Eine Mitschrift zu der Vorlesung

„Theoretische Informatik 2“

gehalten an der

Johann Wolfgang von Goethe Universität Frankfurt

von

Herr Prof. Dr. Wotschke

Fassung vom 19. Oktober 2000

Autoren:

Frank Bergmann (bergmann@informatik.uni-frankfurt.de),

Jörn Gersdorf (gersdorf@informatik.uni-frankfurt.de),

Martin Klossek (klossek@informatik.uni-frankfurt.de),

Fabian Wleklinski (wleklins@informatik.uni-frankfurt.de)

1 Inhaltsverzeichnis

Induktionsschritt:

Man beweise durch Induktion $\forall n \geq 3$:

$$q_0 \notin \delta(q_0, x_1 \dots x_n)$$

$$q_1 \in \delta(q_0, x_1 \dots x_n) \Leftrightarrow \text{n ungerade } \wedge x_1 \dots x_n = (ab)^{\frac{n-1}{2}} a$$

$$q_2 \in \delta(q_0, x_1 \dots x_n) \Leftrightarrow \text{n gerade } \wedge x_1 \dots x_n = (ab)^{\frac{n}{2}}$$

$$q_3 \in \delta(q_0, x_1 \dots x_n) \Leftrightarrow n = 3m+1 \wedge x_1 \dots x_n = (abb)^{\frac{n-1}{3}} a$$

$$q_4 \in \delta(q_0, x_1 \dots x_n) \Leftrightarrow n = 3m+2 \wedge x_1 \dots x_n = (abb)^{\frac{n-2}{3}} ab$$

$$q_5 \in \delta(q_0, x_1 \dots x_n) \Leftrightarrow n = 3m \wedge x_1 \dots x_n = (abb)^{\frac{n}{3}}$$

Diese Behauptung müsste nun per Induktion formal bewiesen werden.

Gesamtbeweis

Zusammenfassend mit dem gelungenen Induktionsbeweis folgt also:

$$\begin{aligned}
&\forall n \geq 3: && x_1 \dots x_n \in T(M) \\
&\overset{Def.T}{\Leftrightarrow} && \delta(q_0, x_1 \dots x_n) \cap F \neq \emptyset \\
&\overset{Def.F}{\Leftrightarrow} && q_2 \in \delta(q_0, x_1 \dots x_n) \vee q_5 \in \delta(q_0, x_1 \dots x_n) \qquad (4.13) \\
&\overset{Induktionsbew.}{\Leftrightarrow} && x_1 \dots x_n = (ab)^{\frac{n}{2}} \vee x_1 \dots x_n = (abb)^{\frac{n}{3}} \\
&\Rightarrow && T(M) = \left\{ (ab)^n \middle| n \geq 1 \right\} \cup \left\{ (abb)^n \middle| n \geq 1 \right\}
\end{aligned}$$

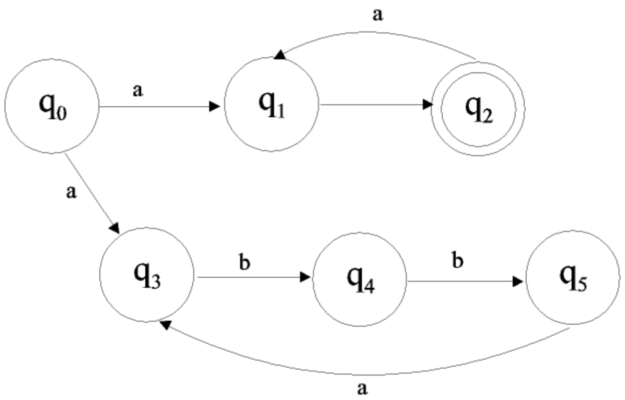

Abbildung 6 – Beispiel eines NFA

Aus diesem Transitionsdiagramm kann man nun die folgenden Transitionen erkennen:

$$\begin{aligned}&\delta(q_0,e)=\{q_0\}\\&\delta(q_0,a)=\{q_1,q_3\}\\&\delta(q_0,ab)=\{q_2,q_4\}\\&\delta(q_0,aba)=\{q_1\}\\&\delta(q_0,abb)=\{q_5\}\end{aligned}\tag{4.12}$$

Um diese zu erhalten, geht man wie folgt vor (wir betrachten das Beispiel $\delta(q_0,ab)\rightarrow\delta(q_0,aba)$):

Betrachte die beiden Zustände q_2 und q_4 aus $\delta(q_0,ab)$. Wohin gelangt man jeweils bei einer weiteren Eingabe von „a“? Von q_2 aus gelangt man nach q_1 (also bilde die Menge $\{q_1\}$), von q_4 aus gelangt man mit „a“ nirgendwohin (bilde die leere Menge { }). Dann vereinige die gefundenen Ergebnismengen. Es ergibt sich die Menge $\{q_1\}$. Also gilt: $\delta(q_0,aba)=\{q_1\}$.

Wir beweisen nun bei diesem NFA, dass er die Sprache $L=\left\{(ab)^n \middle| n\geq 1\right\}\cup\left\{(abb)^n \middle| n\geq 1\right\}$ abbildet.

Wir verwenden hierbei Induktion.

Induktionsverankerung (n <= 2):

$$\begin{aligned}&\forall n\leq 2:\delta(q_0,x_1\ldots x_n)\cap F\neq\emptyset\\&\Leftrightarrow q_2\in\delta(q_0,x_1\ldots x_n)\\&\Leftrightarrow x_1\ldots x_n=ab\end{aligned}$$

---

5. $\delta : Q \times \Sigma \rightarrow P(Q) = 2^Q$ (Potenzmenge) ist die Übergangsfunktion

Wichtig hierbei ist, dass die Ergebnismenge der Übergangsfunktion $\delta'\left(\left[p_1, p_2, \ldots, p_j\right], a\right) = \left[r_1, r_2, \ldots, r_k\right]$ nun also die Potenzmenge von Q ist. δ liefert jetzt also immer eine Menge von Zuständen. Dabei bedeutet $\delta(q,a)$ die Menge aller Zustände p, für die es einen mit a markierten Übergang von q nach p gibt. $\delta(q,a) = \varnothing \in P(Q)$ bedeutet, dass der Übergang für (q,a) undefiniert ist.

4.3.2 Erweiterung von δ des NFA

Die Funktion δ kann folgendermassen auf eine Funktion δ* ausgedehnt werden.

Definition (δ*):

(Erweiterung von $\delta : Q \times \Sigma \rightarrow P(Q)$ auf $\delta^* : Q \times \Sigma^* \rightarrow P(Q)$):

1. $\delta^*(q,e) := \{q\} \in 2^Q$
2. $\delta^*(q,x) := \delta(q,x) \qquad \forall x \in \Sigma$
3. $\delta(q, x_1 \ldots x_n x_{n+1}) := \bigcup\limits_{p \in \delta^*(q, x_1 \ldots x_n)} \delta(p, x_{n+1})$
4. Konvention: δ^* □ δ

4.3.3 Die vom NFA erkannte Sprache

Definition (vom NFA erkannte Sprache):

Sei $M = (Q, \Sigma, \delta, q_0, F)$ ein nichtdeterministischer endlicher Automat (NFA). Dann heißt $T(M) := \left\{x \,\middle|\, x \in \Sigma^* \wedge \left(\delta(q_0, x) \cap F \neq \varnothing\right)\right\}$ die von M erkannte Sprache.

Anmerkung: Diese Definition impliziert, dass es *wenigstens einen* Weg von Startzustand aus geben muss, mit dem man über das Wort x in einem Endzustand landet.

