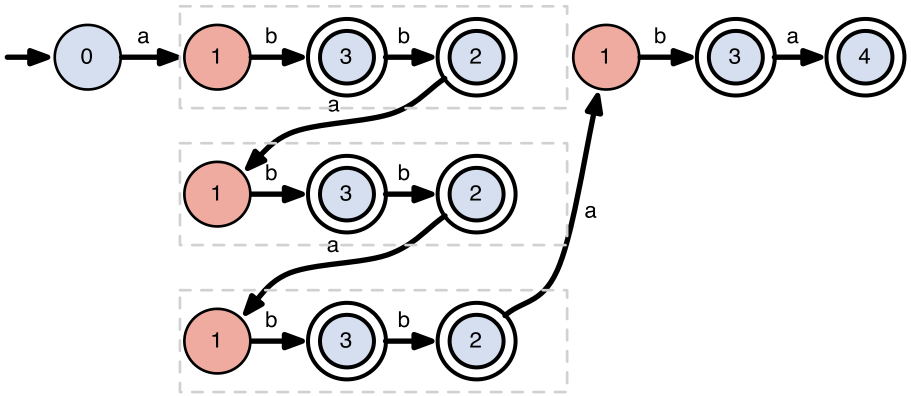
Berechenbarkeitstheorie

6. Vorlesung



Dr. Franziska Jahnke
Institut für Mathematische Logik und Grundlagenforschung
WWU Münster

Erinnerung: MN-Relation

Definition

Sei L eine Sprache über Σ. Die **Myhill-Nerode Relation (MN-Relation)** $\equiv_L$ zu L ist definiert als

$$\forall u, v \in \Sigma^* : \quad u \equiv_L v :\Longleftrightarrow \forall z \in \Sigma^* : uz \in L \Leftrightarrow vz \in L.$$

Eigenschaften

- $\equiv_L$ ist eine Äquivalenzrelation (transitiv, symmetrisch, reflexiv)
- $\equiv_L$ ist eine Rechtskongruenz
- $\equiv_L$ saturiert L

Lemma (letztes Mal)

Wenn die MN-Relation einer Sprache L endlichen Index (d.h. endlich viele Äquivalenzklassen) hat, dann ist L regulär.

Die Relation eines DEA

Definition

Sei $M = (Q, \Sigma, \delta, q_0, F)$ ein DEA. Die **Relation von M** $\equiv_M$ ist definiert als

$$\forall u, v \in \Sigma^* : \quad u \equiv_M v :\iff \delta^*(q_0, u) = \delta^*(q_0, v).$$

D.h. u, v stehen in Relation, wenn ihre Läufe im gleichen Zustand enden.

Eigenschaften

- $\equiv_M$ ist eine Äquivalenzrelation (transitiv, symmetrisch, reflexiv)
- $\equiv_M$ ist eine Rechtskongruenz
- $\equiv_M$ saturiert L
- $\equiv_M$ hat Index $|Q|$

