Institut für Formale Methoden der Informatik
Universität Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

Diplomarbeit Nr. 3332

Die Holonomie–Zerlegung von Automaten

Martin P. Seybold

Studiengang:	Informatik
Prüfer:	Prof. Dr. V. Diekert
Betreuer:	Dr. M. Kufleitner
begonnen am:	14.02.2012
beendet am:	15.08.2012
CR-Klassifikation:	F4.3

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Diese Diplomarbeit beschäftigt sich mit einer intuitiven, aber trotzdem möglichst kompakten Darstellung der Holonomie–Zerlegung von Automaten, die ausschließlich elementare Mittel nutzt. Durch die Formulierung des Problems als Graph konnten bisherige Beweise vereinfacht werden, sodass nur noch Überdeckungen, statt relationalen Überdeckungen, benötigt werden. Neu ist, dass der hier gegebene Beweis sogar konstruktiv statt induktiv ist. Die graphentheoretische Formulierung ermöglicht eine einfache Abschätzung der Faktorzahl einer vollständigen, sogenannten Krohn–Rhodes–Zerlegung.

Endliche Automaten und die damit beschriebenen regulären Sprachen sind Standardwerkzeuge der Informatik. Sie sind ein allgemeines Modell für die strukturierte Abarbeitung von Benutzereingaben. Die bekanntesten Anwendungen sind Fahrkartenautomaten, die Suche von Mustern in Texten oder Bestellprozesse. Aber auch biologische Stoffwechselvorgänge versucht man mit Hilfe von endlichen Automaten zu formalisieren[6][5]. Für die theoretische Beschreibung eines realen Computers wird pragmatischerweise oft ein anderes Maschinenmodell, wie etwa eine Turingmaschine, herangezogen. Jedoch kommt ein endlicher Automat, der potentiell sehr groß sein kann, einem realen Computer sehr nahe, denn der Speicher ist inhärent endlich. Die mathematisch grundlegende Beschreibung endlicher Automaten ist gegeben durch Halbgruppen[9]. Um die Struktur und damit die Komplexität einer solchen Maschine besser zu verstehen bietet sich das Studium von Halbgruppen und deren hierarchische Zerlegungen an.

In gleicher Weise wie sich eine natürliche Zahl in ein Produkt von Primzahlen zerlegen lässt, kann man Ähnliches für eine Halbgruppe erreichen. Dieses fundamentale Resultat der Theorie über endliche Halbgruppen ist als Krohn–Rhodes–Zerlegung bekannt. Demnach kann jede Halbgruppe in ein Produkt von einfachen, nicht weiter zerlegbaren Gruppen und Flip–Flops zerlegt werden. Flip–Flops sind drei–elementige Monoide, deren Elemente alle idempotent sind.

Es gibt eine Vielzahl an Theoremen und unterschiedlichen Beweisen, die dieses Resultat implizieren. Die Holonomie–Zerlegung ist seither das Theorem, welches eine Krohn–Rhodes–Zerlegung mit der kleinsten Anzahl an Faktoren erreicht. Sie ist sogar so effizient, dass Implementierungen vorliegen und praktische Probleme damit untersucht werden[2][6][5].

Nach der ursprünglichen Beweisidee von Zeiger ist nun die Version von Eilenberg die allgemeine Arbeitsgrundlage[3, p.33-57] vieler Autoren. Jedoch wird die algebraische Notation und die im Beweis benutzten Methoden beklagt[2][8]. Diese Diplomarbeit liefert eine kompakte algebraische Darstellung der Holonomie–Zerlegung, die mit einfachen Mitteln auskommt.

2 Grundlagen

Alle Funktionen, die in dieser Arbeit angegeben werden, sind total. Außerdem sind alle Mengen endlich und mit großen, lateinischen Buchstaben bezeichnet, wohingegen Elemente mit kleinen Buchstaben bezeichnet werden. Außerdem wird vorausgesetzt, dass der Leser vertraut mit endlichen Automaten und den Syntaktischen–Halbgruppen ist, die solchen Automaten haben. Der endliche Automat in Abbildung 2 definiert die Sprache $L = (a|b)^*(aa|bb)(a|b)^*$ über dem Alphabet $\{\, a, b \,\}$. Für alle Beispiele dieser Arbeit werden wir diesen Automaten zugrunde legen. Die Syntaktische–Halbgruppe der Sprache L ist gegeben durch

$$Synt^+(L) = \{s_1 = [4,4,4,4], s_2 = [3,4,3,4], s_3 = [2,2,4,4],$$
$$s_4 = [2,4,2,4], s_5 = [3,3,4,4]\}$$