4.3.4 Beispiel eines NFA

Wir betrachten den NFA, der die Sprache $L = \left\{(ab)^n \,\middle|\, n \geq 1\right\} \cup \left\{(abb)^n \,\middle|\, n \geq 1\right\}$ akzeptiert:

Zu (4.5)**:**

Es gilt:

$$\delta\left(q_0, x_1 \ldots x_n x_{n+1}\right) = q_2 = \delta\left(\underbrace{\delta\left(q_0, x_1 \ldots x_n\right)}_{q_1}, x_{n+1}\right)$$

$$\Rightarrow \delta\left(q_0, x_1 \ldots x_{n+1}\right) = q_1 \wedge n \text{ gerade}$$

Auch dieser Fall scheidet aus, weil n ungerade ist.

Zu (4.6)**:**

Dieser Fall ist ähnlich wie beim Fall n ungerade zuvor

zu (4.7)**:**

Ist genauso wie oben.

4.2.5 Beweis der Sprachäquivalenz

Wir müssen nun noch mit Hilfe der aus dem Induktionsbeweis gewonnenen Erkenntnis, wann die Endzustände erreicht werden, zeigen, dass der endliche Automat aus Abbildung 5 tatsächlich T(M) realisiert:

$$\begin{aligned} x_1 \ldots x_n \in T(M) \quad & \Leftrightarrow \delta\left(q_0, x_1 \ldots x_n\right) \in F \\ & \Leftrightarrow \delta\left(q_0, x_1 \ldots x_n\right) = F \\ & \overset{Ind.-Beweis}{\Leftrightarrow} x_1 \ldots x_n = (ab)^{\frac{n}{2}} \wedge \text{n gerade} \end{aligned} \tag{4.11}$$

$$\Rightarrow T(M) = \left\{(ab)^n \middle| n \geq 1\right\}$$

□

4.3 Nichtdeterministische Endliche Automaten (NFA)

Neben den deterministischen endlichen Automaten (DFA) existieren auch nichtdeterministische endliche Automaten (NFA), die sich dadurch auszeichnen, dass bei einem Zustand bei demselben Eingabesymbol keine, eine oder mehr Transitionen erlaubt sind.

Die nichtdeterministischen Automaten sind insbesondere ein nützliches Konzept zum Beweis von Sätzen. Weiter wird sich zeigen, dass die NFAs äquivalent zu den DFAs sind. Insbesondere kann man auch DFAs als einen Spezialfall der NFAs auffassen, nämlich als einen, bei dem es je Zustand eine einzige Transitions für jedes Symbol gibt.

Um zu bestimmen, ob eine bestimmte Zeichenkette w von einem DEA akzeptiert wird, genügt es, diesen einen Pfad zu prüfen. Bei einem NFA kann es viele Pfade geben, die mit w markiert sind. Hier müssen also alle Pfade überprüft werden.

4.3.1 Formale Definition

Definition (NFA):

Ein nichtdeterministischer endlicher Automat ist ein Quintupel $M = \left(Q, \Sigma, \delta, q_0, F\right)$ mit:

1. Q ist eine endliche Menge von Zuständen
2. `T` ist eine endliche Menge von Eingabesymbolen
3. $q_0 \in Q$ ist der Anfangszustand
4. $F \subseteq Q$ ist die Menge der Endzustände (= akzeptierten Zustände)

2 Vorlesung vom 11. April 2000

2.1 Mengen, Mengenoperationen und Relationen

2.1.1 Funktion, Umkehrfunktionen und Abbildungen

Eine Funktion ist eine eindeutige Zuordnung der Elemente einer Menge *A* zu den Elementen einer Menge *B*. Jedem Element von *A* darf höchstens ein Element von *B* zugeordnet sein, verschiedenen Elementen von *A* kann aber dasselbe Element von *B* zugeordnet sein. Es braucht nicht jedem Element von *A* ein Element aus *B* zugeordnet zu sein.

Für beliebige Funktionen gilt:

$$A, B \text{ Mengen, } A \subseteq S_1, B \subseteq S_2, f : S_1 \to S_2$$

$$\begin{aligned} f(A) & \underset{\text{Df}}{=} \left\{ f(x) \middle| x \in A \right\} \\ f'(B) & \underset{\text{Df}}{=} \left\{ x \middle| x \in S_1, f(x) \in B \right\} \end{aligned} \tag{2.1}$$

$$\begin{aligned} A & \subseteq f'\left(f(A)\right) \\ B & \supseteq f\left(f'(B)\right) \end{aligned} \tag{2.2}$$

$$\begin{aligned} f\left(A_1 \cup A_2\right) & = f\left(A_1\right) \cup f\left(A_2\right) \\ f\left(A_1 \cap A_2\right) & \subseteq f\left(A_1\right) \cap f\left(A_2\right) \end{aligned} \tag{2.3}$$

Anmerkungen dazu:

Es ist zu beachten, dass *f'()* keinesfalls die Umkehrfunktion ist – zu dieser wird es erst durch die bijektive Eigenschaft.

Bei der obigen Betrachtung von *A*, *B*, *S₁*, *S₂* und *f()* existieren drei Sonderfälle. 1) Ein Element aus *A* kann nicht nach *B* abgebildet werden, weil f() für dieses Element nicht definiert ist. 2) Für ein bestimmtes Element aus *B* gibt es kein Element aus *A*, das auf dieses Element abgebildet wird. 3) Zwei oder mehr Elemente aus *A* werden auf ein Element in *B* abgebildet. (Die vierte, logische Kombination, nämlich dass ein Element aus *A* auf mehrere Elemente aus *B* abgebildet wird, verbietet der Funktionsbegriff.)

2.1.2 Injektivität, Surjektivität und Bijektivität

Die Begriffe Injektivität, Surjektivität und Bijektitivät entstammen dem mathematischen Sprachgebrauch und müssen daher hier nicht näher erläutert werden. Bedeutsam sind aber die Auswirkungen auf die oben gemachten Aussagen:

$$\begin{aligned} & f \text{ injektiv} \Rightarrow A = f'\left(f(A)\right) \\ & f \text{ injektiv} \Rightarrow f\left(A_1 \cap A_2\right) = f\left(A_1\right) \cap f\left(A_2\right) \end{aligned} \tag{2.4}$$

$$\begin{aligned} & f \text{ surjektiv} \Rightarrow B = f\left(f'(B)\right) \\ & f \text{ surjektiv} \Rightarrow f'\left(B_1 \cap B_2\right) = f'\left(B_1\right) \cap f'\left(B_2\right) \end{aligned} \tag{2.5}$$

$$f \text{ bijektiv} \Rightarrow f^{-1} \text{ (Inverse Funktion) existiert mit } \mathit{Identität} = f \circ f' = f' \circ f \tag{2.6}$$

Generell gilt, es existiert eine bijektive Abbildung zwischen zwei Mengen genau dann, wenn ihre Mächtigkeit identisch ist:

$$|A| = |B| \Leftrightarrow \exists \text{ eine bijektive Funktion } f \text{ mit } f : A \to B \tag{2.7}$$

2.1.3 Relationen

Eine binäre Relation *R* auf einer Menge *M* ist eine Teilmenge von *M*x*M*. Sind $a,b \in M$ und gilt $(a,b) \in R$, so sagt man: „*a* und *b* stehen in der Relation *R*.“ Gelegentlich schreibt man statt $(a,b) \in R$ auch aRb. Eine Relation kann über eine oder mehrere der folgenden Eigenschaften verfügen:

1. Reflexivität: $\forall a \in M : (a,a) \in R$
2. Transitivität: $\forall a,b,c \in M : (a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R$
3. Symmetrie: $\forall a,b \in M : (a,b) \in R \Rightarrow (b,a) \in R$
4. Antisymmetrie: $\forall a,b \in M : (a,b) \in R \wedge (b,a) \in R \Rightarrow a = b$

Beachte: Symmetrie und Transitivität implizieren nicht Reflexivität! Zur Bewertung einer Relation muss jede dieser vier Aussagen einzeln überprüft werden.

