Seminararbeit

Charakterisierung regulärer Sprachen und regulärer numerischer Prädikate durch logische Formeln

ausgeführt von

Stefan Schrott

unter der Anleitung von

Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

Wien, am 11. November 2019

Inhaltsverzeichnis

1 Grundlagen und Notation

1.1 Reguläre Sprachen

Im Folgenden bezeichnen wir eine endliche Menge A als Alphabet. A^* bezeichnet das freie Monoid über A, also die Menge der endlichen Zeichenketten aus Elementen von A. Für $w \in A^*$ bezeichnen wir mit $|w|$ die Länge des Wortes. Eine Menge $L \subseteq A^*$ wird als Sprache bezeichnet.

Ein nicht-deterministischer endlicher Automat ist ein Tupel $\mathcal{M} = (Q, i, \mathcal{E}, F)$, wobei Q eine endliche Menge von Zuständen ist, $i \in Q$ der sogenannte Anfangszustand ist und $F \subseteq Q$ eine Menge von Endzuständen ist. $\mathcal{E} \subseteq Q \times A \times Q$ wird als Übergangrelation bezeichnet.

Ein $\mathcal{M}$-Pfad ist eine endliche Folge von Tupeln $(q_0, a_1, q_1), (q_1, a_2, q_2), \ldots, (q_{n-1}, a_n, q_n)$, wobei $a_1, \ldots a_n \in A$ und $q_0, \ldots, q_n \in Q$. Wir sagen, der Automat $\mathcal{M}$ akzeptiert ein Wort $w = a_1 \cdots a_n$, falls es einen $\mathcal{M}$-Pfad $(q_0, a_1, q_1), (q_1, a_2, q_2), \ldots, (q_{n-1}, a_n, q_n)$ gibt, sodass $q_0 = i$ und $q_n \in F$.

Eine Sprache L heißt regulär, falls es eine nicht-deterministischen Automaten gibt, der ein Wort $w \in A^*$ genau dann akzeptiert, wenn es in L enthalten ist.

Wir geben nun einen anderen Zugang zur Definition regulärer Sprachen an:

Die Menge der regulären Ausdrücke über einem Alphabet A ist induktiv wie folgt definiert:

1. Für $w \in A^*$ ist $\{w\}$ ein regulärer Ausdruck
2. $\emptyset$ ist ein regulärer Ausdruck
3. Für reguläre Ausdrücke E_1 und E_2 ist $E_1 \cup E_2$ ein regulärer Ausdruck
4. Für reguläre Ausdrücke E_1 und E_2 ist $E_1 E_2$ ein regulärer Ausdruck
5. Für einen regulären Ausdruck E ist auch E^* ein regulärer Ausdruck

Es gilt nun:

Satz 1.1. *Eine Sprache ist genau dann regulär, wenn sie durch einen regulären Ausdruck beschrieben werden kann.*

1.2 Prädikatenlogik und V-Strukturen

Im Folgenden sind $x, x_1, x_2, y, y_1, y_2, \ldots$ Variablen erster Ordnung und $X, X_1, X_2, \ldots, Y, Y_1, Y_2, \ldots$ Variablen zweiter Ordnung, dh Relationsvariablen. Wir werden im Folgenden nur einstellige Relationsvariablen betrachten.

Wir betrachten j-stellige numerische Prädikate R_i^j und für $a \in A$ das einstellige Prädikat Q_a. Auf die Interpretation dieser Prädikate gehen wir später ein.

In Folgenden verzichten wir auf die Verwendung von Konstanten- und Funktionssymbolen. Atomformeln erster Ordnung sind also $Q_a x$ für $a \in A$ und eine Variable x, sowie $R_i^j(x_1, \ldots, x_i)$ für ein numerisches Prädikat R_i^j und Variablen $x_1, \ldots, x_n$.

Formeln erster Ordnung sind dann induktiv definiert:

- Atomformeln sind Formeln.
- Wenn ϕ und ψ Formeln sind, dann sind auch $\phi \wedge \psi$ und $\neg\phi$ Formeln.
- Wenn x eine Variable und ϕ eine Formel ist, dann ist auch $\exists x\phi$ eine Formel.

Wir vereinbaren auch folgende Abkürzungen bzw Schreibweisen: $\phi \vee \psi$ steht für $\neg(\neg\phi \wedge \neg\psi)$, $\phi \to \psi$ steht für $\neg\phi \vee \psi$ und der Allquantor wird über den Existenzquantor definiert: $\forall x\phi$ bedeutet $\neg\exists x\neg\phi$.

Zur Definition von monadische Formeln zweiter Ordnung ergänzen wir die Menge der Atomformeln um Ausdrücke der Form $X(x)$, wobei X ein Relationsvariable und x eine Variable ist. Für das Bilden von monadischen Formeln zweiter Ordnung fügen wir folgende Regel hinzu: Sei ϕ eine Formel und X eine Relationsvariable, dann ist $\exists X\phi$ wieder eine Formel.

Kurz gesagt ist der Unterschied zwischen Formeln erster Ordnung und monadischen Formeln zweiter Ordnung also, dass man nicht nur über Elemente des Universums, sondern auch über Teilmengen quantifizieren kann.

Wir wenden uns nun der Semantik unserer Formeln zu, das heißt wir wollen klären, was heißt, dass ein Wort $w \in A^*$ eine Formel ϕ erfüllt, in Zeichen: $w \models \phi$.

Der Ausdruck $Q_a x$ soll beispielsweise bedeuten, dass der x-te Buchstabe des betrachteten Wortes ein a ist.

Wir geben nun eine genaue der Definition des Begriffes der numerischen Relation:

Definition 1.2. *Eine k-stellige numerische Relation P ordnet jedem $n \in \mathbb{N}$ eine k-stellige Relation P_n auf $\{1, \ldots, n\}$ zu.*

Beispiel 1.3. *Sei R eine k-stellige Relation auf $\mathbb{N}$. Dann induziert R eine k-stellige numerische Relation P, indem man $P_n := R \cap \{1, \ldots, n\}^k$ setzt. So kann man beispielweise aus dem üblichen $<$ auf $\mathbb{N}$ eine numerische Relation $<$ gewinnen.*

Es kommt aber nicht jede numerische Relation auf diese Weise zu Stande. Man kann zB eine einstellige numerische Relation last durch $last_n := \{n\}$ definieren. Der Ausdruck $last(x)$ ist nun genau dann wahr, wenn x die Position des letzten Buchstaben des betrachteten Wortes ist.

Im Folgenden wird uns vor allem die Bedeutung von geschlossenen Formeln interessieren und es ist intuitiv auch relativ klar, wie diese zu verstehen sind. Wir stehen aber vor dem Problem, dass wir auch Formeln mit freien Variablen eine Bedeutung geben müssen, um induktive Definition und Beweise über die Formelstruktur zu ermöglichen. Zu diesem Zweck führen wir das Hilfsmittel der V-Strukturen ein:

Definition 1.4. *Sei A ein Alphabet und V eine endliche Menge von Variablen erster Ordnung. Eine V-Struktur über A ist ein Wort*

$$(a_1, U_1) \ldots (a_n, U_n)$$

über dem Alphabet $A \times 2^V$ sodass $U_1, \ldots, U_n$ eine Partition von V ist.

