Theoretische Informatik HS23

Nicolas Wehrli

Übungsstunde 04

21. Oktober 2023

ETH Zürich
nwehrl@ethz.ch

Heute

1. Feedback zur Serie
2. Beweise für Nichtregularität
   - Kurze Wiederholung vom letzten Mal
   - Theorie für Nichtregularitätsbeweise - continued
   - Sprachen mit Einsymbolalphabet
3. Nichtdeterministische Endliche Automaten

Feedback zur Serie

Feedback

- Generell gut gelöst. War nicht das schwierigste Blatt.
- Aufpassen auf Flüchtigkeitsfehler!
- λ nicht vergessen!
- Macht euch bei den Klassen das Leben nicht schwer.

Beweise für Nichtregularität

Theorie für Nichtregularitätsbeweise - Lemma 3.3

Sei $A = (Q, \Sigma, \delta_A, q_0, F)$ ein EA. Seien $x, y \in \Sigma^*, x \neq y$, so dass

$$\hat{\delta}_A(q_0, x) = p = \hat{\delta}_A(q_0, y)$$

für ein $p \in Q$ (also $x, y \in \mathrm{Kl}[p]$). Dann existiert für jedes $z \in \Sigma^*$ ein $r \in Q$, so dass xz und $yz \in \mathrm{Kl}[r]$, also gilt insbesondere

$$xz \in L(A) \iff yz \in L(A)$$

Generelle Tips:

- Betrachtet $|Q| + 1$ Wörter für Pigeonhole-Principle.
- Geeigneten Suffix finden.

Theorie für Nichtreguläritätsbeweise - Pumping Lemma

Sei L regulär. Dann existiert eine Konstante $n_0 \in \mathbb{N}$, so dass jedes Wort $w \in \Sigma^*$ mit $|w| \geq n_0$ in drei Teile x, y und z zerlegen lässt, das heisst $w = yxz$, wobei

(i) $|yx| \leq n_0$

(ii) $|x| \geq 1$

(iii) entweder $\{yx^kz \mid k \in \mathbb{N}\} \subseteq L$ oder $\{yx^kz \mid k \in \mathbb{N}\} \cap L = \emptyset$.

Generelle Tips:

- Das gewählte Wort hängt sehr wahrscheinlich von n_0 ab.
- Es ist meist einfacher, das Wort so zu konstruieren, dass man nur ein Zeichen pumpt (i.e. x besteht nur aus einem Zeichen).
- Aufpassen auf Quantoren! Wir dürfen ein Wort wählen (mit Länge $\geq n_0$) und müssen dann zeigen, dass **keine** Partition davon existiert, die (i)-(iii) erfüllt.

Beispielaufgabe 1 - Pumping Lemma

Versuchen wir zu beweisen, dass

$$L_2 = \{wabw^{\mathbf{R}} \mid w \in \{a, b\}^*\}$$

nicht regulär ist.

Beispielaufgabe 1 - Pumping Lemma

Wir nehmen zum Widerspruch an, dass L_2 regulär ist.

Das Pumping-Lemma (Lemma 3.4) besagt, dass dann eine Konstante $n_0 \in \mathbb{N}$ existiert, so dass sich jedes Wort $w \in \Sigma*$ mit $|w| \geq n_0$ in drei Teile y, x, und z zerlegen lässt. ($\implies w = yxz$). Wobei folgendes gelten muss:

(i) $|yx| \leq n_0$
(ii) $|x| \geq 1$
(iii) **entweder** $\{yx^kz \mid k \in \mathbb{N}\} \subseteq L_2$ **oder** $\{yx^kz \mid k \in \mathbb{N}\} \cap L_2 = \emptyset$

Beispielaufgabe 1 - Pumping Lemma

Wir wählen $w = a^{n_0}aba^{n_0}$. Es ist leicht zu sehen das $|w| = 2n_0 + 2 \geq n_0$.

Da nach (i), $|yx| \leq n_0$ gelten muss, haben wir $y = a^l$ und $x = a^m$ für beliebige $l, m \in \mathbb{N}, l + m \leq n_0$.
Somit gilt $z = a^{n_0-(l+m)}aba^{n_0}$

Nach (ii) ist $m \geq 1$.

Wir haben also $\{yx^kz \mid k \in \mathbb{N}\} = \{a^{n_0-m+km}aba^{n_0} \mid k \in \mathbb{N}\}$

Beispielaufgabe 1 - Pumping Lemma

Da $yx^1z = a^{n_0}aba^{n_0}$ und

$a^{n_0}aba^{n_0} \in \{a^{n_0-m+km}aba^{n_0} \mid k \in \mathbb{N}\} \wedge a^{n_0}aba^{n_0} \in L_2$ gilt, folgt

$$\{a^{n_0-m+km}aba^{n_0} \mid k \in \mathbb{N}\} \cap L_2 \neq \emptyset$$

Wenn wir nun $k = 0$ wählen und uns daran erinnern, dass $m \geq 1$, erhalten wir folgendes

$$\Rightarrow yx^0z = yz = a^{n_0-m}aba^{n_0} \notin L_2$$

Daraus folgt,

$$\{a^{n_0-m+km}aba^{n_0} \mid k \in \mathbb{N}\} \nsubseteq L_2$$

Somit gilt (iii) nicht.