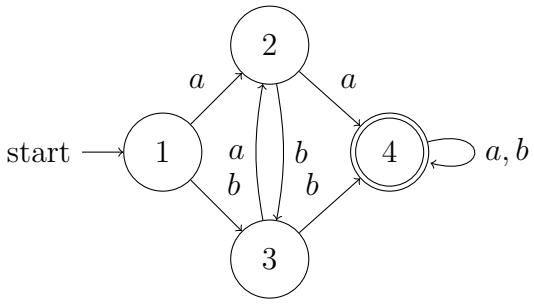

Abbildung 2.1: Endlicher Automat der Sprache $L = (a|b)^*(aa|bb)(a|b)^*$.

Definition 2.1: (X, S) heißt *Transformations–Halbgruppe*, falls X eine nicht leere Menge, die sogenannte Zustandsmenge, und S eine Halbgruppe ist. Außerdem existiert eine *rechts–Wirkung* $\alpha : X \times S \to X$ beschrieben durch $(x, s) \mapsto x \cdot s$, welche $x \cdot (s_1 s_2) = (x \cdot s_1) \cdot s_2$ erfüllt. Die rechts–Wirkung, und dadurch die Transformations–Halbgruppe, heißt *treu*, falls für $s_1 \neq s_2$ ein $x \in X$ existiert mit $x \cdot s_1 \neq x \cdot s_2$. Außerdem heißt (X, S) *Transformations–Monoid*, falls S ein Monoid ist und $x \cdot 1 = x$ für alle $x \in X$. Weiter heißt (X, S) *Transformations–Gruppe*, falls S zusätzlich eine Gruppe ist.

Im Folgenden bezeichnen wir mit "$\cdot$" die rechts–Wirkung und mit dem leeren Operator "" die Halbgruppen Operation. Ein Beispiel für eine treue Transformations–Halbgruppe ist $(S \cup \{\, 1 \,\}, S)$, wobei die rechts–Wirkung gleich der erweiterten Halbgruppen Operation ist.

Definition 2.2: Das *Kranzprodukt* von Transformations–Halbgruppen ist $(X_1, S_1) \wr \ldots \wr (X_n, S_n) = (X, W)$, wobei $X = \prod_{i=1}^{n} X_i$ und $W = \prod_{i=1}^{n} S_i^{X_{i+1} \times \ldots \times X_n}$. Wegen $(S_1^{X_2})^{X_3} = S_1^{(X_2, X_3)}$ ist das Produkt in der Tat assoziativ. Wir definieren nun erst die rechts–Wirkung und finden anschließend eine kompatible Halbgruppen Operation auf W. Wir betrachten das Ergebnis von zwei Funktionen $f = (f_1, \ldots, f_n), g = (g_1, \ldots, g_n) \in W$ auf $x = (x_1, \ldots, x_n) \in X$:

$$
\begin{aligned}
(x \cdot f) \cdot g &= \begin{pmatrix} x_1 \cdot f_1(x_2, \ldots, x_n) \\ \vdots \\ x_n \cdot f_n() \end{pmatrix} \cdot g \\
&= \begin{pmatrix} \Big(x_1 \cdot f_1(x_2, \ldots, x_n)\Big) & \cdot & g_1(x_1 \cdot f_1(x_2, \ldots, x_n)\ ,\ \ldots\ ,\ x_n \cdot f_n()) \\ & \vdots & \\ \Big(x_n \cdot f_n()\Big) & \cdot & g_n() \end{pmatrix} \\
&= \begin{pmatrix} x_1 & \cdot & \Big[\ f_1\Big(x_2, \ldots, x_n\Big)\ g_1\Big(x_1 \cdot f_1(x_2, \ldots, x_n)\ ,\ \ldots\ ,\ x_n \cdot f_n()\Big)\ \Big] \\ & \vdots & \\ x_n & \cdot & \Big[f_n()\ g_n()\Big] \end{pmatrix}
\end{aligned}
$$

Da die eckige Klammer von Komponente i nur von Zuständen x_j mit höherem Index $j > i$ abhängt, ist sie eine Funktion $h_i \in S_i^{X_{i+1} \times \ldots \times X_n}$. Damit definiert $fg = h$ eine abgeschlossene Operation auf W, die außerdem assoziativ ist, da die Halbgruppe der jeweiligen Komponente bereits assoziativ war. Außerdem zeigt die Rechnung die Treue von (X, W), falls jeder der Faktoren treu war.