Definition 1.5. *Sei A ein Alphabet, V_1 eine endliche Menge von Variablen erster Ordnung und V_2 eine endliche Menge von Variablen zweiter Ordnung. Eine (V_1, V_2)-Struktur über A ist ein Wort*

$$(a_1, S_1, T_1) \ldots (a_n, S_n, T_n)$$

über dem Alphabet $A \times 2^{V_1} \times 2^{V_2}$, sodass $S_1, \ldots, S_n$ eine Partition von V_1 ist.

Sei I eine Interpretation, das heißt eine Funktion, die jedem numerischen Prädikat R_i^j eine j-stellige numerische Relation zuordnet. Wir können nun induktiv die Interpretation der Formeln bezüglich dieser Interpretation I definieren: Sei w eine (V_1, V_2)-Struktur, dann gelte:

$$
\begin{aligned}
w \models_I Q_a x &: \iff w \text{ enthält einen Buchstaben } (a, S, T) \text{ mit } x \in S \\
w \models_I R_i^j(x_1, \ldots, x_j) &: \iff \begin{cases} I \text{ ordnet } R_i^j \text{ die } j\text{-stellige Relation } P_{|w|} \text{ auf } \{1, \ldots, |w|\} \text{ zu,} \\ x_k \text{ kommt an der Stelle } p_k \text{ in } w \text{ vor und } P_{|w|}(p_1, \ldots, p_j) \end{cases} \\
w \models_I (\phi \wedge \psi) &: \iff w \models_I \phi \text{ und } w \models_I \psi \\
w \models_I \neg\phi &: \iff w \not\models_I \phi \\
w \models_I \exists x \phi &: \iff \begin{cases} w = (a_1, S_1, T_1) \ldots (a_n, S_n, T_n) \text{ und } \exists i \in \{1, \ldots, n\} : \\ (a_1, S_1, T_1) \ldots (a_i, S_i \cup \{x\}, T_i) \ldots (a_n, S_n, T_n) \models_I \phi \end{cases} \\
w \models_I X(x) &: \iff w \text{ enthält einen Buchstaben } (a, S, T) \text{ mit } x \in S \text{ und } X \in T \\
w \models_I \exists X \phi &: \iff \begin{cases} w = (a_1, S_1, T_1), \ldots, (a_n, S_n, T_n) \text{ und } \exists J \subseteq \{1, \ldots, |w|\} \\ \text{sodass für } T_i' := T_i \cup \{X\} \text{ falls } i \in J \text{ bzw } T_i' = T_i \text{ sonst gilt:} \\ w' := (a_1, S_1, T_1'), \ldots, (a_n, S_n, T_n') \models_I \phi \end{cases}
\end{aligned}
$$

Daraus ergibt sich auch die Interpretation der anderen Booleschen Operationen und des Allquantors. Außerdem erhält man damit eine Interpretation von V-Strukturen, indem man $V_2 = \emptyset$ setzt und eine Interpretation für Wörter, indem man $V_1 = V_2 = \emptyset$ wählt.

Wir können nun – bei gegebenem Alphabet A und Interpretation I – die von einer Formel akzeptierte Sprache definieren:

Definition 1.6. *Sei ϕ eine geschlossene monadische Formel zweiter Ordnung. Dann ist die von ϕ akzeptierte Sprache definiert als*

$$L_\phi := \{w \in A^* : w \models_I \phi\}.$$

Zwei geschlossene Formeln ϕ und ψ heißen äquivalent, falls $L_\phi = L_\psi$.

2 Charakterisierung regulärer Sprachen durch SOM[+1]

Wir betrachten monadische Formeln zweiter Ordnung mit den numerischen Predikaten R_1^2 und R_2^2. Die Interpretation I interpretiere $R_1^2(x, y)$ mit $x = y$ und $R_2^2(x, y)$ mit $y = x + 1$. Der Übersicht halber werden wir in Zukunft die Prädikatsymbole in den Formeln durch $x = y$ und $y = x + 1$ ersetzen. Die auf die Weise definierte Sprache bezeichnen wir mit SOM[+1].

Das Ziel dieses Abschnittes ist der Beweis der folgenden Aussage:

Satz 2.1. *Eine Sprache $L \subseteq A^*$ ist genau dann regulär, wenn es eine Formel ϕ in SOM[+1] gibt, sodass $L = L_\phi$.*

Wir zeigen zuerst die folgende Richtung der Äquivalenz:

Lemma 2.2. *Sei $L \subseteq A^*$ regulär. Dann gibt es eine Formel ϕ in SOM[+1], sodass $L = L_\phi$.*

Beweis. Wir beginnen mit folgender Beobachtung: Sei $\mathcal{M} = (\{q_0, \ldots, q_{n-1}\}, q_o, F, \mathcal{E})$ ein nicht deterministischer Automat für das Alphabet A und $w = a_1 \ldots a_{|w|} \in A^*$ ein Wort, das von $\mathcal{M}$ akzeptiert wird. Dann gibt es einen $\mathcal{M}$-Pfad $(p_0, a_1, p_1), \ldots, (p_{|w|-1}, a_{|w|}, p_{|w|})$ mit $p_0 = q_0$ und $p_{|w|} \in F$. Dieser Pfad induziert eine Partition $X_0, \ldots X_{n-1}$ der Menge $\{1, \ldots, |w|\}$, indem man definiert:

$$X_j := \{k \in \{1, \ldots, |w|\} : p_{k-1} = q_j\}.$$

Diese Partition erfüllt folgende Eigenschaften:

(i) $1 \in X_0$ (da $p_0 = q_0$ gilt)

(ii) $j \in X_k \wedge j+1 \in X_\ell \implies (q_k, a_j, q_\ell) \in \mathcal{E}$ (das ist die $\mathcal{M}$-Pfad-Eigenschaft)

(iii) $|w| \in X_k \implies \exists q \in F : (q_k, a_{|w|}, q) \in \mathcal{E}$ (da $q_{|w|} \in F$ gilt)

Umgekehrt kann man aus einer Partition $X_0, \ldots, X_{n-1}$, die (i) bis (iii) erfüllt, einen akzeptierenden $\mathcal{M}$-Pfad für das Wort w rekonstruieren: Man setzt $p_k := q_j$, falls $k+1 \in X_j$, und $p_{|w|} := q$ für ein q, das $(q_{|w|-1}, a_{|w|}, q) \in \mathcal{E}$ erfüllt (so eines existiert wegen (iii)).

Insgesamt charakterisiert die Existenz einer solchen Partition also genau jene Wörter, die von $\mathcal{M}$ akzeptiert werden. Unser Ziel ist es nun, eine monadische Formel zweiter Ordnung zu finden, die genau dann erfüllbar ist, wenn eine derartige Partition existiert.

Die Formel

$$\phi_p : \forall x \left[\bigvee_{i=0}^{n-1} X_i(x) \wedge \bigwedge_{0 \le i < j \le n-1} (X_i(x) \wedge X_j(x)) \right]$$

stellt sicher, dass $X_0, \ldots, X_{n-1}$ eine Partition ist.