2.1.4 Äquivalenzrelationen

Man spricht von einer „*Äquivalenzrelation*“, wenn eine Relation reflexiv, transitiv und symmetrisch ist, und von einer Ordnung, wenn eine Relation reflexiv, transitiv und antisymmetrisch ist. Zum Beispiel ist die normale Vergleichsoperation auf der Menge der reellen Zahlen („=“) eine Äquivalenzrelation, und die kleiner-gleich-Operation („≤“) eine Ordnung.

2.1.5 Äquivalenzklassen

Alle Elemente *b* einer Menge *M*, die zu einem gegebenen Element *a* äquivalent sind, bilden zusammen die „*Äquivalenzklasse*“ des Elementes *a*:

$$[a] \underset{Df}{=} \{ b \mid b \in A \wedge \hat{\ } b \square a \} \tag{2.8}$$

Ist die Schnittmenge zweier Äquivalenzklassen nicht leer, so sind die Äquivalenzklassen identisch:

$$[a] \cap [b] \neq \varnothing \Rightarrow [a] = [b] \tag{2.9}$$

Bei den Äquivalenzklassen kommt die reflexive Eigenschaft der Relationen zum Tragen, da ohne diese Eigenschaft ein Element nicht in seiner eigenen Äquivalenzklasse enthalten wäre.

Es besteht ein Zusammenhang zwischen den Indizes der Äquivalenzklassen und der Anzahl der Zustände eines Automaten.

2.1.6 Kollektionen

Eine Kollektion $C = \{ C_i \mid i \in I \}$ ist eine Menge von Elementen C_i, die über einen Index *i* indiziert werden können, der aus der Indiziermenge *I* stammt.

2.1.7 Partitionen

Eine Kollektion von Mengen C_i heißt *Partition* von *A* genau dann wenn 1) alle Mengen C_i disjunkt oder gleich sind, 2) jede Menge C_i eine Teilmenge von *A* ist, und 3) die Vereinigung aller Mengen C_i die Menge *A* ergibt:

$$\begin{aligned} C \text{ ist Partition von } A \underset{Df}{\Leftrightarrow}\ & 1)\ \forall i,j \in I : C_i = C_j \vee (C_i \cap C_j = \varnothing) \\ & 2)\ \forall i \in I : C_i \subseteq A \\ & 3)\ \bigcup_{i \in I} C_i = A \end{aligned} \tag{2.10}$$

$$\delta(q_0, x_1 \ldots x_n) = q_1$$

$$\overset{IV}{\Rightarrow} x_1 \ldots x_n = (ab)^{\frac{n-1}{2}} a \wedge x_{n+1} = a$$

$$\Rightarrow x_1 \ldots x_n x_{n+1} \square \text{"sonst"}$$

I.2 (q3)

$$\delta(q_0, x_1 \ldots x_n) = q_3$$

$$\overset{IV}{\Rightarrow} x_1 \ldots x_n \square \text{"sonst"} \wedge (x_{n+1} = a \vee x_{n+1} = b)$$

$$\Rightarrow x_1 \ldots x_n x_{n+1} \square \text{"sonst"}$$

„$\Leftarrow$“ Jetzt beweisen wir den Rückweg und beachten zuvor die folgende Regel:

$$x_1 \ldots x_{n+1} \square \text{"sonst"}$$

$$\Rightarrow \mathrm{x}_1 \ldots x_n \square \neg\text{sonst} \ \vee\ \mathrm{x}_1 \ldots x_n \square \text{sonst}$$

II. 1 (not sonst)

$$x_1 \ldots x_n \square \neg\text{sonst}$$

$$\overset{\substack{\text{n ungerade} \\ \text{IV}}}{\Rightarrow} \mathrm{x}_1 \ldots x_n = (ab)^{\frac{n-1}{2}}$$

$$\overset{\substack{x_1 \ldots x_{n+1} \\ =\text{sonst}}}{\Rightarrow} \delta(q_0, x_1 \ldots x_n) = q_1 \wedge x_{n+1} = a$$

$$\Rightarrow \delta(q_0, x_1 \ldots x_{n+1}) = \delta\left(\underbrace{\delta(q_0, x_1 \ldots x_n)}_{q_1}, a \right) = q_3$$

II.2 (sonst)

$$x_1 \ldots x_n \square \text{"sonst"}$$

$$\overset{IV}{\Rightarrow} \delta(q_0, x_1 \ldots x_n) = q3$$

$$\overset{\substack{Def\,\delta \\ Transitionsdiagr.}}{\Rightarrow} \delta(q_0, x_1 \ldots x_{n+1}) = \delta(\delta(q_0, x_1 \ldots x_n), x_{n+1}) = q3$$

zu (4.7)**:**

$\delta(q_0, x_1 \ldots x_{n+1}) = q_0$ ist ein Widerspruch, da $n+1 \geq 2$. Damit kann dieser Fall nicht vorkommen.

Fall 2: n+1 ungerade, n gerade

Dieser Fall ist ganz analog wie Fall 1 zu behandeln:

Zu (4.4)**:**

$$\delta(q_0, x_1 \ldots x_n x_{n+1}) = q_1 \overset{Def\,\delta}{=} \delta\left(\underbrace{\delta(q_0, x_1 \ldots x_n)}_{q_0 \vee q_2}, x_{n+1} \right)$$

q_0 scheidet nach der Induktionsannahme aus, weil $n \geq 1$ gilt.

$$\overset{Def\,\delta}{\Leftrightarrow} \delta(q_0, x_1 \ldots x_n) = q_2 \wedge x_{n+1} = a$$

$$\overset{IV}{\Leftrightarrow} x_1 \ldots x_n = (ab)^{\frac{n}{2}} \wedge x_{n+1} = a$$

$$\Leftrightarrow x_1 \ldots x_n x_{n+1} = (ab)^{\frac{n}{2}} a$$

Wie ist das nun zu lesen? Um nach q_1 zu kommen, muss man nach dem Transitionsdiagramm im vorletzten Schritt in q_0 oder q_2 gewesen sein.

Weil nun $n+1 \geq 2 \Rightarrow n \geq 1$ gilt, kann kann Fall q_0 schon mal nicht vorkommen. q_2 kann nicht vorkommen, weil n ungerade ist. Damit gilt die Prämisse von (4.4) nicht und die Implikation von links nach rechts ist wahr. Liest man (4.4) von rechts nach links, dann gelten q_0 / q_2 ebenfalls nicht und damit ist die Äquivalenz (4.4) insgesamt gezeigt.

Zu (4.5)**:**

$$\delta(q_0, x_1 \ldots x_n x_{n+1}) = q_2 \overset{\text{Def. von } \delta}{=} \delta\left(\underbrace{\delta(q_0, x_1 \ldots x_n)}_{=q_1}, x_{n+1}\right) \tag{4.9}$$

Wieder haben wir das Transitionsdiagramm betrachtet und sind diesmal nur auf q_1 als letzten möglichen Schritt gestoßen.