Dies ist ein Widerspruch! Somit haben wir gezeigt, dass die Sprache $L_2 = \{wabw^{\mathbf{R}} \mid w \in \{a,b\}^*\}$ nicht regulär ist.

Theorie für Nichtregularitätsbeweise - Satz 3.1 (Kolmogorov)

> Sei $L \subseteq (\Sigma_{\text{bool}})^*$ eine reguläre Sprache. Sei $L_x = \{y \in (\Sigma_{\text{bool}})^* \mid xy \in L\}$ für jedes $x \in (\Sigma_{\text{bool}})^*$. Dann existiert eine Konstante **const**, so dass für alle $x, y \in (\Sigma_{\text{bool}})^*$
>
> $$K(y) \leq \lceil \log_2(n+1) \rceil + \textbf{ const},$$
>
> falls y das n-te Wort in der Sprache L_x ist.

Wie wir sehen werden, beruht der Nichtregularitätsbeweis darauf, dass die Differenz von $|w_{n+1}| - |w_n|$ für kanonische Wörter $(w_i)_{i \in \mathbb{N}}$ beliebig gross werden kann.

Beispielaufgabe 2 - Kolmogorov Methode

Verwenden Sie die Methode der Kolmogorov-Komplexität, um zu zeigen, dass die Sprache

$$L_1 = \{0^{n^2 \cdot 2^n} \mid n \in \mathbb{N}\}$$

nicht regulär ist.

Beispielaufgabe 2 - Kolmogorov Methode

Angenommen L_1 sei regulär.

Wir betrachten

$$L_{0^{m^2 \cdot 2^m + 1}} = \{y \mid 0^{m^2 \cdot 2^m + 1} y \in L_1\}.$$

Da

$$\begin{aligned}(m+1)^2 \cdot 2^{m+1} &= (m^2 + 2m + 1) \cdot 2^{m+1} \\ &= m^2 \cdot 2^m + m^2 \cdot 2^m + (2m+1) \cdot 2^{m+1} \\ &= m^2 \cdot 2^m + (m^2 + 4m + 2) \cdot 2^m\end{aligned}$$

ist für jedes $m \in \mathbb{N}$ das Wort $y_1 = 0^{(m^2+4m+2) \cdot 2^m - 1}$ das kanonisch erste Wort der Sprache $L_{0^{m^2 \cdot 2^m + 1}}$.

Beispielaufgabe 2 - Kolmogorov Methode

Nach Satz 3.1 existiert eine Konstante c, unabhängig von m, so dass

$$K(y_1) \leq \lceil \log_2(1+1) \rceil + c = 1 + c.$$

Die Anzahl aller Programme, deren Länge kleiner oder gleich $1 + c$ sind, ist endlich.

Da es aber unendlich viel Wörter der Form $0^{(m^2+4m+2)\cdot 2^m - 1}$ gibt, ist dies ein Widerspruch.

Demzufolge ist L_1 nicht regulär.

$\blacksquare$

Beispielaufgabe 3 - Direkte Methode (Lemma 3.3)

Verwende eine direkte Argumentation über den Automaten (unter Verwendung von Lemma 3.3), um zu zeigen, dass die Sprache

$$L_2 = \{w \in \{0,1\}^* \mid |u|_0 \leq |u|_1 \text{ für alle Präfixe } u \text{ von } w\}$$

nicht regulär ist.

Beispielaufgabe 3 - Direkte Methode (Lemma 3.3)

Angenommen L_2 sei regulär.

Dann existiert ein Endlicher Automat $A = (Q, \{0,1\}, \delta, q_0, F)$ mit $L(A) = L_2$.

Wir betrachten die Wörter

$$1, 1^2, ..., 1^{|Q|+1}$$

Per Pigeonhole-Principle existiert $i, j \in \{1, ..., |Q| + 1\}$ mit $i < j$, so dass

$$\hat{\delta}(q_0, 1^i) = \hat{\delta}(q_0, 1^j).$$

Nach Lemma 3.3 gilt nun für alle $z \in \{0,1\}^*$

$$1^i z \in L_2 \iff 1^j z \in L_2$$

Beispielaufgabe 3 - Direkte Methode (Lemma 3.3)

Sei $z = 0^j$. Wir haben dann also

$$1^i z = 1^i 0^j \notin L_2,$$

da $i < j$ und ein Wort auch ein Präfix von sich selbst ist (Die Bedingung $|1^i 0^j|_0 \leq |1^i 0^j|_1$ wird verletzt). Aber wir haben auch

$$1^j z = 1^j 0^j \in L_2,$$

was zu einem Widerspruch führt. Also ist die Annahme falsch und L_2 nicht regulär.

