + m = k$. Dann gibt es akzeptierenden Läufe $i_A \xrightarrow{v_1}_A a_1 \xrightarrow{v_2}_A \cdots \xrightarrow{v_n}_A a_n \in F_A$ und $i_B \xrightarrow{w_1}_B b_1 \xrightarrow{w_2}_B \ldots \xrightarrow{w_m} b_m \in F_B$. [...] Nun existiert der Lauf $i \xrightarrow{x_1} q_1 \xrightarrow{x_2} \ldots \xrightarrow{x_k} q_k \in F$. Also wird x von $A \sqcup\!\sqcup B$ akzeptiert.

Versuch 2
Wir leiten den Shuffle mithilfe einiger Homomorphismen und einem Durchschnitt ab. Für jedes Paar aus Sprachen $L, M \subseteq \Sigma^*$ soll es ein Alphabet Σ' und geeignete Homomorphismen $f, g, h : \Sigma'^* \to \Sigma^*$ geben, sodass man die folgende Umformung erreicht.

$$L \sqcup\!\sqcup M = h\left(f^{-1}(L) \cap g^{-1}(M)\right)$$

Zunächst entledigen wir uns der Ambiguität, von welchem der beiden Seiten ein Buchstabe in einem Shuffle-Wort stammen. Dazu trennen wir die Alphabete beider Seiten. Das erweiterte Alphabet $\Sigma' = \Sigma \times 0, 1$ soll diese Information hergeben: Ein erweitertes Symbol $\langle s, 0 \rangle$ soll aussagen, dass das Symbol s aus einem Wort der Sprache L stammt. Mit 1 sind dementsprechend Symbole der Wörter aus K auszustatten.

Lemma 1
Seien $\Gamma \subseteq \Delta$ Alphabete und $v \in \Gamma^*$.

Wir definieren eine *Selektion* als einen Homomorphismus $\sigma_\Gamma : \Delta^* \to \Gamma^*$ buchstabenweise für alle $s \in \Delta$ mit $\sigma_\Gamma(s) = \begin{cases} s & s \in \Gamma \\ \varepsilon & s \notin \Gamma \end{cases}$.

Es gelten $\{v\} \sqcup\!\sqcup (\Delta \setminus \Gamma)^* = \sigma_\Gamma^{-1}(v) = (\Delta \setminus \Gamma)^* \sqcup\!\sqcup \{v\}$.

Beweis
Wir zeigen eine Gleichung induktiv, die andere folgt aus der Kommutativität des Shuffle.

Induktionsanfang: $\{\varepsilon\} \sqcup\!\sqcup \Delta^* = \Delta^* = \sigma_\Gamma^{-1}(\varepsilon)$.

Induktionsschluss: Sei $v = a.v'$ mit $a \in \Gamma$.

$$
\begin{aligned}
\{v\} \sqcup\!\sqcup (\Delta \setminus \Gamma)^* &= \bigcup_{w \in (\Delta\setminus\Gamma)^*} v \sqcup\!\sqcup w && \text{Def. Sprach-Shuffle}\\
&= v \sqcup\!\sqcup \varepsilon \cup \bigcup_{b.w' \in (\Delta\setminus\Gamma)^+} v \sqcup\!\sqcup bw' && \text{Kommutativität von } \cup\\
&= v.\varepsilon \cup \bigcup_{b.w' \in (\Delta\setminus\Gamma)^+} \left(a\left(v' \sqcup\!\sqcup bw'\right) \cup b\left(v \sqcup\!\sqcup w'\right)\right) && \text{Def. Wort-Shuffle}\\
&= v.\varepsilon \cup \bigcup_{b.w' \in (\Delta\setminus\Gamma)^+} a\left(v' \sqcup\!\sqcup bw'\right) \cup \bigcup_{b.w' \in (\Delta\setminus\Gamma)^+} b\left(v \sqcup\!\sqcup w'\right) && \text{Kommutativität von } \cup\\
&= a\left(v' \sqcup\!\sqcup \varepsilon\right) \cup \bigcup_{b.w' \in (\Delta\setminus\Gamma)^+} a\left(v' \sqcup\!\sqcup bw'\right) \cup \bigcup_{b.w' \in (\Delta\setminus\Gamma)^+} b\left(v \sqcup\!\sqcup w'\right) && v = a.v' \text{ und Def. Shuffle}\\
&= \bigcup_{w \in (\Delta\setminus\Gamma)^*} a\left(v' \sqcup\!\sqcup w\right) \cup \bigcup_{b.w' \in (\Delta\setminus\Gamma)^+} b\left(v \sqcup\!\sqcup w'\right) && \text{Kommutativität von } \cup\\
&= \bigcup_{w \in (\Delta\setminus\Gamma)^*} a\left(v' \sqcup\!\sqcup w\right) \cup (\Delta \setminus \Gamma) \bigcup_{w' \in (\Delta\setminus\Gamma)^*} \left(v \sqcup\!\sqcup w'\right) && \text{Kommu. + Distr.}\\
&= a \bigcup_{w \in (\Delta\setminus\Gamma)^*} \left(v' \sqcup\!\sqcup w\right) \cup (\Delta \setminus \Gamma) \bigcup_{w' \in (\Delta\setminus\Gamma)^*} \left(v \sqcup\!\sqcup w'\right) && \text{Distributivität}\\
&= (\Delta \setminus \Gamma)^* a \bigcup_{w \in (\Delta\setminus\Gamma)^*} \left(v' \sqcup\!\sqcup w\right) && \text{Ardens Lemma, vgl. mit Zeile 1}\\
&= (\Delta \setminus \Gamma)^* a \sigma_\Gamma^{-1}\left(v'\right) && \text{Induktionsvoraussetzung}\\
&= \sigma_\Gamma^{-1}(\varepsilon).a.\sigma_\Gamma^{-1}\left(v'\right) = \sigma_\Gamma^{-1}\left(a.v'\right) = \sigma_\Gamma^{-1}(v) && \text{Def. } \sigma_\Gamma
\end{aligned}
$$

Dadurch folgt die Aussage für alle $v \in \Gamma^*$. $\square$

Korollar 2
Für jede Sprache $L \subseteq \Gamma^*$ gilt $L \sqcup\!\sqcup \Delta^* = \sigma_\Gamma^{-1}(L)$.