Myhill-Nerode-Äquivalenz

Niklas Rieken

June 7, 2016

Bisher sind reguläre Sprachen durch Formalismen wie reguläre Ausdrücke und endliche Automaten charakterisiert worden. Nun soll eine Eigenschaft gefunden werden, die reguläre Sprachen auf einer stark mathematisch-strukturellen Ebene charakterisiert, d.h. mit Aussagen, die sich auf die Struktur

$$(\Sigma^*, \cdot, \varepsilon)$$

beziehen. Diese Struktur bezeichnet man auch als *Wortmonoid*.

Grundlegende Überlegungen

Bevor wir zur eigentlichen Definition der Myhill-Nerode-Äquivalenz kommen, wiederholen wir ein paar Definitionen:

Definition 1. Eine **Äquivalenzrelation** über einer Menge A ist eine zweistelltige Relation $\sim \subseteq A \times A$, die

(i) reflexiv (für alle x gilt $x \sim x$),

(ii) symmetrisch (wenn $x \sim y$ dann auch $y \sim x$) und

(iii) transitiv (wenn $x \sim y$ und $y \sim z$ dann auch $x \sim z$)

ist.

Da die Myhill-Nerode-Relation eigentlich sogar etwas mehr ist, hier noch eine weitere Definition:

Definition 2. Sei A eine Menge und $\circ$ eine zweistellige Funktion auf A. Eine Relation $\sim \subseteq A \times A$ heißt **rechtsseitige Kongruenz** (bezüglich $\circ$), wenn

(i) $\sim$ eine Äquivalenzrelation ist und

(ii) $\circ$ diese Relation respektiert (d.h. für alle $x \sim y$ und alle $z \in A$ gilt $x \circ z \sim y \circ z$).

Die Myhill-Nerode-Äquivalenz ist definiert durch:

Definition 3. Sei Σ ein Alphabet und $L \subseteq \Sigma^*$. Seien $u, v \in \Sigma^*$. u und v heißen **Myhill-Nerode-äquivalent** ($u \sim_L v$) genau dann, wenn für alle $w \in \Sigma^*$ gilt, dass $uw \in L$ g.d.w. $vw \in L$.

Diese Relation ist streng genommen nicht nur eine Äquivalenz sondern auch eine rechtsseitige (!) Kongruenz, deswegen sind auch die Begriffe *Myhill-Nerode-Rechtskongruenz* und – nicht ganz korrekterweise – *Myhill-Nerode-Kongruenz* gebräuchlich.

Eine einfacher Folgerung aus der Definition ist

Lemma 4. *Sei $L \subseteq \Sigma^*$ eine Sprache. Für alle $u, v, w \in \Sigma^*$ mit $u \sim_L v$ gilt*

$$uw \sim_L vw.$$

Zuletzt der Begriff der Äquivalenzklasse:

Definition 5. Sei A eine Menge und $\sim \subseteq A \times A$ eine Äquivalenzrelation. Eine Menge $A' \subseteq A$ heißt **Äquivalenzklasse**, wenn

(i) Wenn $a \in A'$ und $b \sim a$, dann ist auch $b \in A'$,

(ii) Für alle $a, b \in A'$ gilt $a \sim b$.

Man benennt Äquivalenzklassen auch durch einzelne Repräsentanten, z.B. mit $[u]_L$ oder $u/_L$ für die Äquivalenzklasse in der alle Elemente enthalten sind, die zu u äquivalent sind. Die Vereinigung aller Äquivalenzklassen zu einer Äquivalenz über einer Menge A bildet stets eine Partition von A.

Finden der Äquivalenzklassen

Lemma 4 kann dafür verwendet werden um Äquivalenzklassen (der Myhill-Nerode-Äquivalenz $\sim_L$) zu finden. Wir gehen dabei wie folgt vor:
Wir starten mit dem leeren Wort ε und der zugehörigen Äquivalenzklasse $[\varepsilon]_L$. Danach wiederholen wir folgende Schritte bis keine neue Äquivalenzklassen mehr gefunden werden:
Für jedes Symbol $a \in \Sigma$ und jede bisher gefundene Äquivalenzklasse $[u]_L$ betrachte die Äquivalenzklasse $[ua]_L$. Ist $[ua]_L = [v]_L$ für eine bereits gefundene Äquivalenzklasse, passiert nichts. Ist dies nicht der Fall, fügen wir $[ua]_L$ als neue Äquivalenzklasse hinzu.

Beachte, dass dieses Verfahren nur für reguläre Sprachen terminiert. Nicht-reguläre Sprachen haben unendlich viele Äquivalenzklassen (s. Satz 6).

Dazu machen wir ein Beispiel. Sei

$$L = \{w \in \{a, b\}^* \mid w \text{ beginnt mit } b \text{ und nach jedem } a \text{ folgt sofort ein } b\}.$$

- Jedes Wort aus $\{a, b\}^*$ hat eine Äquivalenzklasse, also auch ε. Wir bezeichnen diese mit $[\varepsilon]_L$.

- Betrachte nun $[\varepsilon a]_L = [a]_L$. Es ist $[a]_L \neq [\varepsilon]_L$ (also $a \not\sim_L \varepsilon$), da b die Wörter trennt, d.h. $a \cdot b \notin L$, aber $\varepsilon \cdot b \in L$. d.h. $[a]_L$ ist eine neue Äquivalenzklasse.

- Betrachte nun $[\varepsilon b]_L = [b]_L$. Es ist $[b]_L \neq [\varepsilon]_L$, da ε die Wörter trennt, d.h. $b \cdot \varepsilon \in L$, aber $\varepsilon \cdot \varepsilon \notin L$. Außerdem $[b]_L \neq [a]_L$, weil ε die Wörter trennt, d.h. $b \cdot \varepsilon \in L$, aber $a \cdot \varepsilon \notin L$.