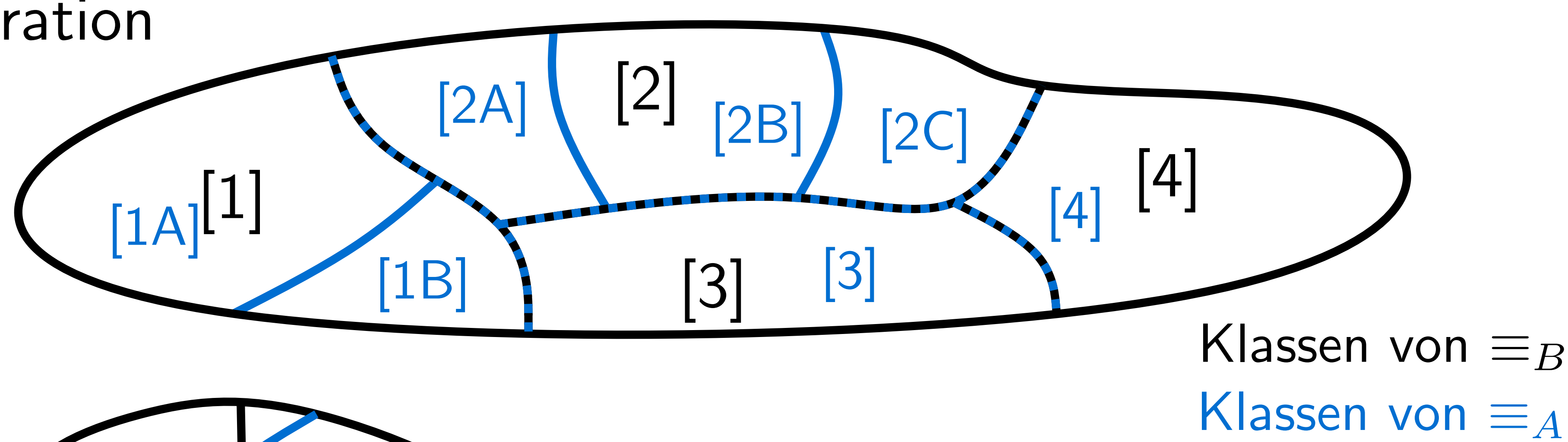
Verfeinerungen

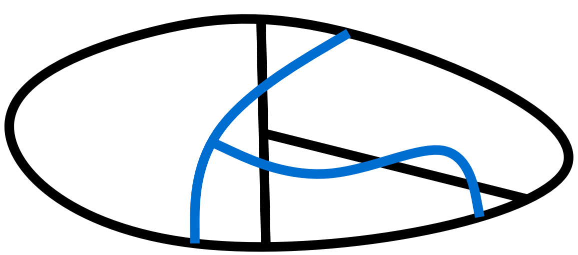
Definition

Seien $\equiv_A$ und $\equiv_B$ zwei Äquivalenzrelationen.
Wir sagen $\equiv_A$ **verfeinert** $\equiv_B$, gdw.

$$x \equiv_A y \implies x \equiv_B y.$$

Illustration





Nicht erlaubt!!

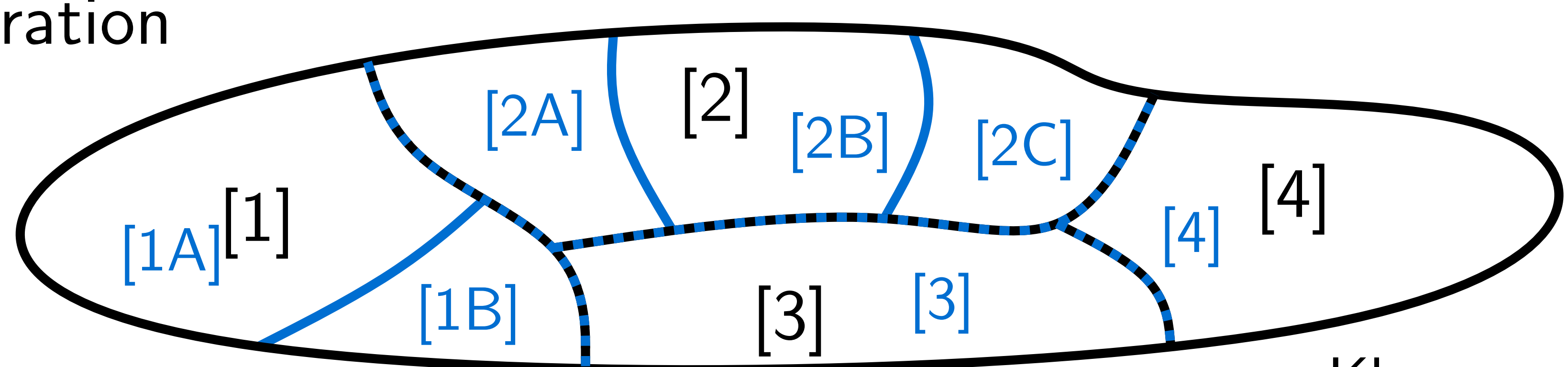
Verfeinerungen

Definition

Seien $\equiv_A$ und $\equiv_B$ zwei Äquivalenzrelationen.
Wir sagen $\equiv_A$ **verfeinert** $\equiv_B$, gdw.