Die Bedingung (i) wird durch

$$\phi_1 : \forall x \left[(\forall y : x \neq y + 1) \to X_0(x) \right]$$

beschrieben, wobei $(\forall y : x \neq y + 1)$ codieren soll, das $x = 1$ ist. Bedingung (ii) kann durch

$$\phi_2 : \forall x \forall y \left[y = x + 1 \to \bigwedge_{0 \le i,j \le n-1} \left(X_i(x) \wedge X_j(y) \to \bigvee_{a \in S_{ij}} Q_a x \right) \right]$$

beschrieben werden, wobei $S_{ij} = \{a \in A : (q_i, a, q_j) \in \mathcal{E}\}$. Für die Bedingung (iii) verwenden wir die Formel

$$\phi_3 : \forall x \left[\forall y (y \neq x + 1) \to \bigwedge_{i=0}^{n-1} \left(X_i(x) \to \bigvee_{a \in T_i} Q_a x \right) \right],$$

wobei $T_i = \{a \in A : \exists q \in F : (q_i, a, q) \in \mathcal{E}\}$.

Für die Formel

$$\phi : \exists X_0 \ldots \exists X_{n-1} : \phi_p \wedge \phi_1 \wedge \phi_2 \wedge \phi_3$$

gilt nun $w \models \phi$ genau dann, wenn es eine Partition mit den Eigenschaften (i) bis (iii) gibt, und das ist wiederum genau dann der Fall, wenn w vom Automaten $\mathcal{M}$ akzeptiert wird. □

Für die andere Richtung der Äquivalenz zeigen wir:

Lemma 2.3. *Sei V_1 eine endliche Menge von Variablen erster Ordnung und V_2 eine endliche Menge von Variablen zweiter Ordnung. Dann gilt für jede SOM[+1]-Formel ϕ mit freien Variablen erster Ordnung in V_1 und freien Variablen zweiter Ordnung in V_2: L_ϕ ist eine reguläre Sprache.*

Beweis. Wir zeigen die Aussage per Induktion über den Formelaufbau:

- Der Automat $(2^{V_1}, \emptyset, \{V_1\}, \mathcal{E})$, wobei

  $$\mathcal{E} := \{(U_1, (a, S, T), U_2) \in 2^{V_1} \times (A \times 2^{V_1} \times 2^{V_2}) \times 2^{V_1} : U_2 = U_1 \uplus S\}$$

  erkennt, ob ein $w \in (A \times 2^{V_1} \times 2^{V_2})^*$ eine (V_1, V_2)-Struktur ist. Daher ist die Menge der (V_1, V_2)-Strukturen eine reguläre Sprache (als Teilmenge von $A \times 2^{V_1} \times 2^{V_2}$). Wir bezeichnen diese Menge im Folgenden mit $\mathcal{L}$.

- Der Automat $(\{q_0, q_1\}, q_0, \{q_1\}, \mathcal{E})$, wobei

  $$\mathcal{E} := \{(q_u, (b, S, T), q_u) : b \in A, S \in 2^{V_1}, T \in 2^{V_2}\} \cup \{(q_0, (a, S, T), q_1) : x \in S \in 2^{V_1}, T \in 2^{V_2}\}$$

  überprüft, ob ein $w \in (A \times 2^{V_1} \times 2^{V_2})^*$ einen Buchstaben (a, S, T) mit $x \in S$ enthält. Das zeigt, dass die Sprache

  $$\mathcal{L} \cap \{w \in (A \times 2^{V_1} \times 2^{V_2})^* : w \text{ enthält einen Buchstaben } (a, S, T) \text{ mit } x \in S\}$$

  regulär ist. Dies ist aber genau die Menge der (V_1, V_2)-Strukturen, die $Q_a x$ erfüllen.

- Seien $x, y \in V_1$ beliebig. Der Automat $(2^{V_1}, \emptyset, \{V_1\}, \mathcal{E})$, wobei

  $$\mathcal{E} := \{(U_1, (a, S, T), U_2) \in 2^{V_1} \times (A \times 2^{V_1} \times 2^{V_2}) \times 2^{V_1} : U_2 = U_1 \uplus S, x \in S \iff y \in S\}$$

  erkennt die Menge der (V_1, V_2)-Strukturen, die $x = y$ erfüllen.

- Für $x, y \in V_1$ betrachten wir den Automaten $\mathcal{M} = (\{q_0, q_1, q_2\}, q_0, \{q_2\}, \mathcal{E})$, wobei

  $$\begin{aligned}\mathcal{E} = &\{(q_i, (a, S, T), q_i) : i \in \{0, 2\}, a \in A, S \in 2^{V_1 \setminus \{x,y\}}, T \in 2^{V_2}\} \\ &\cup \{(q_0, (a, S \cup \{x\}, T), q_1) : a \in A, S \in 2^{V_1 \setminus \{x,y\}}, T \in 2^{V_2}\} \\ &\cup \{(q_1, (a, S \cup \{y\}, T), q_2) : a \in A, S \in 2^{V_1 \setminus \{x,y\}}, T \in 2^{V_2}\}.\end{aligned}$$

  Man sieht leicht, dass $L(\mathcal{M}) \cap \mathcal{L}$ genau die Menge der (V_1, V_2)-Strukturen ist, die $y = x + 1$ erfüllen.

- Für $x \in V_1$ und $X \in V_2$ betrachten wir den Automaten $\mathcal{M} = (\{q_0, q_1\}, q_0, \{q_1\}, \mathcal{E})$, wobei

  $$\begin{aligned}\mathcal{E} = &\{(q_i, (a, S, T), q_i) : i \in \{0, 1\}, a \in A, S \in 2^{V_1}, T \in 2^{V_2}\} \\ &\cup \{(q_0, (a, S \cup \{x\}, T \cup \{X\}), q_1) : a \in A, S \in 2^{V_1}, T \in 2^{V_2}\}.\end{aligned}$$

  Man sieht leicht, dass $L(\mathcal{M}) \cap \mathcal{L}$ genau die Menge der (V_1, V_2)-Strukturen ist, die $X(x)$ erfüllen.

  Somit ist Aussage für alle Atomformeln gezeigt.

- Die Booleschen Operationen sind ebenfalls leicht, weil $L_{\phi\wedge\psi} = L_\phi \cap L_\psi$ bzw $L_{\neg\phi} = \mathcal{L} \cap L_\phi^c$ gilt und die Klasse der regulären Sprachen bzgl Durchschnitt und Komplement abgeschlossen ist.

- Wir nehmen nun an, dass ϕ die Form $\exists x\psi$ hat und dass die Aussage für ψ schon gezeigt ist. Dann gilt insbesondere: Die Menge der $(V_1 \cup \{x\}, V_2)$-Strukturen, die ψ erfüllen, ist regulär und wird daher von einem Automaten $\mathcal{M} = (Q, q_0, F, \mathcal{E})$ entschieden. Wir definieren nun einen neuen Automaten $\mathcal{M}' = (Q \times \{0,1\}, (q_0, 0), F \times \{1\}, \mathcal{E}')$, wobei

$$\begin{aligned}\mathcal{E}' := \{((q,u),(a,S,T),(q',u)) : u \in \{0,1\}, x \notin S, (q,(a,S,T),q') \in \mathcal{E}\} \\ \cup\{((q,0),(a,S\setminus\{x\},T),(q',1)) : x \in S, (q,(a,S,T),q') \in \mathcal{E}\ \}.\end{aligned}$$

  Man sieht leicht, dass $\mathcal{M}'$ eine (V_1, V_2)-Struktur w genau dann akzeptiert, wenn es ein $i \in \{1, \ldots, |w|\}$ gibt, sodass man S_i durch $S_i \cup \{x\}$ ersetzen kann und w dann von $\mathcal{M}$ erfüllt wird; also leistet $\mathcal{M}'$ das gewünschte.