An dieser Definition lässt sich auch die enge Verbindung des Kranzprodukts zu einem Maschinenmodell sehen, welches nach jedem parallelen Rechenschritt eine begrenzte Menge an Information austauscht.

2.1 Teiler und Überdeckungen

Die Definitionen und Beweise der folgenden Unterkapitel sind der Darstellung in [1] nachempfunden.

Definition 2.3: Eine Halbgruppe S *teilt* eine Halbgruppe T, bezeichnet durch $S \prec T$, falls eine Unterhalbgruppe $T' \subseteq T$ sowie ein surjektiver Homomorphismus $\psi : T' \to S$ existiert.

Diese Definition lässt sich auf natürliche Weise auf Transformations–Halbgruppen erweitern.

Definition 2.4: Eine Transformations–Halbgruppe (X, S) *teilt (stark)* eine Transformations–Halbgruppe (Y, T), bezeichnet durch $(X, S) \prec (Y, T)$, falls es eine Unterhalbgruppe

$T' \subseteq T$, einen surjektiven Morphismus $\varphi : Y \to X$ und einen surjektiven Homomorphismus $\psi : T' \to S$ gibt so, dass

$$\varphi(y \cdot t) = \varphi(y) \cdot \psi(t)$$

für alle $y \in Y$ und $t \in T'$ gilt.

Die Relation Teilbarkeit ist transitiv durch Verkettung der Morphismen. Da der Nachweis von Homomorphismen nicht immer leicht ist, hat sich die Methode der Überdeckung als sehr hilfreich erwiesen [1][3].

Definition 2.5: Seien (X, S), (Y, T) beliebige, möglicherweise nicht treue, Transformations–Halbgruppen und $\varphi : Y \to X$ eine beliebige Surjektion. Wir nennen ein Element $\widehat{s} \in T$ ein *Cover* von $s \in S$, falls für alle $y \in Y$ gilt:

$$\varphi(y) \cdot s = \varphi(y \cdot \widehat{s})$$

Falls jedes Element $s \in S$ mindestens ein Cover besitzt nennen wir φ eine *Überdeckung* und schreiben $(X, S) \prec_\varphi (Y, T)$.

Der Formalismus von Teilbarkeit und Überdeckung ist eng verbunden. Das folgende Lemma zeigt wie Überdeckungen bequem Beweise von Teilbarkeit ermöglichen.

Lemma 2.1: *Seien (X, S), (Y, T) Transformations–Halbgruppen. Falls (X, S) treu ist impliziert $(X, S) \prec_\varphi (Y, T)$ bereits $(X, S) \prec (Y, T)$.*

Beweis: Betrachte $S_\varphi = \{ (s, \hat{s}) \} \subseteq S \times T$. Wir definieren eine Operation auf dieser Menge durch $(s_1, \widehat{s_1})(s_2, \widehat{s_2}) = (s_1 s_2, \widehat{s_1 s_2})$. Da die zweite Komponente durch das Ergebnis der Ersten bestimmt wird, haben wir tatsächlich eine Halbgruppe. Falls wir eine Unterhalbgruppe $R_\varphi \subseteq S_\varphi$ finden, wobei die Projektion auf die erste Komponente $\pi_1(R_\varphi)$ surjektiv bleibt und $\pi_2(R_\varphi)$ injektiv ist, haben wir auch einen surjektiven Homomorphismus $\pi_2(R_\varphi) \to \pi_1(R_\varphi) = S$ gefunden. Angenommen $(s_1, t), (s_2, t)$ sind Elemente von S_φ. Da φ surjektiv ist erhalten wir für $s_1 \neq s_2$ aus der Treue $x \cdot s_1 = \varphi(y) \cdot s_1 = \varphi(y \cdot t) \neq x \cdot s_2 = \varphi(y \cdot t)$. Daher ist $S_\varphi = R_\varphi$ bereits so eine Unterhalbgruppe und wir haben einen surjektiven Homomorphismus gefunden. □

2.2 Konstanten

Definition 2.6: Sei (X, S) eine Transformations–Halbgruppe, wir definieren den *Abschluss unter Konstanten* als:

$$\overline{(X, S)} = (X, S \cup \overline{X})$$

wobei $\overline{X} = \{ \bar{x} \mid x \in X \}$. Durch Erweitern der rechts–Wirkung mit $y \cdot \bar{x} = x$ für alle $x, y \in X$ und der Halbgruppen Operation mit $s\bar{x} = \bar{x}$ und $\bar{x}s = \overline{x \cdot s}$ für jedes $s \in S, \bar{x} \in \overline{X}$, erhalten wir in der Tat eine Transformations–Halbgruppe.

