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

$$L \sqcup\!\sqcup M = h(f(L) \cap g(M))$$

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.

**Lemma 1**
Seien $\Sigma$ ein Alphabet, $v, w \in \Sigma^*$ zwei Wörter.

Wir definieren die Homomorphismen $\rho_0, \rho_1 : \Sigma^* \to (\Sigma \times \{0, 1\})^*$ und $\pi_\Sigma : (\Sigma \times \{0, 1\})^* \to \Sigma^*$ buchstabenweise für alle $s \in \Sigma$ und $b \in \{0, 1\}$ mit $\rho_b(s) = \langle s, b\rangle$ und $\pi_\Sigma(\langle s, b\rangle) = s$.

Es gilt $v \sqcup\!\sqcup w = \pi_\Sigma(\rho_0(v) \sqcup\!\sqcup \rho_1(w))$.

**Beweis:**
Induktion über $v, w \in \Sigma^*$ (quasi über $|v| \cdot |w| \in \mathbb{N}$).

Zu Anfang betrachten wir $v = \varepsilon$ oder $w = \varepsilon$: Daraus folgt $\rho_0(v) = \varepsilon$ oder $\rho_1(w) = \varepsilon$.

$$\begin{aligned}
\pi_\Sigma(\rho_0(v) \sqcup\!\sqcup \rho_1(w)) &= \pi_\Sigma(\rho_0(v).\rho_1(w)) \\
&= \pi_\Sigma(\rho_0(v)).\pi_\Sigma(\rho_1(w)) \\
&= v.w \\
&= v \sqcup\!\sqcup w
\end{aligned}$$

Sei $1 < k \in \mathbb{N}$. Als Voraussetzung gelte $v' \sqcup\!\sqcup\, w' = \pi_\Sigma(\rho_0(v') \sqcup\!\sqcup\, \rho_1(w'))$ für alle $v', w' \in \Sigma^*$ mit $|v'| \cdot |w'| < k$. Seien $v = a.v'$, $w = b.w' \in \Sigma^*$ mit $a, b \in \Sigma$ und $|v| \cdot |w| = k$.

$$
\begin{aligned}
\pi_\Sigma(\rho_0(v) \sqcup\!\sqcup\, \rho_1(w)) &= \pi_\Sigma\big(\rho_0\big(a.v'\big) \sqcup\!\sqcup\, \rho_1\big(b.w'\big)\big) \\
&= \pi_\Sigma\big(\langle a, 0\rangle.\rho_0\big(v'\big) \sqcup\!\sqcup\, \langle b, 1\rangle.\rho_1\big(w'\big)\big) \\
&= \pi_\Sigma\big(\langle a, 0\rangle.\big(\rho_0\big(v'\big) \sqcup\!\sqcup\, \langle b, 1\rangle.\rho_1\big(w'\big)\big) \cup \langle b, 1\rangle.\big(\langle a, 0\rangle.\rho_0\big(v'\big) \sqcup\!\sqcup\, \rho_1\big(w'\big)\big)\big) \\
&= \pi_\Sigma\big(\langle a, 0\rangle.\big(\rho_0\big(v'\big) \sqcup\!\sqcup\, \rho_1(w)\big) \cup \langle b, 1\rangle.\big(\rho_0(v) \sqcup\!\sqcup\, \rho_1\big(w'\big)\big)\big) \\
&= \pi_\Sigma\big(\langle a, 0\rangle.\big(\rho_0\big(v'\big) \sqcup\!\sqcup\, \rho_1(w)\big)\big) \cup \pi_\Sigma\big(\langle b, 1\rangle.\big(\rho_0(v) \sqcup\!\sqcup\, \rho_1\big(w'\big)\big)\big) \\
&= a.\pi_\Sigma\big(\rho_0\big(v'\big) \sqcup\!\sqcup\, \rho_1(w)\big) \cup b.\pi_\Sigma\big(\rho_0(v) \sqcup\!\sqcup\, \rho_1\big(w'\big)\big) \\
&= a.\big(v' \sqcup\!\sqcup\, w\big) \cup b.\big(v \sqcup\!\sqcup\, w'\big) \\
&= v \sqcup\!\sqcup\, w
\end{aligned}
$$

Diese Aussage gilt nun für alle $k \in \mathbb{N}$ und somit für jedes Paar aus Wörtern. □

**Korollar 2**
Für alle Sprachen $L, M \subseteq \Sigma^*$ gilt $L \sqcup\!\sqcup\, M = \pi_\Sigma(\rho_0(L) \sqcup\!\sqcup\, \rho_1(M))$.