- Wir nehmen an, dass ϕ von der Gestalt $\exists X\psi$ ist und dass nach Induktionsvorraussetzung die Menge der $(V_1, V_2 \cup \{X\})$-Strukturen, die ψ erfüllen, regulär ist, also von einem Automaten $\mathcal{M} = (Q, q_0, F, \mathcal{E})$ entschieden wird. Wir betrachten den Automaten $\mathcal{M}' := (Q, q_0, F, \mathcal{E}')$, wobei

$$\mathcal{E}' := \{(q,(a,S,T\setminus\{X\}),q') : (q,(a,S,T),q') \in \mathcal{E}\}.$$

  Man sieht leicht, dass ein w von $\mathcal{M}'$ akzeptiert wird, genau dann wenn $w \models \exists X\psi$.

□

Beweis von Satz 2.1. Die eine Richtung der Äquivalenz ist Lemma 2.2 und die andere Richtung folgt aus Lemma 2.3, wenn man $V_1 = V_2 = \emptyset$ setzt. □

Ein Existenzsatz ist eine geschlossene Formel, die aus einen Block von Existenzquantoren zweiter Ordnung gefolgt von einer Formel erster Ordnung besteht.

Korollar 2.4. *Jeder Satz in SOM[+1] ist äquivalent zu einem Existenzsatz.*

Beweis. Sei ϕ ein Satz in SOM[+1], dann ist L_ϕ nach Satz 2.1 regulär. Lemma 2.2 liefert nun einen Existenzsatz ψ, sodass $L_\phi = L_\psi$. □

3 Reguläre numerische Prädikate

Wir betrachten nun den Spezialfall, dass das Alphabet A einelementig ist, also $A = \{a\}$. In diesem Fall kann eine Sprache $L \subseteq A^*$ vermittels der Abbildung $w \mapsto |w|$ als eine Teilmenge von $\mathbb{N}$ betrachtet werden.

Wir erinnern daran, dass eine k-stellige numerische Relation P jedem $n \in \mathbb{N}$ eine k-stellige Relation P_n auf $\{1, \ldots, n\}$ zuordnet, und führen nun den Begriff der regulären numerischen Relation ein:

Definition 3.1. *Sei ϕ eine SOM[+1]-Formel mit freien Variablen erster Ordnung $x_1, \ldots, x_k$ und ohne freien Variablen zweiter Ordnung bezüglich dem Alphabet $\{a\}$. Dann definiert ϕ eine numerische Relation P durch*

$$(j_1, \ldots, j_k) \in P_n :\iff w \models \phi,$$

wobei $w = (a, S_1) \cdots (a, S_n)$ jene $\{x_1, \ldots, x_k\}$-Struktur ist, die $x_i \in S_{j_i}$ für $i = 1, \ldots, k$ erfüllt.

Eine numerische Relation, die auf diese Weise durch eine SOM[+1]-Formel definiert werden kann, wird regulär genannt.

Das Ziel dieses Abschnittes ist der Beweis der folgenden Aussage:

Satz 3.2. *Eine numerische Relation ist genau dann regulär, wenn sie durch eine Formel erster Ordnung definierbar ist, in der alle Atomformeln die Form $x < y$ oder $x \equiv_m 0$ haben.*

Dabei ist $x \equiv_m y$ eine Kurzschreibweise für $x \equiv y \mod m$. Eine Richtung dieser Äquivalenz ist mit unseren bisherigen Resultaten sehr einfach zu beweisen:

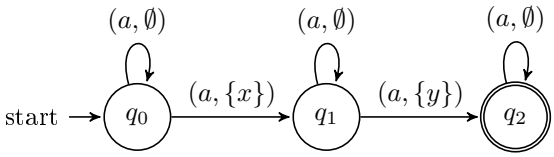
Lemma 3.3. *Sei eine numerische Relation P durch eine Formel erster Ordnung, in der alle Atomformeln die Form $x < y$ oder $x \equiv_m 0$ haben, definierbar. Dann ist P regulär.*

Beweis. Da jede Formel erster Ordnung insbesondere eine monadische Formel zweiter Ordnung ist, reicht es aus zu zeigen, dass die Atomformeln $x < y$ und $x \equiv 0 \mod m$ in SOM[+1] definierbar sind. Nach Satz 2.1 reicht es also zu zeigen

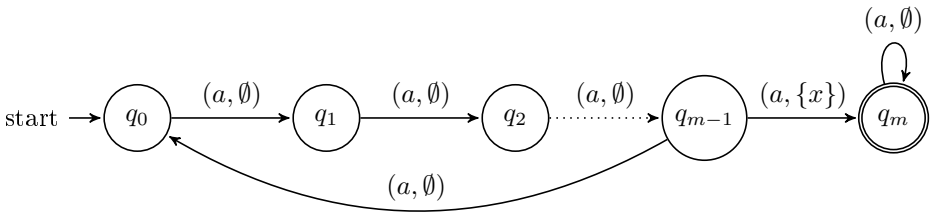
(i) dass die Menge aller $\{x, y\}$-Strukturen, die $x < y$ erfüllen, eine reguläre Sprache über dem Alphabet $\{a\} \times 2^{\{x,y\}}$ ist;

(ii) und dass die Menge aller $\{x\}$-Strukturen, die $x \equiv_m 0$ erfüllen, eine reguläre Sprache über dem Alphabet $\{a\} \times 2^{\{x\}}$ ist.

Für (i) geben wir den folgenden Automaten an:



und bei gegebenem m gibt es auch einen Automaten, der (ii) zeigt:



□

Für den Beweis der anderen Richtung der Äquivalenz beweisen wir zuerst eine Charakterisierung der regulären Sprachen über dem Alphabet $\{a\}$:

Proposition 3.4. *Eine Sprache $L \subseteq \{a\}^*$ ist genau dann regulär, wenn es ein $n \in \mathbb{N}$ sowie $r_1, \dots r_n$ und $s_1, \dots, s_n \in \mathbb{N}$ gibt, sodass*

$$L = \bigcup_{i=1}^{n} a^{r_i}(a^{s_i})^* \tag{1}$$

Für den Beweis benötigen wir:

Lemma 3.5 (Lemma von Bézout)**.** *Seien $p, q \in \mathbb{N} \setminus \{0\}$ relativ prim. Dann existieren $s, t \in \mathbb{Z}$, sodass $sp + tq = 1$.*

Für $A, B \subseteq \mathbb{N}$ sei $A + B := \{a + b : a \in A, b \in B\}$ und in Anlehnung an den Kleene-Stern sei

$$A^* := \bigcup_{n \in \mathbb{N}} \underbrace{A + A + \cdots + A}_{n\text{-mal}}.$$

Mit der Kommutativität der Addition sieht man leicht, dass gilt $(A + B)^* = A^* + B^*$.