Wir betrachten nun zunächst den Weg von links nach rechts in (4.5)**:**

$$\delta(q_0, x_1 \ldots x_n x_{n+1}) = q_2 \overset{\text{Def. von } \delta}{=} \delta\left(\underbrace{\delta(q_0, x_1 \ldots x_n)}_{=q_1}, x_{n+1}\right)$$

$$\overset{IV}{\Rightarrow} x_1 \ldots x_n = (ab)^{\frac{n-1}{2}} a \wedge x_{n+1} = b$$

$$\Rightarrow x_1 \ldots x_{n+1} = (ab)^{\frac{n+1}{2}}$$

Natürlich muss auch der Rückweg gezeigt werden. Dies funktioniert aber analog:

$$\text{n ungerade } \wedge \mathrm{x}_1 \ldots x_{n+1} = (ab)^{\frac{\mathrm{n}+1}{2}}$$

$$\Rightarrow n+1 \text{ gerade } \wedge \mathrm{x}_1 \ldots x_{n+1} = (ab)^{\frac{\mathrm{n}+1}{2}}$$

$$\Rightarrow n+1 \text{ gerade } \wedge \mathrm{x}_1 \ldots x_{n+1} = (ab)^{\frac{\mathrm{n}-1}{2}} ab$$

$$\overset{IV}{\Rightarrow} \delta(q_0, x_1 \ldots x_n) = q_1 \wedge x_{n+1} = b$$

$$\overset{Def.\delta,IV}{\Rightarrow} \delta(q_0, x_1 \ldots x_{n+1}) = q2$$

Damit haben wir die Äquivalenz gezeigt.

Zu (4.6)**:**

Hier ergibt sich:

$$\delta(q_0, x_1 \ldots x_n x_{n+1}) = q_2 \overset{\text{Def. von } \delta}{=} \delta\left(\underbrace{\delta(q_0, x_1 \ldots x_n)}_{=q_0 \vee q_1 \vee q_2 \vee q_3}, x_{n+1}\right) \tag{4.10}$$

Wie zuvor scheidet q_0 aus, da $n \geq 1$ und q_2 scheidet aus, weil n ungerade ist.

„$\Rightarrow$“ Wir wählen zunächst den Schritt von links nach rechts:

I.1 (q1)

Die Menge der Äquivalenzklassen aller Elemente einer gegebenen Menge *A* ist eine Partition von *A*: $C = \{[a] \mid a \in A\}$ ist eine Partition von *A*.

2.2 Algebraische Strukturen

2.2.1 Die algebraische Struktur

Die algebraische Struktur ist wichtig, da sich jeder endlicher Automat als algebraische Struktur darstellen lässt. Die algebraische Struktur besteht aus einer Menge, und aus einer Rechenoperation auf dieser Menge:

$$\langle S, \circ \rangle \text{ ist eine algebraische Struktur} \underset{Df}{\Leftrightarrow} \begin{array}{l} 1)\ S \text{ ist eine Menge} \\ 2)\ \circ : SxS \to S \end{array} \tag{2.11}$$

Schreibweise: $\circ(a,b)$ oder $a \circ b$.

2.2.2 Die Halbgruppe

Die Halbgruppe ist eine algebraische Struktur, für deren Operation das Assoziativgesetz gilt:

$$\langle S, \circ \rangle \text{ ist eine Halbgruppe} \underset{Df}{\Leftrightarrow} \begin{array}{l} 1)\ \langle S, \circ \rangle \text{ ist eine algebraische Struktur} \\ 2)\ \forall \mathrm{s}_1, \mathrm{s}_2, \mathrm{s}_3 \in S : \circ(\circ(s_1, s_2), s_3) = \circ(s_1, \circ(s_2, s_3)) \end{array} \tag{2.12}$$

2.2.3 Das Monoid

Das Monoid ist eine Halbgruppe mit Einselement:

$$\langle S, \circ \rangle \text{ ist ein Monoid} \underset{Df}{\Leftrightarrow} \begin{array}{l} 1)\ \langle S, \circ \rangle \text{ ist eine Halbgruppe} \\ 2)\ \exists \mathrm{e} \in \mathrm{S}\ \forall \mathrm{s} \in \mathrm{S} : \mathrm{e} \circ \mathrm{s} = \mathrm{s} \circ \mathrm{e} = \mathrm{s} \end{array} \tag{2.13}$$

2.2.4 Das freie Erzeugendensystem, das freie Monoid

G ist ein freies Erzeugendensystem für $\langle S, \circ \rangle$, wenn 1) jedes Element aus *S* als Kombination von Elementen aus *G* darstellbar ist, und 2) jede dieser Darstellungen eindeutig ist.

$$G \text{ ist ein freies Erzeugendensystem für } \langle S, \circ \rangle \underset{Df}{\Leftrightarrow}$$

$$\begin{array}{l} 1)\ \forall s \in S \setminus \{e\} \exists g_1, \ldots, g_n \in G : s = g_1 \circ \ldots \circ g_n \\ 2)\ \mathrm{s} = g_{i_1} \circ \ldots \circ g_{i_n} \wedge \mathrm{s} = g_{j_1} \circ \ldots \circ g_{j_n} \Rightarrow n = m \wedge g_{i_k} = g_{j_k} \quad 1 \leq k \leq n \end{array} \tag{2.14}$$

Schreibweise: „*G* ist ein freies Erzeugendensystem für $\langle S, \circ \rangle$“ oder „$\langle S, \circ \rangle$ ist ein freies Monoid über *G*“.

Beispiele:

$\langle N, + \rangle$ ist ein freies Monoid über {1}, $\langle N, + \rangle$ ist kein freies Monoid über {1,2}

2.2.5 Der Homomorphismus

Ein *Homomorphismus* ist die Kombination zweier algebraischer Strukturen $\langle S_1, \circ \rangle$, $\langle S_2, \bullet \rangle$ und einer Funktion *h()*, die die Eigenschaft besitzt, kommutativ bezüglich der Verknüpfungsoperationen (der algebraischen Strukturen) zu sein:

$$h \text{ ist ein Homomorphismus} \Leftrightarrow$$

$$\begin{array}{l} 1)\ h : S_1 \to S_2 \\ 2)\ \forall a_1, a_2 \in S_1 : h(a_1 \circ a_2) = h(a_1) \bullet h(a_2) \end{array} \tag{2.15}$$

2.2.6 Der Isomorphismus

Ein *Isomorphismus* ist ein bijektiver Homomorphismus. Wenn zwei Mengen isomorph zueinander sind, bedeutet das, dass sie sich (von den Bezeichnern ihrer Elemente abgesehen) nicht voneinander unterscheiden lassen. Ein minimaler Automat ist „bis auf Isomorphismen exakt bestimmt“.

$$\begin{aligned} &h \text{ ist ein Isomorphismus} \Leftrightarrow \\ &\quad 1)\ h : \langle S_1, \circ \rangle \to \langle S_2, \bullet \rangle \text{ ist ein Homomorphismus} \\ &\quad 2)\ h : S_1 \to S_2 \text{ ist bijektiv} \end{aligned} \tag{2.16}$$

Beispiele:

h(n)=2ⁿ: *h* ist Homomorphismus, aber nicht Isomorphismus

2.2.7 Abzählbarkeit

Eine Menge *M* heißt *„abzählbar unendlich*“, wenn es eine bijektive Abbildung ihrer Elemente auf die Menge der natürlichen Zahlen gibt:

$$M \text{ ist abzählbar unendlich} \Leftrightarrow \exists\, f : M \to N \,\middle|\, f \text{ ist bijektiv} \tag{2.17}$$

$$M \text{ ist überabzählbar unendlich} \Leftrightarrow \neg\, M \text{ ist abzählbar unendlich} \tag{2.18}$$

Anmerkung: Wie es der Name sagt, bedeutet „Abzählbarkeit“, dass die Elemente einer Menge zwar zahlreich oder unendlich sind, dass sie aber dennoch abzählbar sind.