- Betrachte nun $[aa]_L$. Es ist $[aa]_L = [a]_L$, da es kein trennendes Wort gibt (egal, was man anhängt, man kann nicht mehr in der Sprache landen in beiden Fällen, da das Wort nicht mit b beginnt).

- Betrachte nun $[ab]_L$. Es ist $[ab]_L = [a]_L$, da es kein trennendes Wort gibt (egal, was man anhängt, man kann nicht mehr in der Sprache landen in beiden Fällen, da das Wort nicht mit b beginnt).

- Betrachte nun $[ba]_L$. Dies ist eine neue Äquivalenzklasse, da $ba \not\sim_L \varepsilon$ (trennendes Wort ε), $ba \not\sim_L a$ (trennendes Wort b) und $ba \not\sim_L b$ (trennendes Wort ε).

- Betrachte nun $[bb]_L$. Es ist $[bb]_L = [b]_L$, da es kein trennendes Wort gibt.

- Die Klassen $[aaa]_L, [aab]_L, [aba]_L, [abb]_L, [bba]_L, [bbb]_L$ müssen wir nicht mehr betrachten, da diese nach Lemma 4 mit $[a]_L, [a]_L, [a]_L, [a]_L, [ba]_L, [b]_L$ zusammenfallen (z.B. $[bb \cdot a]_L = [b \cdot a]_L$, da $bb \sim_L b$ und $\sim_L$ ist rechtsseitige Kongruenzrelation bzgl. $\cdot$).

- Berachte nun $[baa]_L$. Hier gilt. $[baa]_L = [a]_L$, da es kein trennendes Wort gibt (egal was wir anhängen, wir landen nicht mehr in der Sprache, da au für jedes u nicht mit b beginnt und $baau$ für jedes u das Infix aa besitzt (oder: es ein a gibt auf das kein b folgt)).

- Betrachte nun $[bab]_L$. Es ist $[bab]_L = [b]_L$, da es kein trennendes Wort gibt.

- Damit sind alle Äquivalenzklassen gefunden: $[\varepsilon]_L, [a]_L, [b]_L, [ba]_L$. Dieser Punkt ist für Studenten oft erstmal schwierig zu sehen. Es folgt aber direkt aus der rechtsseitigen Kongruenz bzw. Lemma 4. Egal welches Wort wir betrachten, wir können es einer dieser Äquivalenklassen zuordnen.

Wofür ist das nützlich?

Die Myhill-Nerode-Äquivalenz ist inhaltlich eines der schönsten Sachen in FoSAP, weil sie 1. eine notwendige und hinreichende Bedingung liefert, dass eine Sprache regulär ist und weil sie 2. auch einen direkten Weg zu einem minimalen deterministischen endlichen Automaten liefert.

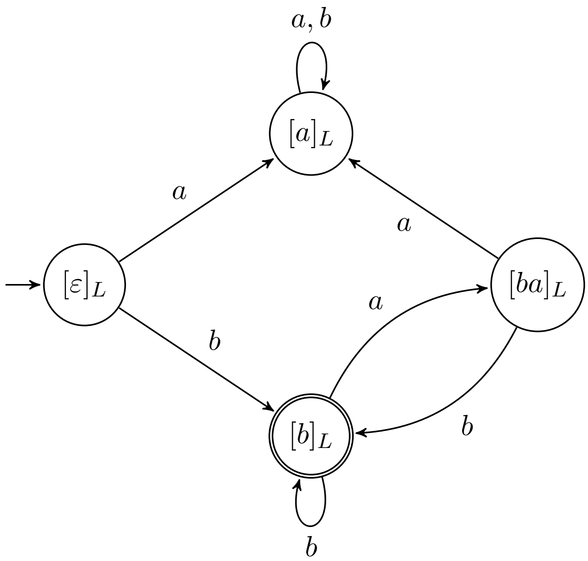

Figure 1: Minimaler DFA für die Sprache L.

Theorem 6 (Satz von Nerode)**.** *Eine Sprache ist genau dann regulär, wenn die Anzahl der Myhill-Nerode-Äquivalenzklassen endlich ist.*

Man schreibt auch $index(\sim_L) < \infty$. Die Sprache L im Beispiel hat $index(\sim_L) = 4 < \infty$ und ist somit regulär. Betrachte nun ein Standardbeispiel für eine nicht-reguläre Sprache

$$K = \{a^n b^n : n \in \mathbb{N}\}.$$

K ist nicht regulär. Betrachte die Wörter $u_i = a^i$ und $u_j = a^j$ mit $i \neq j$. Es gilt offensichtlich $u_i \not\sim_K u_j$, denn das Wort b^i trennt die Wörter, weil $u_i b^i = a^i b^i \in K$, aber $u_j b^i = a^j b^i \notin K$. Da es unendlich viele $i, j \in \mathbb{N}$ mit $i \neq j$ gibt, gibt es auch unendlich viele Äquivalenzklassen. Also ist K nach dem Satz von Nerode nicht regulär.

Theorem 7. *Der minimale DFA zu einer reguläre Sprache L ist isomorph zum Myhill-Nerode-DFA:*

$$\mathcal{A}_L = (\Sigma^*/_L, \Sigma, \delta, [\varepsilon]_L, \{[u]_L : u \in L\}),$$

mit $\delta([u]_L, a) = [ua]_L$.

Für die Sprache L erhalten wir also den DFA in Abbildung 1.