$$x \equiv_A y \implies x \equiv_B y.$$

Illustration



Klassen von $\equiv_B$
Klassen von $\equiv_A$

Bsp. $a \; R_3 \; b :\iff a \equiv b \mod 3$
$a \; R_6 \; b :\iff a \equiv b \mod 6$

$\rightarrow R_6$ verfeinert R_3

Lemma 4

$$\equiv_M \text{ ist eine Verfeinerung von } \equiv_{L(M)}$$

Beweis

Wir zeigen etwas Stärkeres:
Jede Rechtskongruenz $\equiv$, die L saturiert, verfeinert $\equiv_L$

$$u \equiv v \implies \forall z \in \Sigma^*: (uz \equiv vz) \qquad \text{Eigenschaft (4')}$$

$$\implies \forall z \in \Sigma^*: (uz \in L \Leftrightarrow vz \in L) \qquad \text{Eigenschaft (5)}$$

$$\implies u \equiv_L v \qquad \text{Def. } \equiv_L$$

$\rightarrow \quad \equiv_M$ verfeinert $\equiv_{L(M)}$ $\square$

Konsequenz: M hat nicht weniger Zustände als $M(\equiv_{L(M)})$
$M(\equiv_{L(M)})$ ist ein minimaler DEA

Satz 6 (Satz von Myhill–Nerode)

$$L \in \text{REG} \iff \equiv_L \text{ hat endlichen Index}$$

Beweis $(\Rightarrow)$

$$\begin{aligned} L \in \text{REG} &\Rightarrow \exists \text{DEA } M : L(M) = L \\ &\Rightarrow \equiv_M \text{ saturiert } L \\ &\Rightarrow \equiv_M \text{ verfeinert } \equiv_L \\ &\Rightarrow \text{Index} \equiv_L \leq \text{Index} \equiv_M < \infty \end{aligned}$$

Lemma 4

Beweis $(\Leftarrow)$

$\equiv_L$ hat endlichen Index $\Rightarrow M(\equiv_L)$ ist DEA der L erkennt

(nach Lemma 3)

$\Rightarrow L$ ist regulär □

Satz 7

Sei M ein kollabierter Automat, dann gilt M und $M(\equiv_{L(M)})$ sind isomorph.

Beweis Wenn M kollabiert gilt: $\forall p, q \in Q\colon p \approx q \iff p = q \qquad (*)$

Erinnerung: $p \approx q$ wenn $\forall z \in \Sigma^*\colon \quad \delta^*(p,z) \in F \Leftrightarrow \delta^*(q,z) \in F$

$$
\begin{aligned}
x \equiv_{L(M)} y &\iff \forall z \in \Sigma^*(xz \in L \Leftrightarrow yz \in L) && \text{Def } \equiv_L \\
&\iff \forall z \in \Sigma^*(\delta^*(q_0, xz) \in F \Leftrightarrow \delta^*(q_0, yz) \in F) && \text{Def. Akz.} \\
&\iff \forall z \in \Sigma^*(\delta^*(\delta^*(q_0, x), z) \in F \Leftrightarrow \delta^*(\delta^*(q_0, y), z) \in F) && \\
&\iff \delta^*(q_0, x) \approx \delta^*(q_0, y) && \text{Def. } \approx \\
&\iff \delta^*(q_0, x) = \delta^*(q_0, y) && \text{folgt aus } (*) \\
&\iff x \equiv_M y && \text{Def } \equiv_M
\end{aligned}
$$

Das heißt, $\equiv_M$ und $\equiv_{L(M)}$ stimmen in ihren Äquivalenzklassen überein

Bijektion

Sei $M = (Q, \Sigma, \delta, q_0, F)$ der kollabierte DEA und
$M(\equiv_{L(M)}) = (Q', \Sigma, \delta', q_0', F')$

für ein z mit $\delta^*(q_0, z) = q$

$$\underbrace{q \in Q \underbrace{\overset{1:1}{\longleftrightarrow}}_{\text{Umbennenung}} [z]_{\equiv_M} \overset{1:1}{\longleftrightarrow} [z]_{\equiv_{L(M)}} \overset{1:1}{\longleftrightarrow} [z]_{\equiv_{L(M)}} \in Q'}_{\text{Bijektion}}$$