Beispiel:

Die Menge der rationalen Zahlen ist abzählbar unendlich, die Menge der irrationalen Zahlen (und damit auch die Menge der reellen Zahlen) ist überabzählbar unendlich.

2.2.8 Konkatenation

Die Konkatenation zweier Mengen S_1 und S_2 ist die Menge aller „zusammengesetzten“ Elemente dieser beiden Mengen:

$$S_1 \bullet S_2 \underset{Df}{=} \left\{ uv \,\middle|\, u \in S_1, v \in S_2 \right\} \tag{2.19}$$

2.3 Sprachen

Sei Σ eine endliche Menge von Symbolen, und • der Operator für die Konkatenation. Eine Sprache *L* ist definiert als Teilmenge der Menge aller Wörter über diesem Symbolalphabet:

$$\begin{aligned} &\Sigma^0 \underset{Df}{=} \{e\} && \text{(das leere Wort)} \\ &\Sigma^1 \underset{Df}{=} \Sigma && \text{(Wörter der Länge 1)} \\ &\vdots \\ &\Sigma^n \underset{Df}{=} \Sigma^{n-1} \bullet \Sigma && \text{(Wörter der Länge n)} \end{aligned} \tag{2.20}$$

$$\begin{aligned} &\Sigma^* \underset{Df}{=} \bigcup_{n=0}^{\infty} \Sigma^n && \text{(Alle Wörter über } \Sigma\text{)} \\ &\Sigma^+ \underset{Df}{=} \bigcup_{n=1}^{\infty} \Sigma^n && \text{(Alle Wörter über } \Sigma \text{ außer dem leeren Wort)} \end{aligned} \tag{2.21}$$

$$L \text{ ist eine Sprache über dem Alphabet } \Sigma \underset{Df}{\Leftrightarrow} L \subseteq \Sigma^* \tag{2.22}$$

$\langle \Sigma^*, \bullet \rangle$ ist das freie Monoid über Σ, wobei die Konkatenation („•“) die Operation ist. Σ dient hier als freies Erzeugendensystem.

Eingabefolgen) dieser Zustand erreicht werden kann. Diese Überlegungen führen uns zu den folgenden Behauptungen:

4.2.2 Induktionsbehauptungen:

$$\delta(q_0, x_1 \dots x_n) = q_1 \Leftrightarrow \text{n ungerade } \wedge x_1 \dots x_{n-1} = (ab)^{\frac{n-1}{2}} \wedge x_n = a \tag{4.4}$$

$$\delta(q_0, x_1 \dots x_n) = q_2 \Leftrightarrow \text{n gerade } \wedge x_1 \dots x_n = (ab)^{\frac{n}{2}} \tag{4.5}$$

$$\delta(q_0, x_1 \dots x_n) = q_3 \Leftrightarrow x_1 \dots x_n \;\square\; \text{"sonst"} \tag{4.6}$$

$$\delta(q_0, x_1 \dots x_n) \neq q_0 \tag{4.7}$$

Als Erläuterung der Induktionsbehauptungen betrachten wir (4.4): Nach dem Transitionsdiagramm kann q_1 nur dann erreicht werden, wenn – ausgehend vom Startzustand q_0 - eine „ab“-Folge mit abschließendem „a“ als Eingabezeichenkette vorliegt (z. B. „ababababa“). Die Anzahl der Zeichen ist hierbei stets ungerade.

4.2.3 Induktionsverankerung:

Wir beweisen durch Induktion über die Länge der Eingabefolgen und wählen n=1 (also eine Zeichenkette der Länge 1). Wir zeigen für die einzelnen Induktionsbehauptungen deren Richtigkeit für n=1:

zu (4.4) $\delta(q_0, x_1) = q_1 \Leftrightarrow x_1 = a \Leftrightarrow x_1 = (ab)^{\frac{0}{2}} a$

zu (4.5) $\delta(q_0, x_1) = q_2$ tritt nicht auf (siehe Erläuterung)

zu (4.6) $\delta(q_0, x_1) = q_3 \Leftrightarrow x_1 = b \Leftrightarrow x_1 = \text{"sonst"}$

zu (4.7) $\delta(q_0, x_1) \neq q_0$ (siehe Erläuterung)

Hierzu folgende Erläuterungen: Die Äquivalenzen sind natürlich dadurch zu zeigen, dass man die Implikationen sowohl von links nach rechts ($\Rightarrow$) als auch von rechts nach links ($\Leftarrow$) begründen muss.

Zum Falle von (4.5) ist zu sagen, dass zunächst („$\Rightarrow$“) der Fall, mit n=1 (nur einem Zeichen) q_2 nicht zu erreichen ist. Damit ist die Prämisse falsch, die Implikation also wahr. Die andere Richtung („$\Leftarrow$“): n ist ungerade, damit ist wiederum die Prämisse falsch und die Implikation wahr.

Zu (4.7): Nach dem Transitionsdiagramm wird q_0 bereits mit einem Eingabezeichen verlassen und kann nie wieder erreicht werden.

4.2.4 Induktionsschritt ($n \to n+1$):

Wir nehmen hier eine Fallunterscheidung vor. Solche Fallunterscheidungen sind in Induktionsbeweisen von endlichen Automaten häufig vorzunehmen. In unserem Falle bietet sich eine Fallunterscheidung nach dem Kriterium „n gerade?“ an, da dieses Kriterium in unseren Induktionsbehauptungen eine Rolle spielt.

Fall 1: n+1 gerade, n ungerade

Zu (4.4)**:**

$$\delta(q_0, x_1 \dots x_n x_{n+1}) = q_1 \overset{\text{Def. von } \delta}{=} \delta\left(\underbrace{\delta(q_0, x_1 \dots x_n)}_{= q_0 \vee q_2}, x_{n+1} \right) \tag{4.8}$$

4 Vorlesung vom 18. April 2000

4.1 Beweis eines DFA (deterministischer endlicher Automat)

Bereits im letzten Protokoll wurde unser Beispielautomat vorgestellt. Er erkennt die folgende Sprache:

$$T(M) := \{(ab)^n \mid n \geq 1\} \subseteq \Sigma^* \qquad (4.1)$$

Der Automat selbst ist in der folgenden Abbildung graphisch dargestellt:

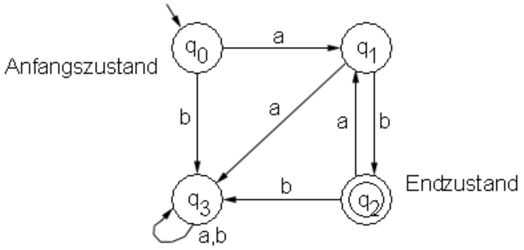

Abbildung 5 - Beispiel eines endlichen Automaten

4.2 Vorgehensweise

Was haben wir nun zu tun, wenn wir beweisen wollen, dass der gezeigte endliche Automat wirklich die Sprache T(M) akzeptiert? Wir müssen zeigen, dass der Automat wirklich nur für die Zeichenfolgen im Endzustand $q_2 \in F = \{q2\}$ landet, die in der Sprachspezifikation (4.1) angegeben wurden.