Proposition 3.6. *Seien $a, b \in \mathbb{N}$ und $p, q \in \mathbb{N} \setminus \{0\}$ und seien die arithmetischen Progressionen $A := \{a + kp : k \in \mathbb{N}\}$ und $B := \{b + \ell q : \ell \in \mathbb{N}\}$. Dann gibt es ein $c \in \mathbb{N}$ und eine endliche Menge $E \subseteq \mathbb{N}$, sodass für $C := \{c + m \cdot \mathrm{ggT}(p, q) : m \in \mathbb{N}\}$ gilt:*

$$A + B = C \cup E.$$

Beweis. Wir zeigen zuerst: Für p, q relativ prim gibt es ein $N(p, q) \in \mathbb{N}$, sodass:

$$\forall n \geq N(p, q) : \exists k, \ell \in \mathbb{N} : n = kp + \ell q \tag{2}$$

Seien dafür $k_0, \ell_0 \in \mathbb{N}$ sowie $0 \leq d_1 \leq p - 1$ und $0 \leq d_2 \leq q - 1$ sodass

$$\left\lfloor \frac{n}{2} \right\rfloor = k_0 p + d_1 \qquad \text{und} \qquad \left\lceil \frac{n}{2} \right\rceil = \ell_0 q + d_2, \tag{3}$$

und $s, t \in \mathbb{Z}$, sodass $sp + tq = 1$. Dann gilt für $d := d_1 + d_2 \in \{0, \dots, p + q - 2\}$:

$$n = \left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = k_0 p + \ell_0 q + d = k_0 p + \ell_0 q + d(sp + tq) = (k_0 + ds)p + (\ell_0 + dt)q.$$

Wir müssen nun sicherstellen, dass $k_0 + ds, \ell_0 + dt \geq 0$ für hinreichend große n gilt.

Man sieht leicht, dass es ein $N \in \mathbb{N}$ gibt, sodass für $n \geq N$ die Zahlen k_0 und ℓ_0 gewählt wie in (3) immer die Ungleichungen $k_0 \geq (p - q - 2)|s|$ und $\ell_0 \geq (p - q - 2)|t|$ gelten. Daraus folgt sofort $k_0 \geq d|s|$ und $\ell_0 \geq d|t|$ und weiter $k_0 + ds, \ell_0 + dt \geq 0$.

Wir wenden uns nun dem Beweis der eigentlichen Aussage zu; seien also $A := \{a + kp : k \in \mathbb{N}\}$ und $B := \{b + \ell q : \ell \in \mathbb{N}\}$ zwei gegebene arithmetische Progressionen. Wir schreiben $p' = p/\mathrm{ggT}(p, q)$

und $q' = q/\mathrm{ggT}(p,q)$ und definieren $c := a + b + N(p',q')\mathrm{ggT}(p,q)$, wobei $N(p',q')$ (2) erfüllt, und definieren weiters $C := \{c + m \cdot \mathrm{ggT}(p,q) : m \in \mathbb{N}\}$.

Wir wollen nun $C \subseteq A + B$ zeigen, sei also $n = c + m \cdot \mathrm{ggT}(p,q)$. Wegen (2) gibt es $k, \ell \in \mathbb{N}$ sodass $N(p',q') + m = kp' + \ell q'$. Es gilt dann

$$\begin{aligned} n &= c + m \cdot \mathrm{ggT}(p,q) = a + b + (N(p',q') + m)\mathrm{ggT}(p,q) = a + b + (kp' + \ell q')\mathrm{ggT}(p,q) \\ &= a + kp + b + \ell q \in A + B. \end{aligned}$$

Wir definieren nun $E := (A + B) \setminus C$. Die Gleichheit $A + B = C \cup E$ ist nun offensichtlich; es verbleibt zu zeigen, dass E tatsächlich endlich ist. Sei $n \in A + B$ dann

$$n = a + kp + bq = a + b + kp'\mathrm{ggT}(p,q) + \ell q'\mathrm{ggT}(p,q) = c + (kp' + \ell q' - N(p',q'))\mathrm{ggT}(p,q),$$

also ist $n \in C$, falls $kp' + \ell q' - N(p',q') \geq 0$, was für alle bis auf endlich viele $k, \ell \in \mathbb{N}$ der Fall ist. □

Korollar 3.7. *Sei A eine arithmetische Progression. Dann gibt es eine arithmetische Progression B und eine endliche Menge E sodass*

$$A^* = B \cup E.$$

Beweis. Sei $A = \{a + kp : k \in \mathbb{N}\}$, so gilt

$$\underbrace{A + A + \cdots + A}_{n\text{-mal}} = \left\{ na + \sum_{i=1}^{n} k_i p : k_i \in \mathbb{N} \right\} = \{na + kp : k \in \mathbb{N}\}$$

und daher ist

$$A^* = \{na + kp : n, k \in \mathbb{N}\} = \{na : n \in \mathbb{N}\} + \{kp : k \in \mathbb{N}\},$$

also Summe zweier arithmetischer Progressionen. Damit liefert Proposition 3.6 das gewünschte Resultat. □

Wir übersetzen diese zahlentheoretischen Resultate nun in Resultate über reguläre Ausdrücke über dem einelementigen Alphabet. Dies ist sehr einfach möglich, da die Abbildung

$$\phi : a^* \to \mathbb{N} : w \mapsto |w|$$

ein Monoidisomorphismus vom freien Monoid über der einelementigen Menge in das additive Monoid $\mathbb{N}$ ist. Es gilt also für $L_1, L_2 \subseteq \{a\}^*$:

$$\phi(L_1 L_2) = \phi(L_1) + \phi(L_2) \text{ und } \phi(L_1 \cup L_2) = \phi(L_1) \cup \phi(L_2).$$

Daraus folgt auch, dass ϕ mit dem $*$ verträglich ist:

$$\phi(L^*) = \phi\left(\bigcup_{n\in\mathbb{N}} \underbrace{L \cdots L}_{n\text{-mal}} \right) = \bigcup_{n\in\mathbb{N}} \phi\left(\underbrace{L \cdots L}_{n\text{-mal}} \right) = \bigcup_{n\in\mathbb{N}} \underbrace{\phi(L) + \cdots + \phi(L)}_{n\text{-mal}} = \phi(L)^*.$$

Lemma 3.8. *(a) Seien $r_1, r_2, s_1, s_2 \in \mathbb{N}$ gegeben. Dann gibt es $r, s, t_1, \ldots, t_n$ sodass:*

$$a^{r_1}(a^{s_1})^* a^{r_2}(a^{s_2})^* = a^r(a^s)^* \cup \bigcup_{i=1}^{n} a^{t_i}$$

(b) Seien $r, s \in \mathbb{N}$ gegeben. Dann gibt es $p, q, t_1, \ldots, t_n$ sodass:

$$(a^r(a^s)^*)^* = a^p(a^q)^* \cup \bigcup_{i=1}^{n} a^{t_i}$$

Beweis. Offensichtlich sind Ausdrücke der Form $\phi(a^r(a^s)^*)$ arithmetische Progressionen. Die Aussage (a) folgt also aus Proposition 3.6 und die Aussage (b) aus Korollar 3.7. □

Wir geben nun einige einfach Rechenregeln für Sprachen über dem einelementigen Alphabet an:

Lemma 3.9. *Seien $L_1, \ldots L_n, M_1, \ldots, M_m \subseteq \{a\}^*$. Dann gilt:*

(a) $\left(\bigcup_{i=1}^n L_i\right)\left(\bigcup_{j=1}^m M_i\right) = \bigcup_{i=1}^n \bigcup_{j=1}^m L_i M_j$