$\blacksquare$

Sprachen mit Einsymbolalphabet

Angenommen es handelt sich bei $L \subseteq \Sigma^*$ um eine Sprache über einem unären Alphabet ($|\Sigma| = 1, \Sigma = \{x\}$).

Dann gilt:

$$\forall w \in \Sigma^* : w = x^{|w|}$$

Insbesondere gibt es für jede Länge nur ein Wort.

Sei die Folge $(w_i)_{i \in \mathbb{N}}$ kanonisch geordnet, so dass $w_i \in L$ (Wenn L endlich betrachten wir nur endlich viele Wörter der Folge).

Durch das gilt folgendes

$$\forall w \in \Sigma^*.\ \forall k \in \mathbb{N}.\ |w_k| < |w| < |w_{k+1}| \implies w \notin L$$

Beispielaufgabe 4 - Pumping Lemma

Zeigen Sie, dass

$$L = \{0^{n \cdot \lceil \sqrt{n} \rceil} \mid n \in \mathbb{N}\}$$

nicht regulär ist.

Beispielaufgabe 4 - Pumping Lemma

Angenommen $L = \{0^{0\cdot\lceil\sqrt{0}\rceil}, 0^{1\cdot\lceil\sqrt{1}\rceil}, 0^{2\cdot\lceil\sqrt{2}\rceil}, ...\}$ sei regulär.

Seien $w_0, w_1, w_2, ...$ die Wörter von L in kanonischer Reihenfolge. Nach dem Pumping Lemma gibt es ein $n_0 \in \mathbb{N}$, dass die Bedingungen (i)-(iii) erfüllt sind.

Wir wählen $w = w_{n_0^2} = 0^{n_0^2\lceil\sqrt{n_0^2}\rceil} \in L$.

Es ist leicht zu sehen das $|w| \geq n_0$ und folglich existiert eine Aufteilung $w = yxz$ ($y = 0^l$, $x = 0^m$ und $z = 0^{n_0^2\lceil\sqrt{n_0^2}\rceil - l - m}$), die (i)-(iii) erfüllt.

Da nach (i) $|yx| = l + m \leq n_0$, folgt $|x| = m \leq n_0$.

Aus (ii) folgt $|x| = m \geq 1$.

Beispielaufgabe 4 - Pumping Lemma

Wegen $|yx^2z| = |yxz| + |x|$ gilt also $|yxz| < |yx^2z| \leq |yxz| + n_0$.

Das nächste Wort in L nach $w_{n_0^2}$ ist $w_{n_0^2+1}$ und es gilt

$$\begin{aligned}
|w_{n_0^2+1}| - |w_{n_0^2}| &= (n_0^2 + 1) \cdot \lceil \sqrt{n_0^2 + 1} \rceil - n_0^2 \cdot \lceil \sqrt{n_0^2} \rceil \\
&= (n_0^2 + 1) \cdot \lceil \sqrt{n_0^2 + 1} \rceil - n_0^2 \cdot n_0 \\
&> (n_0^2 + 1) \cdot n_0 - n_0^3 \\
&= n_0
\end{aligned}$$

Die strikte Ungleichung gilt da $n_0 \in \mathbb{N}$ und $n_0 = \left\lceil \sqrt{n_0^2} \right\rceil < \sqrt{n_0^2 + 1} \leq \left\lceil \sqrt{n_0^2 + 1} \right\rceil$.

$$\implies |w_{n_0^2+1}| \geq |w_{n_0^2}| + (n_0 + 1)$$

Beispielaufgabe 4 - Pumping Lemma

Somit gilt

$$|w_{n_0^2}| < |yx^2z| < |w_{n_0^2+1}|$$

Daraus folgt $yx^2z \notin L$, während $yxz \in L$, in Widerspruch zu (iii).

$\blacksquare$

Beispielaufgabe 5 - Kolmogorov Methode

Zeigen Sie, dass

$$L = \{0^{n \cdot \lceil \sqrt{n} \rceil} \mid n \in \mathbb{N}\}$$

nicht regulär ist.

Beispielaufgabe 5 - Kolmogorov Methode

Widerspruchsannahme: Sei L regulär.