Die *allgemeine Vorgehensweise* lautet für einen solchen Beweis dann wie folgt:

1. Aufstellen von Induktionsbehauptungen für jeden Zustand des endlichen Automaten, also für jedes $q \in Q$. Die Induktionsbehauptungen haben die allgemeine Form

   $$\delta(q_0, x_1, \ldots, x_n) = q_i \Leftrightarrow \{\text{Bedingung für Erreichen des Zustandes}\} \qquad (4.2)$$

2. Beweis der Behauptungen per Induktion
3. Beweis der gewünschten Spracheigenschaft durch folgende Äquivalenz. Mit „gewünschter Sprachspezifikation" ist eine Beschreibung von $x_1 \ldots x_n$ in der Form gemeint, dass $x_1 \ldots x_n$ die gewünschte Sprache darstellen.

   $$x_1 \ldots x_n \in T(M) \Leftrightarrow \{\text{gewünschte Sprachspezifikation}\} \qquad (4.3)$$

Bei oberflächlicher Betrachtungsweise fragt man sich leicht, wieso es nicht reicht, die Induktionsbehauptungen für die Endzustände zu beweisen. Dies liegt daran, dass die Endzustände i. d. R. nur über andere Zustände erreicht werden können, deren Eigenschaften also auch bewiesen werden müssen.

4.2.1 Beweis des Beispiels

Zu zeigen:

Wir haben zu zeigen: $T(M) = \{(ab)^n \mid n \geq 1\}$

Wir stellen nun zunächst die Induktionsbehauptungen gemäß (4.2) auf. Hierzu betrachten wir im Transitionsdiagramm (Abbildung 5) jeden einzelnen Zustand und überlegen uns, wann (für welche

---

Die Menge aller Wörter über einem Alphabet Σ (entspricht Σ^*) ist abzählbar unendlich; die Menge aller Sprachen über Σ ist überabzählbar unendlich.

2.4 Grammatiken

Die zulässige Form der Sätze einer Sprache nennt man *Syntax*, die Bedeutung der Sätze wird durch die *Semantik* beschrieben. Zur Festlegung der Syntax einer Spracheverwendet man Grammatiken. Eine Grammatik ist eine Menge von Regeln, die bestimmen, welche Sätze zur Sprache gehören, und welche nicht. Man spricht von *Chomsky-Grammatiken*, wenn eine Grammatik durch vier Angaben definiert wird: durch eine Menge von *Terminalsymbolen*, eine Menge von *Nichtterminalsymbolen*, eine Menge von Grammatikregeln und durch ein Startsymbol.

Von einer Grammatik wird gefordert, dass sie ein endlich langer Beschreibungsmechanismus für eine Sprache ist. Solche endlich langen Beschreibungsmechanismen können der Länge nach, und innerhalb einer Länge alphabetisch geordnet werden. Somit ist die Menge der Grammatiken abzählbar unendlich. Weil die Menge der Sprachen aber überabzählbar unendlich ist, folgt daraus, dass es Sprachen gibt, die keine Grammatik haben können.

Wie viele Sprachen gibt es, die eine Grammatik haben?

Weil es insgesamt nur abzählbar unendlich viele Grammatiken gibt, ist auch die Menge aller Grammatiken für eine beliebige Sprache über Σ nur abzählbar unendlich. Daraus folgt, dass die Menge der Sprachen mit Grammatik höchstens ebenfalls abzählbar unendlich ist. „Höchstens" deswegen, weil u.U. mehrere Grammatiken die selbe Sprache beschreiben.

Wie viele Sprachen gibt es, die keine Grammatik haben?

Es gibt überabzählbar unendlich viele Sprachen, die keine Grammatik haben. Der Beweis gestaltet sich recht einfach. Wir haben bereits festgestellt, dass es nur abzählbar unendlich viele Sprachen gibt, die eine Grammatik haben. Gäbe es ebenfalls nur abzählbar unendlich viele Sprachen, die keine Grammatik haben, so würden auch insgesamt nur abzählbar unendlich viele Sprachen existieren. Wir haben aber bereits festgestellt, dass überabzählbar unendlich viele Sprachen existieren (Widerspruch!).

2.5 Klassifizierung von Sprachen

Noam Chomsky hat 1956 eine Klassifizierung der künstlichen Sprachen vorgeschlagen, die sich bis heute erhalten hat. Sie sieht vor, Grammatiken in insgesamt vier verschiedene Gruppen zu kategorisieren. Jede Gruppe verfeinert die vorhergehende Gruppe, bzw. beinhaltet sie. Zu diesen vier Gruppen hat sich im Laufe der Zeit eine fünfte Gruppe gesellt:

Klassifizierung nach Chomsky	Verschiedene Methoden (Klassen), Automaten (Klassen)	Grammatiken
Chomsky-3	Endliche Automaten - deterministisch - nichtdeterministisch	Reguläre Grammatiken
Chomsky-2	Pushdown-Automaten (Kellerautomaten)	Kontext-freie Grammatiken
	Deterministische Pushdown-Automaten	LR(z) – Grammatiken
Chomsky-1	Linear beschränkte Automaten	Kontext-sensitive Grammatiken
Chomsky-0	Turing-Maschinen	Rekursiv aufzählbare Mengen

3 Vorlesung vom 13. April 2000

3.1 Abzählbarkeit von Mengen, Diagonalisierung

3.1.1 Mächtigkeit von Mengen

Mengen sind endliche oder unendliche Ansammlungen von Elementen. Die Anzahl dieser Elemente einer Menge wird *Mächtigkeit* oder auch *Kardinalität* genannt. Die formale Notation dafür ist:

$$|M| = \text{Mächtigkeit der Menge M} \tag{3.1}$$

Haben zwei Mengen M_1 und M_2 die gleiche Mächtigkeit und existiert zwischen den beiden Menge eine bijektive Abbildung, gilt also

$$\begin{gathered} |M_1| = |M_2| \\ f: M_1 \to M_2 \mid \text{f ist bijektiv} \end{gathered} \tag{3.2}$$

so heißen die Mengen *gleichmächtig*. Für den Spezialfall, dass eine Menge M gleichmächtig der Menge der natürlichen Zahlen □ ist, so ist die Menge M *abzählbar unendlich*. Endliche Mengen sind immer *abzählbar*. Dementsprechend wird eine Menge, deren Mächtigkeit größer der Menge der natürlichen Zahlen ist, für die es also keine bijektive Abbildung zwischen den beiden Mengen gibt und die somit nicht abzählbar ist, *überabzählbar* genannt.

Einfacher ausgedrückt sind Mengen genau dann abzählbar, wenn ihre Elemente durchnumeriert werden können. Dann existiert eine surjektive Abbildung der natürlichen Zahlen auf die betrachtete Menge, so dass jedes Element der Menge einer natürlichen Zahl zugeordnet ist.

3.1.2 one-to-one-Mapping

Die im vorangegangenen Abschnitt beschriebene Gleichmächtigkeit zweier Mengen kann auch mit dem Schlagwort *one-to-one-mapping* illustriert werden. Seien beispielsweise folgende Mengen gegeben:

$$S_1 = \{\text{gerade Zahlen}\} \text{ und } S_2 = \{\text{alle ganzen Zahlen}\} \tag{3.3}$$

Dann kann S_1 eindeutig auf S_2 abgebildet werden mit der Funktion

$$\begin{gathered} S_1 \to S_2 \\ f(2i) \to i \end{gathered} \tag{3.4}$$

Es liegt eine bijektive Abbildung zwischen den beiden Mengen vor, so dass die Mengen von gleicher Mächtigkeit (Kardinalität) sind. Man kann den Begriff one-to-one-mapping verwenden, da jedes Element der einen Menge genau einem Element der anderen Menge zugeordnet wird und umgekehrt.