(b) $\left(\bigcup_{i=1}^n L_i\right)^* = L_1^* \cdots L_n^*$

Beweis. Den Punkt (a) beweist man durch einfaches Nachrechnen. Für (b) bemerken wir zuerst, dass für $A, B \subseteq \mathbb{N}$ gilt

$$\begin{aligned}(A \cup B)^* &= \left\{\sum_{i=1}^{n} c_i : n \in \mathbb{N}, c_1, \ldots, c_n \in A \cup B\right\} \\ &= \left\{\sum_{i=1}^{n} a_i + \sum_{i=1}^{m} b_i : n, m \in \mathbb{N}, a_1, \ldots, a_n \in A, b_1, \ldots, b_m \in B\right\} \\ &= \left\{\sum_{i=1}^{n} a_i : n \in \mathbb{N}, a_1, \ldots, a_n \in A\right\} + \left\{\sum_{i=1}^{m} b_i : b_1 \ldots, b_m \in B\right\} = A^* + B^*.\end{aligned}$$

Daraus folgt $(L_1 \cup L_2)^* = L_1^* L_2^*$. Die Aussage für allgemeines n kann man daraus nun per Induktion folgern. □

Der Beweis von Proposition 3.4 ist nur mehr ein Zusammentragen der bisherigen Resultate:

Beweis von Proposition 3.4. Nach Satz 1.1 beschreibt jeder reguläre Ausdruck eine reguläre Sprache, daher ist die Sprache L definiert wie in (1) regulär. Umgekehrt reicht es wegen Satz 1.1 zu zeigen:

Für jeden regulären Ausdruck E gibt es einen regulären Ausdruck E', sodass E' in der Form

$$\bigcup_{i=1}^{n} a^{r_i}(a^{s_i})^* \tag{4}$$

ist und sodass E und E' dieselbe Sprache beschreiben. Wir führen den Beweis per Induktion über die Struktur regulärer Ausdrücke:

Für die regulären Ausdrücke $\emptyset$ und $\{a^k\}$ ist die Aussage trivial. Wenn E_1 und E_2 die Gestalt (4) haben, so hat offensichtlich auch $E_1 \cup E_2$ diese Gestalt.

Seien nun E_1 und E_2 von der Gestalt (4). Wegen Lemma 3.9(a) können wir oBdA annehmen, dass $E_1 = a^{r_1}(a^{s_1})^*$ und $E_2 = a^{r_2}(a^{s_2})^*$. Lemma 3.8(a) liefert nun einen zu E_1E_2 äquivalenten regulären Ausdruck in der Form (4).

Seien nun E von der Gestalt (4). Wegen Lemma 3.9(b) und da wir die Aussage für die Konkatenation schon gezeigt haben, können wir oBdA annehmen, dass $E = a^r(a^s)^*$. Lemma 3.8(b) liefert nun einen zu E^* äquivalenten regulären Ausdruck in der gewünschten Form. □

Wir wenden uns nun wieder dem Beweis der zweiten Richtung der Äquivalenz in Satz 3.2 zu. Dafür benötigen wir noch folgende Hilfsaussage:

Lemma 3.10. *Seien $s, m \in \mathbb{N}$ fest. Dann gibt es eine Formel erster Ordnung, die nur die Atome $x < y$ und $x \equiv_m y$ verwendet und die Relation $x \equiv_m y + s$ definiert.*

Beweis. Um schleppende Formulierungen zu vermeiden, bezeichnen wir im Folgenden Formeln erster Ordnung mit Atomen vom Typ $x < y$ und $x \equiv_m 0$ als zulässige Formeln.

Wir überlegen uns nun wie man gewisse Relationen als zulässige Formel darstellen kann und wenn wir eine solche Darstellung gefunden haben, werden wir den jeweiligen Ausdruck auch als Abkürzung für diese Formel betrachten, das heißt:

Die Relation $x = y$ kann man durch die zulässige Formel

$$\neg(x < y) \wedge \neg(y < x)$$

beschrieben und in Folgenden werden wir $x = y$ als Kurzschreibweise für diese Formel in anderen Formeln verwenden.

Eine zulässige Formel für $x = y + 1$ ist gegeben durch

$$x > y \wedge \forall z(z > y \to \neg(z < x))$$

Daraus kann man für $s \in \mathbb{N}$ fix auch eine zulässige Formel für $x = y + s$ angeben

$$\exists y_1 \cdots \exists y_{\ell-1}(y_1 = y + 1) \wedge \bigwedge_{i=1}^{\ell-2}(y_{i+1} = y_i + 1) \wedge (x = y_{\ell-1} + 1).$$

Man beachte, dass der Ausdruck $x = y + s$ als zweistellige Relation zu betrachten ist und $s \in \mathbb{N}$ ein fester Parameter ist. Wir haben *keine* Formel für die 3-stellige Relation $x = y + z$ gefunden.

Für $x \in \mathbb{N}$ und $0 < p \leq m$ ist

$$(x = p) \vee \exists z((z \equiv_m 0) \wedge (x = z + m))$$

eine zulässige Formel für $x \equiv_m p$. Eine zulässige Formel für $x \equiv_m y$ für x, y beliebig ist nun gegeben durch

$$\bigvee_{p=1}^{m}(x \equiv_m p) \wedge (y \equiv_m p)$$

Nun ist $x \equiv_m y + s$ lediglich eine Kurzschreibweise für $\exists z((x \equiv_m z) \wedge (z = x + s))$. □

Lemma 3.11. *Sei $S_1, \ldots, S_\ell$ eine Partition von $\{x_1, \ldots, x_k\}$, sodass $S_i \neq \emptyset$ für alle $in\{1, \ldots, \ell\}$ und seien $L_0, \ldots, L_\ell \subseteq \{a\}^*$ regulär. Dann existiert eine Formel erster Ordnung mit den Atomen $x < y$ und $x \equiv_m 0$, die die Sprache*

$$L = L_0(a, S_1)L_1(a, S_2) \cdots (a, S_\ell)L_\ell$$

definiert.

Beweis. Für $i \in \{0, \ldots, \ell\}$ gibt es nach Proposition 3.4 $r_0^i, \ldots, r_{n_i}^i, s_0^i, \ldots, s_{n_i}^i \in \mathbb{N}$, sodass

$$L_i = \bigcup_{j=1}^{n_i} a^{r_j^i} \left(a^{s_j^i}\right)^*.$$

Es ist also:

$$\begin{aligned} L &= \left(\bigcup_{j_0=1}^{n_0} a^{r_{j_0}^0} \left(a^{s_{j_0}^0}\right)^*\right)(a, S_1)\left(\bigcup_{j_1=1}^{n_1} a^{r_{j_1}^1} \left(a^{s_{j_1}^1}\right)^*\right)(a, S_2) \cdots (a, S_\ell)\left(\bigcup_{j_\ell=1}^{n_\ell} a^{r_{j_\ell}^\ell} \left(a^{s_{j_\ell}^\ell}\right)^*\right) \\ &= \bigcup_{j_0=1}^{n_0}\bigcup_{j_1=1}^{n_1} \cdots \bigcup_{j_\ell=1}^{n_\ell} \underbrace{a^{r_{j_0}^0} \left(a^{s_{j_0}^0}\right)^* (a, S_1) a^{r_{j_1}^1} \left(a^{s_{j_1}^1}\right)^* (a, S_2) \cdots (a, S_\ell) a^{r_{j_\ell}^\ell} \left(a^{s_{j_\ell}^\ell}\right)^*}_{:= L_{j_0 \cdots j_\ell}} \end{aligned}$$

Es genügt also eine Formel anzugeben, die Sprachen vom Typ

$$a^{r_0}(a^{s_0})^*(a, S_1)a^{r_1}(a^{s_1})^*(a, S_2) \cdots (a, S_\ell)a^{r_\ell}(a^{s_\ell})^*, \tag{5}$$

definiert. Eine Formel für L bekommt man dann als Disjunktion von derartigen Formeln.