Übergänge

$$\delta(q,a) = p \overset{1:1}{\longleftrightarrow} \delta([z]_{\equiv_M}, a) = [za]_{\equiv_M} \overset{1:1}{\longleftrightarrow} \delta'([z]_{\equiv_{L(M)}}, a) = [za]_{\equiv_{L(M)}}$$

Startzustand

$$q_0 \overset{1:1}{\longleftrightarrow} [\varepsilon]_{\equiv_M} \overset{1:1}{\longleftrightarrow} [\varepsilon]_{\equiv_{L(M)}} \overset{1:1}{\longleftrightarrow} q_0'$$

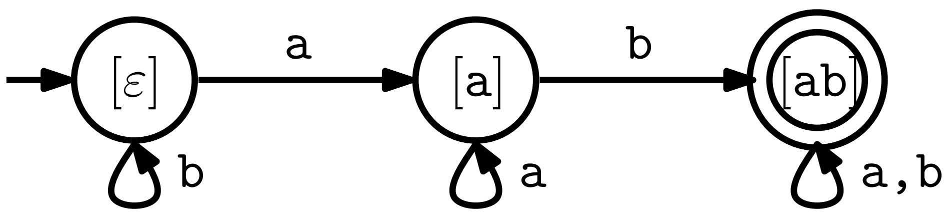
Akz. Zustände

$$q \in F \overset{1:1}{\longleftrightarrow} [z]_{\equiv_M} \subseteq L(M) \overset{1:1}{\longleftrightarrow} [z]_{\equiv_{L(M)}} \subseteq L(M) \overset{1:1}{\longleftrightarrow} [z]_{\equiv_{L(M)}} \in F'$$

$\square$

DEA Minimierung

- Myhill-Nerode Relation:
  $u \equiv_L v :\Longleftrightarrow \forall z \in \Sigma^* : uz \in L \Leftrightarrow vz \in L$
- Mit Hilfe der MN-Relation können wir einen DEA $M(\equiv_L)$ erstellen, der L erkennt



- Der DEA $M(\equiv_L)$ ist ein minimaler Automat für L
- Der kollabierte Automat eines Automaten M stimmt mit dem Automaten der MN-Relation von $L(M)$ überein (nach Umbenennung)
- Satz von Myhill-Nerode: L regulär, gdw. $\equiv_L$ hat Index $< \infty$

Nichtreguläre Sprachen

- Wo liegen die Grenzen des DEA/NEA Berechnungsmodells?
- Einschränkung: Nur endlich viele Zustände & bereits gelesene Zeichen nicht mehr direkt verfügbar
- Konsequenz: Während der Berechnung kann ich nur auf eine beschränkte Anzahl von Informationen über das bereits gelesene Präfix zurückgreifen
- Ein Problem ist deshalb das “Zählen”

Kandidat: $L = \{\mathtt{a}^n\mathtt{b}^n \mid n \geq 0\}$

Satz 9

$$L = \{\mathtt{a}^n\mathtt{b}^n \mid n \geq 0\} \notin \mathsf{REG}$$

Beweis

- Der Satz von Myhill-Nerode gibt uns die stärkste strukturelle Aussage über die regulären Sprachen. ($L \in \mathsf{REG} \quad \Leftrightarrow \quad \equiv_L$ hat endlichen Index)
- Wir müssen zeigen $\equiv_L$ bildet ∞ viele Äquivalenzklassen
- $\mathtt{a}^i \not\equiv_L \mathtt{a}^{i+k}$, für $k > 0$ (Trennwort $\mathtt{b}^i$)
- Äquivalenzklassen: $[\varepsilon], [\mathtt{a}], [\mathtt{aa}], [\mathtt{aaa}], \ldots$
  jedes $\mathtt{a}^i$ liegt in einer eigenen Klasse!
- Da also $\equiv_L$ unendlich viele Äquivalenzklassen hat, ist L nicht regulär!

$\square$