Ein weiteres Beispiel sei mit folgenden Mengen gegeben:

$$S_1 = \{\text{ganze, positive Zahlen}\} \text{ und } S_2 = \{\text{ganze, negative Zahlen}\} \tag{3.5}$$

Auch hier liegt eine eindeutige Abbildung von S_1 auf S_2 vor:

$$\begin{gathered} S_1 \to S_2 \\ f(i) \to -i \end{gathered} \tag{3.6}$$

Folglich sind S_1 und S_2 gleichmächtig, was noch einmal durch eine grafische Diagonalisierung verdeutlicht werden kann.

Zur Vereinfachung der Notation legt man fest, dass

$$\delta^* \;\square\; \delta \tag{3.27}$$

Daraus folgt, dass die *akzeptierte Sprache* des Automaten $M = (Q, \Sigma, \delta, q_0, F)$ definiert ist als

$$T(M) := \{x \mid x \in \Sigma^* \;\wedge\; \delta(q_0, x) \in F\} \tag{3.28}$$

3.3.4 Beispiel eines endlichen Automaten

Ein Beispiel eines endlichen, deterministischen Automaten sei ein Automat, der eine Sprache erkennt, die aus einer beliebig langen Folge von ab besteht:

$$T(M) := \{(ab)^n \mid n \geq 1\} \tag{3.29}$$

Mit Hilfe eines Induktionsbeweises, der ausführlich am nächsten Vorlesungstag behandelt wird, kann die Korrektheit des folgenden Graphen bewiesen werden:

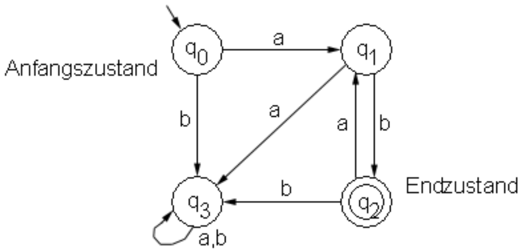

Abbildung 4 - Beispiel eines endlichen Automaten

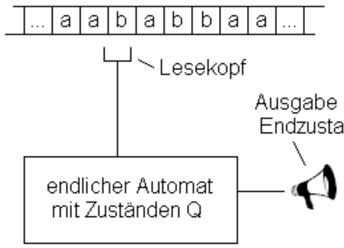

Abbildung 3 - Prinzip eines endlichen Automaten

Die übliche anschauliche Notation eines endlichen Automaten ist der Graph. Eine Kante verbindet Knoten, die den Zuständen entsprechen. Für jedes Zeichen des Eingabealphabets gibt es eine eigene Kante, die vom jeweiligen Zustand zu einem Folgezustand führt.

3.3.2 Definition

Ein *deterministischer endlicher Automat* auch *Finite State Maschine* (FSM) oder *Deterministic Finite Automation* (DFA) genannt, setzt sich aus fünf charakteristischen Eigenschaften zusammen, so dass ein solcher Automat ein 5-Tupel darstellt:

$$M = (Q, \Sigma, \delta, q_0, F) \tag{3.23}$$

Dabei bezeichnet Q die Menge der *Zustände*, Σ das *Eingabealphabet*, δ die *Übergangsfunktion*, q_0 den *Startzustand* und F die Menge der *Endzustände*. Ausführlicher haben die 5 Elemente folgende Funktionen:

- Q ist eine endliche Menge von Zuständen (daher der Name!)
- Σ ist eine endliche Menge von Eingabesymbolen, das Eingabealphabet
- $\delta : Q \times \Sigma \to Q$ ist eine Übergangsfunktion (kartesisches Produkt von Zustand und Eingabesymbol), die einem Zustand und Element des Eingabealphabets einen Folgezustand zuordnet
- q_0 ist der Startzustand des Automaten mit $q_0 \in Q$
- F ist eine Menge von Endzuständen (akzeptierende Zustände) mit $F \subseteq Q$

Charakteristisch für diesen Automatentyp (es gibt auch weitere wie wir später sehen werden) ist, dass jeder Kombination aus Zustand und Eingabesymbol ein eindeutiger Folgezustand zugeordnet wird. Verschiedene Kombinationen können jedoch auf den gleichen Folgezustand zeigen.

3.3.3 Erweiterung von $\delta : Q \times \Sigma \to Q$ auf $\delta^* : Q \times \Sigma^* \to Q$

Um Wörter auf ihre Sprachzugehörigkeit zu prüfen, ist es sinnvoll, als Eingabe für eine Übergangsfunktion nicht nur einzelne Zeichen sondern ganze Wörter zuzulassen. Diese neue Übergangsfunktion wird dann δ^* genannt. Da sie auf dem freien Monoid Σ arbeitet, kann sie auch das leere Wort verarbeiten. Prinzipiell handelt es sich bei δ^* um eine rekursive Mehrfachausführung des einfachen δ.

Es gelten folgende Axiome:

$$\delta^*(q, e) = q \tag{3.24}$$

$$\delta^*(q, a) = \delta(q, a) \quad \forall q \in Q, \forall a \in \Sigma, \tag{3.25}$$

$$\delta^*(q, a_1, a_2, ..., a_n) = \delta(\delta^*(q, a_1, a_2, ..., a_{n-1}), a_n) \tag{3.26}$$

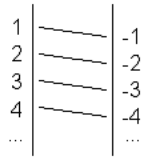

Abbildung 1 - Grafische Zuordnung von Mengenelementen

Zur Motivation ist anzumerken, dass die detaillierte Beschreibung dieses Themas als sinnvoll zu erachten ist, da viele Beweise der kommenden Wochen in ihrer Basis auf diesem Vorgehen basieren und die Begriffe so zu den Essentials der Veranstaltung gehören.

3.1.3 Abzählbarkeit rationaler Zahlen

Ein Beispiel für einen Beweis der Abzählbarkeit einer Menge ist die Abzählbarkeit der rationalen Zahlen. Die rationalen Zahlen ist die Menge der Bruchzahlen, die Vereinigung einer Zählermenge A und einer Nennermenge B mit A und B gleich Menge der ganzen Zahlen $\mathbb{Z}$.

$$p = \frac{a}{b} \text{ mit } a, b \in \mathbb{Z} \tag{3.7}$$

Dies läßt sich leicht mit einer einfachen Darstellung und der aus der Mathematik bekannten Gesetzmäßigkeit beweisen, dass die Vereinigung abzählbar vieler abzählbarer Mengen (wie die der ganzen Zahlen) wieder eine abzählbare Menge ist.

Jedes Element der Zählermenge besitzt eine abzählbare Menge von Elementen im Nenner, die Menge der ganzen Zahlen eben. Ebenso gibt es eine abzählbare Menge von Zählerelementen, so dass man folgendes unendliches Schema anwenden kann, wobei die Pfeile eine lineare Numerierung bedeuten, beginnend mit der linken oberen Ecke. Folglich ist die Menge der rationalen Zahlen abzählbar unendlich.