Nach Lemma 3.10 kann die Relation $x \equiv_m y + s$ durch Formeln erster Ordnung mit Atomen $x < y$ und $x \equiv_m 0$ ausgedrückt werden. Man überlegt sich nun leicht, dass die Formel

$$\bigwedge_{x \in S_1} (x \equiv_{s_0} 0 + r_0) \wedge \bigwedge_{i=1}^{\ell-1} \bigwedge_{x \in S_{i+1}} \bigwedge_{y \in S_i} (x \equiv_{s_i} y + r_i) \wedge \bigwedge_{y \in S_\ell} \forall x((\forall y \neg(x < y)) \rightarrow (x \equiv_{s_\ell} y_\ell + (r_\ell + s_\ell - 1)))$$

die Sprache aus (5) erkennt. □

Proposition 3.12. *Sei P ein reguläres numerisches Prädikat. Dann gibt es eine Formel ϕ erster Ordnung mit Atomen $x < y$ und $x \equiv 0 \mod m$, die P beschreibt.*

Beweis. Sei P ein k-stelliges reguläres numerisches Prädikat. Dann gibt es eine SOM[+1]-Formel ϕ in den freien Variablen $x_1, \ldots, x_k$, sodass $(j_1, \ldots, j_k) \in P_n :\iff w \models \phi$, wobei $w = (a, S_1) \cdots (a, S_n)$ jene $\{x_1, \ldots, x_k\}$-Struktur ist, die $x_i \in S_{j_i}$ für $i = 1, \ldots, k$ erfüllt. Wir bezeichnen mit L_ϕ die reguläre Sprache der $\{x_1, \ldots, x_k\}$-Strukturen über $\{a\}$ mit $w \models \phi$.

Sei $w = (a, S_1) \ldots (a, S_n) \in L_\phi$. Dann gibt es ein $\ell \leq k$ und Indizes $i_1 < \cdots < i_\ell$, sodass $V = \biguplus_{j=1}^{\ell} S_{i_j}$ und $S_{i_j} \neq \emptyset$. Die Familie $(S_{i_1}, \ldots, S_{i_\ell})$ nennen wir auch Ordnungstyp von w, denn es gilt:

$$w \models (x_p < x_q) \iff (x_p \in S_{i_p} \wedge x_q \in S_{i_q} \implies i_p < i_q).$$

Wenn wir a als Kurzschreibweise für $(a, \emptyset)$ verwenden, können wir nun schreiben:

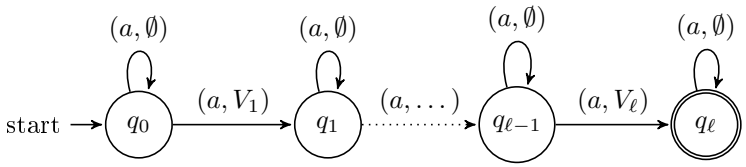
$$w = a^{m_0}(a, S_{i_1})a^{m_1} \dots a^{m_{\ell-1}}(a, S_{i_\ell})a^{m_\ell}$$

mit passenden $m_0, \dots, m_\ell \in \mathbb{N}$. Umgekehrt ist für eine gegebene Partition $\tau = (V_1, \dots, V_\ell)$ von $\{x_1, \dots, x_k\}$ die Menge der $\{x_1, \dots, x_k\}$-Strukturen vom Ordnungstyp τ gegeben durch

$$L_\tau = \{a^{m_0}(a, V_1)a^{m_1} \cdots a^{m_{\ell-1}}(a, V_\ell)a^{m_\ell} : m_0, \dots, m_\ell \in \mathbb{N}\}.$$

Wir bezeichnen mit T_k die Menge der Ordnungstypen für $\{x_1, \dots, x_k\}$-Strukturen; offenbar ist T_k endlich.

Man kann sehr leicht einen Automaten $\mathcal{M}_\tau$ angeben, der L_τ entscheidet:



Daher ist $L_\phi \cap L_\tau$ wieder eine reguläre Sprache und wird daher von einem Automaten $\mathcal{M} = (Q, i, F, \mathcal{E})$ entschieden.

Eine Folge $\alpha = (p_0, q_0, p_1, q_1, \dots, p_\ell, q_\ell)$ mit $p_0, \dots, p_\ell, q_0, \dots, q_\ell \in Q$ heißt Spur der $\{x_1, \dots, x_k\}$-Struktur $w = a^{m_0}(a, S_{i_1})a^{m_1} \cdots a^{m_{\ell-1}}(a, S_{i_\ell})a^{m_\ell}$, falls gilt: Es gibt einen akzeptierenden $\mathcal{M}$-Pfad für w sodass gilt:

- Für alle $i = 0, \dots, \ell$: Der Abschnitt des $\mathcal{M}$-Pfades, der das Teilwort a^{m_i} beschreibt, beginnt in p_i und endet in q_i.
- Für alle $i = 1, \dots, \ell$: $(q_{i-1}, (a, S_i), p_i) \in \mathcal{E}$.

Wir bezeichnen mit T_ϕ^τ die Menge aller Spuren von Wörtern in $L_\phi \cap L_\tau$. Offensichtlich hat T_ϕ^τ maximal $|Q|^{2\ell}$ Elemente, ist also insbesondere endlich.

Für zwei Zustände $p, q \in Q$ sei L_{pq} die Menge Wörter, die durch $\mathcal{M}$-Pfade von p nach q beschrieben werden. Der Automat $\mathcal{M}_{pq} := (Q, p, \{q\}, \mathcal{E})$ zeigt, dass L_{pq} wieder eine reguläre Sprache ist. Die Menge der $\{x_1, \dots, x_k\}$-Strukturen in L_ϕ, die Ordnungstyp τ und Spur α haben, ist also gegeben durch:

$$L_\phi^\tau = L_{p_0,q_0}(a, V_1)L_{p_1,q_1} \cdots L_{p_{\ell-1},q_{\ell-1}}(a, V_\ell)L_{p_\ell,q_\ell}$$

Nach Lemma 3.11 gibt es nun eine Formel erster Ordnung $\psi_{\tau\alpha}$ mit Atomen der Form $x < y$ und $x \equiv_m 0$, die L_ϕ^τ beschreibt, das heißt: $L_\phi^\tau = L_{\psi_{\tau\alpha}}$.

Wegen

$$L_\phi = \bigcup_{\tau \in T_k} L_\phi \cap L_\tau = \bigcup_{\tau \in T_k} \bigcup_{\alpha \in T_\phi^\tau} L_\phi^\tau$$

erfüllt die Formel

$$\psi : \bigvee_{\tau \in T_k} \bigvee_{\alpha \in T_\phi^\tau} \psi_{\tau\alpha}$$

die gewünschte Eingenschaft $L_\phi = L_\psi$. □

4 Charakterisierung ω-regulärer Sprachen

Wir bezeichnen mit A^ω die Menge der unendlichen Zeichenketten von Elementen aus A.