Wir betrachten

$$L_{0^{m\cdot\lceil\sqrt{m}\rceil+1}} = \{y \in \Sigma^* \mid 0^{m\cdot\lceil\sqrt{m}\rceil+1}y \in L\}$$

Dann ist für jedes $m \in \mathbb{N}$ das Wort

$$y_1 = 0^{(m+1)\cdot\lceil\sqrt{m+1}\rceil-(m\cdot\lceil\sqrt{m}\rceil+1)}$$

das kanonisch erste Wort der Sprache $L_{0^{m\cdot\lceil\sqrt{m}\rceil+1}}$.

Beispielaufgabe 5 - Kolmogorov Methode

Nach Satz 3.1 existiert eine Konstante c, so dass gilt

$$K(y_1) \leq \lceil \log_2(1+1) \rceil + c = 1 + c$$

für jedes $m \in \mathbb{N}$.

Da die Länge von $|y_1|$

$$\begin{aligned} |y_1| &= (m+1) \cdot \lceil \sqrt{m+1} \rceil - (m \cdot \lceil \sqrt{m} \rceil + 1) \\ &\geq (m+1) \cdot \lceil \sqrt{m} \rceil - m \cdot \lceil \sqrt{m} \rceil - 1 \\ &= \lceil \sqrt{m} \rceil - 1 \overset{m \to \infty}{\longrightarrow} \infty \end{aligned}$$

beliebig gross werden kann, gibt es unendlich viele Wörter von dieser Form.

Dies ist ein Widerspruch, da es nur endlich viele Programme der Länge maximal $1 + c$ geben kann.

Nichtdeterministische Endliche Automaten

Definition NEA

Ein **nichtdeterministischer endlicher Automat (NEA)** ist ein Quintupel $M = (Q, \Sigma, \delta, q_0, F)$. Dabei ist

(i) Q eine endliche Menge, **Zustandsmenge** genannt,

(ii) Σ ein Alphabet, **Eingabealphabet** genannt,

(iii) $q_0 \in Q$ der **Anfangszustand**,

(iv) $F \subseteq Q$ die Menge der **akzeptierenden Zustände** und

(v) δ eine Funktion von $Q \times \Sigma$ nach $\mathcal{P}(Q)$, **Übergangsfunktion genannt**.

Ein NEA kann zu einem Zustand q und einem gelesenen Zeichen a mehrere oder gar keinen Nachfolgezustand haben.

Konfigurationen für NEAs

Eine **Konfiguration** von M ist ein Tupel $(q, w) \in Q \times \Sigma^*$.

- "M befindet sich in einer Konfiguration $(q, w) \in Q \times \Sigma^*$, wenn M im Zustand q ist und noch das Suffix w eines Eingabewortes lesen soll."
- Die Konfiguration $(q_0, x) \in \{q_0\} \times \Sigma^*$ ist die **Startkonfiguration für das Wort** x.

Ein **Schritt** von M ist eine Relation (auf Konfigurationen) $\vdash_M \subseteq (Q \times \Sigma^*) \times (Q \times \Sigma^*)$, definiert durch

$$(q, w) \vdash_M (p, x) \iff w = ax, a \in \Sigma \text{ und } p \in \delta(q, a)$$

Berechnungen für NEAs

Eine **Berechnung von M** ist eine endliche Folge $C_1, \dots, C_k$ von Konfigurationen, so dass

$$C_i \vdash_M C_{i+1} \text{ für alle } 1 \leq i \leq k.$$

Eine **Berechnung von M auf x** ist eine Berechnung $C = C_0, \dots, C_m$, wobei $C_0 = (q_0, x)$ und **entweder** $C_m \in Q \times \{\lambda\}$ **oder** $C_m = (q, ay)$ für ein $a \in \Sigma, y \in \Sigma^*$ und $q \in Q$, so dass $\delta(q, a) = \emptyset$.

Falls $C_m \in F \times \{\lambda\}$, sagen wir, dass C eine **akzeptierende Berechnung** von M auf x ist, und dass M **das Wort** x **akzeptiert**.

Weitere Definitionen

Die Relation $\vdash^*_M$ ist die reflexive und transitive Hülle von $\vdash_M$, genau wie bei einem EA.

Wir definieren

$$\mathbf{L}(\mathbf{M}) = \{w \in \Sigma^* \mid (q_0, w) \vdash^*_M (p, \lambda) \text{ für ein } p \in F\}$$

als die **von M akzeptierte Sprache.**

Zu der Übergangsfunktion δ definieren wir die Funktion $\hat{\delta} : (Q \times \Sigma^*) \to \mathcal{P}(Q)$ wie folgt:

(i) $\hat{\delta}(q, \lambda) = \{q\}$ für alle $q \in Q$

(ii) $\hat{\delta}(q, wa) = \bigcup_{r \in \hat{\delta}(q,w)} \delta(r, a)$ für alle $q \in Q, a \in \Sigma, w \in \Sigma^*$.