Lemma 2.2: *Sei (X, G) eine treue Transformations–Gruppe, dann haben wir die Division $\overline{(X,G)} \prec (X, U_X) \wr (G, G)$, wobei das Monoid $U_X = \overline{X} \cup \{ 1 \}$ ist.*

Beweis: Sei $\varphi(x, g) = x \cdot g$ und wir setzen $cover : G \cup \overline{X} \to {U_X}^G \times G$ wie folgt:

$$cover_1(y,h) = \begin{cases} 1 & \text{, falls } y \in G \\ \overline{y \cdot h^{-1}} & \text{, falls } y \in \overline{X} \end{cases} \qquad cover_2(y) = \begin{cases} y & \text{, falls } y \in G \\ 1 & \text{, falls } y \in \overline{X} \end{cases}$$

Es gilt für alle $(x, g) \in X \times G$

$$\begin{aligned} &\varphi((x,g) \cdot cover(y)) = \varphi((x,g) \cdot (1,y)) = \varphi(x, gy) = \varphi(x,g) \cdot y && y \in G \\ &\varphi((x,g) \cdot cover(y)) = \varphi(x \cdot \overline{y \cdot g^{-1}}, g \cdot 1)) = \varphi(y \cdot g^{-1}, g) = y = \varphi(x,g) \cdot y && y \in \overline{X} \end{aligned}$$

□

Das treue Transformations–Monoid (X, U_X) lässt sich, ähnlich einer binären Repräsentation, weiter in ein Produkt der kleineren Monoide U_2 mit nur drei idempotenten Elementen ($m^2 = m$) zerlegen.

Lemma 2.3: *Sei $n > 2$ und $i = \lceil log_2(n) \rceil$. Es gelten:*

$$\begin{aligned} (\{ x_0, \ldots, x_{n-1} \}, U_n) &\prec (\{ x_0, \ldots, x_{2^i-1} \}, U_{2^i}) \\ (\{ x_0, \ldots, x_{2^i-1} \}, U_{2^i}) &\prec (\{ x_0, \ldots, x_{2^{i-1}-1} \}, U_{2^{i-1}}) \times (\{ x_0, x_1 \}, U_2) \end{aligned}$$

Beweis: Die Transformations–Monoide sind treu. Für die erste Division sei $\varphi(x_k) = x_{(k \mod n)}$ und da $U_n \subseteq U_{2^i}$ können wir die Cover identisch wählen und es gilt für $l \leq n - 1$:

$$\varphi(x_k \cdot cover(\overline{x_l})) = \varphi(x_k \cdot \overline{x_l}) = x_l = \varphi(x_k) \cdot \overline{x_l}.$$

Für die zweite Division sei $\varphi(x_k, x_l) = x_{(2k+l)}$. Wir geben ein Cover in der Form $cover : U_{2^i} \to U_{2^{i-1}} \times U_2$ an:

$$cover(y) = \begin{cases} (1,1) & \text{, falls } y = 1 \\ (\overline{x_{k/2}}, \overline{x_{(k \mod 2)}}) & \text{, falls } y = \overline{x_k} \end{cases}$$

Es gilt:

$$\begin{aligned} \varphi((x_k, x_l) \cdot cover(\overline{x_m})) &= \varphi((x_k, x_l) \cdot (\overline{x_{m/2}}, \overline{x_{(m \mod 2)}})) \\ &= \varphi(x_{m/2}, x_{(m \mod 2)}) = x_{(m/2)2+(m \mod 2)} = x_m \\ &= \varphi(x_k, x_l) \cdot \overline{x_m}. \end{aligned}$$

□

2.3 Zerlegungen von Gruppen

Lemma 2.4: *Falls N Normalteiler in G ist, gilt die Division*

$$(G, G) \prec (N, N) \wr (G/N, G/N).$$

Beweis: Wir identifizieren die Faktormengen durch die fixierten Repräsentanten $G/N = \{ h_1, \ldots, h_n \}$ wobei $h_i \in G$. Sei $\varphi(n, h_i) = nh_i$ und $cover : G \to N^{G/N} \times G/N$

$$cover_1(g, h) = hg[hg]^{-1} \qquad cover_2(g) = [g]$$

Und wir rechnen nach:

$$\begin{aligned} \varphi((n, h) \cdot cover(g)) &= \varphi(n \cdot hg[hg]^{-1}, h \cdot [g]) = \varphi(nhg[hg]^{-1}, [hg]) \\ &= nhg = \varphi(n, h) \cdot g \end{aligned}$$

□

Definition 2.7: Eine Gruppe G heißt *einfach*, falls jeder Normalteiler N in G entweder trivial $N = \{ 1 \}$ oder ganz $N = G$ ist.