Die Definition eines Büchi-Automaten $\mathcal{M}$ unterscheidet sich von der Definition eines nicht-deterministischer Automaten lediglich im Akzeptanzverhalten: Ein Wort $w \in A^\omega$ wird genau dann akzeptiert, wenn es einen unendlich langen $\mathcal{M}$-Pfad gibt, der im Anfangszustand beginnt und unendlich oft einen Endzustand besucht. Wir bezeichnen die Menge der von $\mathcal{M}$ akzeptierten Wörter als $L_\omega(\mathcal{M})$.

Eine Sprache $L \subseteq A^\omega$ heißt ω-regulär, falls es einen Büchi-Automaten gibt, sodass $L_\omega(\mathcal{M}) = L$.

Bemerkung 4.1. *Für Sprachen $L \subseteq A^*$ kann man die Klasse der regulären Sprachen sowohl über deterministische als auch über nicht-deterministische Automaten definieren. Im Falle von ω-Wörtern ist die nicht mehr Fall: Es gibt ω-reguläre Sprachen, die nicht von einem deterministischen Automaten (mit dem oben beschrieben Akzeptanzverhalten) entschieden werden können.*

Man kann sich leicht überlegen, wie man die Definition von $w \models \phi$ auf ω-Wörter ausdehnt. Es gilt dann ebenfalls der folgende Satz:

Satz 4.2. *Eine Sprache $L \subseteq A^\omega$ ist genau dann ω-regulär, wenn es eine Formel ϕ in SOM[+1] gibt, sodass $L = L_\phi$.*

Beweisskizze. Man kann sich überlegen, dass im Beweis von Satz 2.1 die Endlichkeit der Wörter nur an einer Stelle entscheidend eingegangen ist: Wir haben verwendet, dass der Durchschnitt zweier regulärer Sprachen regulär ist. Der restliche Beweis lässt sich eins zu eins auf ω-Wörter übertragen. □

Der Beweis der ω-Regularität von $L_1 \cup L_2$ verläuft exakt wie im Falle regulärer Sprachen: Man konstruiert aus Automaten $\mathcal{M}_i$, die L_i entscheiden, leicht einen Automaten $\mathcal{M}$, der ein Wort w genau dann akzeptiert, wenn es von einem $\mathcal{M}_i$ akzeptiert wurde.

Hat man die Abgeschlossenheit der ω-regulären Sprachen unter Komplementbildung gezeigt, folgt wegen $L_1 \cap L_2 = (L_1^c \cup L_2^c)^c$ sofort die Abgeschlossenheit unter Durchschnitten. Der entscheide Schritt ist also zu Abgeschlossenheit unter Komplementen zu zeigen. Wir werden das im Folgenden grob skizzieren:

Proposition 4.3. *Sei L eine ω-reguläre Sprache, dann ist $A^\omega \setminus L$ auch ω-regulär.*

Beweisskizze. Man zeigt zuerst, dass gilt: $L \subseteq A^\omega$ ist genau dann ω-regulär, wenn es $J_1, \ldots, J_n \subseteq A^*$ und $K_1, \ldots, K_n \subseteq A^+$ gibt sodass

$$L = \bigcup_{i=1}^{n} J_i K_i^\omega \tag{6}$$

Sei nun $\mathcal{M} = (Q, i, F, \mathcal{E})$ ein Automat. Man kann nun eine Äquivalenzrelation $\equiv_\mathcal{M}$ auf A^+ folgendermaßen definieren: $w \equiv_\mathcal{M} w'$, falls für alle $p, q \in Q$ gilt:

w beschriftet einen $\mathcal{M}$-Pfad von p nach q genau dann wenn w' einen solchen beschriftet und w beschriftet einen $\mathcal{M}$-Pfad von p nach q, der in einem Endzustand vorbeikommt, genau dann wenn w' einen derartigen Pfad beschriftet.

Da die $\equiv_{\mathcal{M}}$-Klassen durch Tupel $(p,q) \in Q^2$ eindeutig bestimmt sind, gibt es nur endliche viele $\mathcal{M}$-Klassen. Man zeigt auch leicht, dass $\equiv_{\mathcal{M}}$-Klassen wieder reguläre Sprachen sind.

Für zwei $\equiv_{\mathcal{M}}$-Klassen $U, V \subseteq A^+$ gilt nun:

$$UV^\omega \cap L \neq \emptyset \implies UV^\omega \subseteq L \tag{7}$$

Existiert nämlich ein $\alpha = uv_1v_2 \cdots \in UV^\omega \cap L$, so gilt für ein beliebiges $\beta = u'v_1'v_2' \cdots \in UV^\omega$, dass $u \equiv_{\mathcal{M}} u'$ sowie $v_i \equiv_{\mathcal{M}} v_i'$ und mit der Definition von $\equiv_{\mathcal{M}}$ sieht man nun leicht, dass β ebenfalls von einem akzeptierten $\mathcal{M}$-Pfad stammt, also $\beta \in L$.

Für eine Menge X sei $\binom{X}{k}$ die Menge der k-elementigen Teilmengen von X. Der Satz von Ramsey sagt nun: Sei X eine unendliche Menge und $K_1, \dots K_t$ eine Partition von $\binom{X}{k}$. Dann gibt ein $T \subseteq X$ unendlich und ein $s \in \{1, \dots, t\}$, sodass $\binom{T}{k} \subseteq K_s$.

Damit wollen wir nun für ein beliebiges $\alpha = a_1a_2a_3 \cdots \in A^\omega$ zeigen, dass es $\equiv_{\mathcal{M}}$-Klassen U, V gibt, sodass $\alpha \in UV^\omega$. Für $i < j \in \mathbb{N}$ sei $\alpha_{ij} := a_i \cdots a_{j-1}$. Offenbar können wir $\binom{\mathbb{N}}{2}$ mit der Menge $\{(i,j) \in \mathbb{N}^2 : i < j\}$ identifizieren.

Für eine $\mathcal{M}$-Klasse M sei $K_M := \{(i,j) : \alpha_{ij} \in M\}$. Dann ist $\{K_M : M \text{ ist } \mathcal{M}\text{-Klasse}\}$ eine endliche Partition von $\binom{\mathbb{N}}{2}$. Nach dem Satz von Ramsey gibt es nun eine $\mathcal{M}$-Klasse V und eine unendliche Menge $I = \{i_1 < i_2 < \cdots\} \subseteq \mathbb{N}$, sodass für alle ℓ gilt $\alpha_{i_\ell i_{\ell+1}} \in V$. Wenn nun U jene $\mathcal{M}$-Klasse bezeichnet, die α_{1i_1} enthält, so folgt $\alpha \in UV^\omega$.

Dies zeigt gemeinsam mit (7), dass

$$A^\omega \setminus L = \bigcup \{UV^\omega : U, V \text{ sind } \mathcal{M}\text{-Klassen sodass } UV^\omega \cap L = \emptyset\},$$

woraus mit (6) folgt, dass $A^\omega \setminus L$ ω-regulär ist. □

Literatur

[1] S. Hetzl. *Theoretische Informatik*. Skriptum zur Vorlesung im Sommersemester 2019. 2019.

[2] H. Straubing. *Finite Automata, Formal Logic, and Circuit Complexity*. Progress in Theoretical Computer Science. Springer Science+Business, 1994.