**Lemma 3**
Seien $\Gamma \cap \Delta = \varnothing$ disjunkte Alphabete und $v \in \Gamma^*$.

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

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

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

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

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

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

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

**Korollar 4**
Für jede Sprache $L \subseteq \Gamma^*$ gilt $L \sqcup\!\sqcup \Delta^* = \sigma_\Gamma^{-1}(L)$.

Wie die disjunkten Quell-Alphabete den Beweis vereinfachen, zeigt dieser nächste Schritt:

**Lemma 5**
Seien $v \in \Gamma^*$ und $w \in \Delta^*$ Wörter mit unterschiedlichen Buchstaben. Es gilt $v \sqcup\!\sqcup w = (\{v\} \sqcup\!\sqcup \Delta^*) \cap (\Gamma^* \sqcup\!\sqcup \{w\})$.

**Beweis:**
Sei $x \in v \sqcup\!\sqcup w$.

Anfang: Es gilt $\varepsilon \in v \sqcup\!\sqcup w$ genau dann, wenn $v = w = \varepsilon$, und damit auch genau dann, wenn $\varepsilon \in \{v\} \sqcup\!\sqcup \Delta^*$ und $\varepsilon \in \Gamma^* \sqcup\!\sqcup \{w\}$.

Schluss: Sei $x = a.x'$ mit $a \in \Gamma$.

$$\begin{aligned}
x \in v \sqcup\!\sqcup w &\iff v = a.v' \wedge x' \in v' \sqcup\!\sqcup w \\
&\iff v = a.v' \wedge x' \in \left(v' \sqcup\!\sqcup \Delta^*\right) \cap \left(\Gamma^* \sqcup\!\sqcup w\right) \\
&\iff v = a.v' \wedge x' \in v' \sqcup\!\sqcup \Delta^* \wedge x' \in \Gamma^* \sqcup\!\sqcup w \\
&\iff v = a.v' \wedge \left(x' \in v' \sqcup\!\sqcup \Delta^* \vee \text{false}\right) \wedge x' \in \Gamma^* \sqcup\!\sqcup w \\
&\iff v = a.v' \wedge \left(x' \in v' \sqcup\!\sqcup \Delta^* \vee x\text{false}\right) \wedge x' \in \Gamma^* \sqcup\!\sqcup w \\
&\iff x \in v \sqcup\!\sqcup \Delta^* \wedge x \in \Gamma^* \sqcup\!\sqcup w \\
&\iff x \in \left(v \sqcup\!\sqcup \Delta^*\right) \cap \left(\Gamma^* \sqcup\!\sqcup w\right)
\end{aligned}$$

□

**Korollar 6**
Für jedes Paar von Sprachen $L \subseteq \Gamma^*$ und $M \subseteq \Delta^*$ gilt $L \sqcup\!\sqcup M = (L \sqcup\!\sqcup \Delta^*) \cap (\Gamma^* \sqcup\!\sqcup M)$.

**Theorem 7**
Reguläre Sprachen sind unter der Shuffle-Operation abgeschlossen:

**Beweis:**
Es seien $L, M \subseteq \Sigma^*$ reguläre Sprachen. Wir nutzen das erweiterte Alphabet $\Gamma := \Sigma \times \{0, 1\}$. Damit ist $L \sqcup\!\sqcup M = \pi_\Sigma(\sigma_0^{-1}(\rho_0(L)) \cap \sigma_1^{-1}(\rho_1(M)))$ ist ebenfalls regulär. □

**Bemerkung:** Folgt man der Konstruktionsfolge für NFAs nach Bild-, Urbild-, und Produktautomaten, so entsteht für den Shuffle exakt der NFA, den wir letztes Mal konstruiert haben.