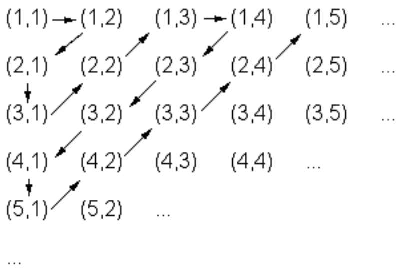

Abbildung 2 - Quadratisch unendliches Schema der Bruchzahlen

Formal läßt sich eine Zeile des Schemas folgendermaßen ausdrücken:

$$P_z := \left\{ \frac{z}{k} \mid k \in \mathbb{Z} \setminus \{0\} \right\} \text{ für } z \in \mathbb{Z} \tag{3.8}$$

Da alle P_z abzählbar sind, ist auch die Vereinigung abzählbar vieler solcher Mengen abzählbar und damit die Menge der rationalen Zahlen abzählbar:

$$\square = \bigcup_{z \in \square} P_z \qquad (3.9)$$

3.1.4 Überabzählbarkeit reeller Zahlen

Die Menge der reellen Zahlen ist die Menge der Dezimalzahlen mit endlichen und unendlicher Periode. Man kann die Zahlen im Bereich]0,1[in einem Schema anordnen und dann eine *Cantorsches Diagonalverfahren* genannte Methode anwenden. Ist bereits dieses Intervall nicht abzählbar, so ist die gesamte Menge der reellen Zahlen überabzählbar.

Nehmen wir zunächst an, das Intervall sei abzählbar und es existiere dementsprechend eine surjektive Abbildung $f : N \to]0,1[$. Sei x_n eine Zahl aus diesem Intervall, die sich aus Stellen $a_1,a_2,a_3,...$ zusammensetzt:

$$\begin{aligned} x_1 &= 0, a_{11}a_{12}a_{13}... \\ x_2 &= 0, a_{21}a_{22}a_{23}... \\ x_3 &= 0, a_{31}a_{32}a_{33}... \\ &... \end{aligned} \qquad (3.10)$$

Sei nun c eine weitere Zahl aus dem Intervall mit

$$c = 0, c_1c_2c_3... \qquad (3.11)$$

wobei sich c_i folgendermaßen zusammensetzt, also Stellen aus x_n neu zusammensetzt (diagonal im Schema wegen a_{ii}):

$$c_i = \begin{cases} 5 \text{ für } a_{ii} \neq 5 \\ 4 \text{ für } a_{ii} = 5 \end{cases} \qquad (3.12)$$

Somit ist gewährleistet, dass c_i niemals gleich a_{ii} ist und mindestens in einer Stelle verschieden. Damit ist c ungleich jedem beliebigen x_n. Wenn das Intervall abzählbar ist, müßte ein x_j mit $x_j = c$ existieren. Das ist jedoch ein Widerspruch und somit ist das Intervall der nicht abzählbar. Daraus folgt, dass die reellen Zahlen ebenfalls nicht abzählbar, sondern überabzählbar sind.

Würde man diesen Beweis auf die Menge der rationalen Zahlen anwenden, könnte man leicht den Fehler machen und übersehen, dass es sich bei x_n um Dezimalzahlen mit unendlicher Periode handelt. So ist bei den rationalen Zahlen das c ebenfalls ungleich jedem beliebigen x_n. Allerdings ist c zugleich auch nicht mehr Element der rationalen Zahlen (sondern der reellen). Die Bedingung der Abgeschlossenheit ist damit nicht mehr erfüllt und somit nichts über die Abzählbarkeit der Menge der rationalen Zahlen ausgesagt.

3.2 Transitive und reflexive Hülle

3.2.1 Definition

Das *Relationenprodukt* zweier Relationen R und S wird folgendermaßen definiert:

$$RS = R \circ S = \{(x,y) \mid \exists z \text{ mit } xRz \wedge zSy\} \qquad (3.13)$$

Dabei wird gewissermaßen die Transitivität über zwei Relationen hinweg ausgedrückt. Insbesondere heißt eine Relation transitiv, wenn das Relationenprodukt mit sich selbst wieder Teilmenge der Relation ist:

$$R \circ R \subseteq R \qquad (3.14)$$

$$R \circ R = \{(x,y) \mid \exists z \text{ mit } xRz \wedge zRy\} \qquad (3.15)$$

Bestimmt man dieses Relationenprodukt unendlich oft und vereinigt anschließend die Relationenprodukte, so erhält man den transitiven Abschluß (auch transitive Hülle genannt):

$$R^+ = tra(R) = \bigcup_{n \geq 1} R^n = R \cup R \circ R \cup R \circ R \circ R \cup R^4 \cup R^5 ... \qquad (3.16)$$

Für R^0 definiert man die identische, reflexive Abbildung auf der Menge A:

$$R^0 = \{(x,x) \mid x \in A\} \qquad (3.17)$$

Die Vereinigung von transitiver Hülle und der identischen Abbildung R0 wird reflexive Hülle genannt:

$$R^* = R^+ \cup R^0 = \bigcup_{n \geq 0} R^n = R^0 \cup R^1 \cup R^2 \cup R^3 \cup R^4 ... \qquad (3.18)$$

Ein interessanter Anwendungsfall der transitiven Hülle in Verbindung mit einer Relationenmatrix ist das Wege-Problem, bei dem die kürzeste Entfernung zwischen zwei Punkten über andere Punkte hinweg gesucht (*traveling salesman problem*)

3.2.2 Beispiele

Sei R eine Relation mit

$$R = \{(1,2),(2,2),(2,3)\} \qquad (3.19)$$

auf der Menge A mit

$$A = \{1,2,3\} \qquad (3.20)$$

Dann ergibt sich die transitive Hülle R^+ von R folgendermaßen

$$R^+ = \{(1,2),(1,3),(2,2),(2,3)\} \qquad (3.21)$$

und die relfexive Hülle R* entsprechend

$$R^* = \{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\} \qquad (3.22)$$

3.3 Endliche Automaten (FSM, DFA)

3.3.1 Veranschaulichung und Darstellung

Ein *Automat* kann als eine Blackbox, beispielsweise als Modell eines elektrischen Schaltwerks betrachtet werden. Füttert man den Automaten mit einer Eingabe, kann er diese akzeptieren oder nicht akzeptieren. Damit lassen sich Eingaben in die Gruppe der erkannten und die Gruppe der nicht erkannten Wörter einordnen, wobei die Menge der erkannten Wörter die Sprache ist, auf die der Automat hält.

Mit Hilfe eines Automaten läßt sich also eine Sprache definieren, genau wie bei der Definition einer Grammatik, nur dass bei der Grammatik die Wörter der Sprache gewissermaßen als Produkt entstehen, während der Automat die Eingabewörter auf ihre Zugehörigkeit zu der betrachteten Sprache prüft.

Wie beschrieben, erkennt ein Automat eine Sprache $L \subseteq \Sigma^*$. Das läuft so ab, dass der Automat ein beliebigen Wort $x_1x_2...x_n$ als Eingabe erhält und Zeichen für Zeichen gemäß Übergangsfunktion abarbeitet. Er wechselt dabei so lange den Zustand, bis das letzte Eingabezeichen erreicht ist. Befindet sich der Automat dann in einem Endzustand, dann gehört das Eingabewort zur Sprache L. Befindet er sich in einem anderen Zustand, gehört das Wort nicht zur Sprache L.

Verdeutlicht wird das Prinzip durch eine bildhafte Darstellung wie folgt. Dabei ließt der Automat über einen Lesekopf die Eingabe vom Eingabeband und wechselt entsprechend der Übergangsfunktion zwischen den Zuständen. Tritt der Automat in einen Endzustand, so wird dies hier durch ein Signal vermerkt.