Korollar 2.5: *Für jede endliche Gruppe G haben wir die Division*

$$(G, G) \prec (G_1, G_1) \wr \ldots \wr (G_m, G_m)$$

wobei in jedem Faktor G_i eine einfache Gruppe steht und $|G_1| \cdot \ldots \cdot |G_m| = |G|$ mit $m \leq \lceil log_2(|G|) \rceil$.

Beweis: Falls G nicht einfach ist existiert ein Normalteiler $\{ 1 \} \subsetneq N \subsetneq G$. Außerdem ist die Faktorgruppe G/N nicht trivial und echt kleiner als G. Durch Induktion mit Lemma 2.4 folgt die Behauptung. □

3 Die Holonomie–Zerlegung

3.1 Der Inklusionsgraph einer Transformations–Halbgruppe

Definition 3.1: Jede Transformations–Halbgruppe (X, S) induziert einen verbundenen, gerichteten azyklischen Graph $\mathcal{G}_{(X,S)} = (V, E)$ durch ihre rechts–Wirkung, mit

$$V = \{ X \cdot s \mid s \in S \} \cup X \cup \{ X \}$$
$$E = \{ (A, B) \mid A \supsetneq B \text{ und } \nexists C \in V : A \supsetneq C \supsetneq B \}.$$

Im Fall der Transformations–Halbgruppe $(S \cup \{ 1 \}, S)$ sind die Green'schen $\mathcal{L}$–Faktormengen die Knoten dieses Graphes.

Lemma 3.1: *Für jeden inneren Knoten $A \in V \setminus X$ gilt $A = \bigcup_{(A,B)\in E} B$. Außerdem ist die Holonomie–Gruppe*

$$G_A = \{ s' : A \to A \mid \exists s \in S : A \cdot s = A \text{ und } \forall x \in A : x \cdot s = x \cdot s' \}$$

entweder leer oder (E_A, G_A) ist eine treue Transformations–Gruppe, wobei $E_A = \{ (B, C) \in E \mid B = A \}$.

Beweis: Ein Element $g \in G_A \neq \emptyset$ ist eine lokale Permutation auf A und es gibt einen Exponenten $i \geq 1$ der g^i zur identischen Transformation $g^i = 1_A \in G_A$ auf A macht. Insbesondere existiert ein inverses Element g^{-1} und G_A ist eine Gruppe. Die rechts–Wirkung eines $g \in G_A$ lässt sich in natürlicher Weise auf die Kanten E_A erweitern, durch $(A, B) \cdot g = (A \cdot g = A, B \cdot g)$. In der Tat definiert dies eine Kante in E_A. Es gilt $|B| = |B \cdot g|$ und $B \cdot g \subsetneq A$. Angenommen $(A, C) \in E_A$ mit $C \subsetneq B \cdot g$. Betrachte $A \supsetneq C \cdot g^{-1} \supsetneq B$, was die Maximalität von B zum Widerspruch führt. Dadurch ist $(A, B \cdot g) \in E_A$. Diese rechts–Wirkung ist assoziativ, da sie es bereits auf (X, S) war. Außerdem ist sie treu, da G_A keine zwei identischen Transformationen enthält. □

Definition 3.2: Wir definieren die Relation $\mathcal{R}$ auf den Knoten durch

$$\mathcal{R} = \{ (A, B) \in V \times V \mid \exists a, b \in S \cup \{ 1 \} : A \cdot a = B \text{ and } B \cdot b = A \}$$

Da wir Reflexivität, Symmetrie und Transitivität haben, ist $\mathcal{R}$ eine Äquivalenzrelation.

Lemma 3.2: *Sei (X, S) eine Transformations–Halbgruppe. Falls $(X \cdot s)\mathcal{R}(X \cdot s')$ dann ist $(E_{X\cdot s}, G_{X\cdot s}) \cong (E_{X\cdot s'}, G_{X\cdot s'})$.*

Beweis: Bezeichne $A = X \cdot s$ und $B = X \cdot s'$ die beiden Knoten in $\mathcal{G}_{(X,S)}$.
"$\prec$": Wegen $A = A \cdot ab$ ist ab eine lokale Permutation auf A. Wir haben $|A| = |B|$ und es gibt eine natürliche Zahl $i \geq 1$ mit $x \cdot (ab)^i = x$ für jedes $x \in A$. Sei $a^- = b(ab)^{i-1}$, $\varphi : E_B \to E_A$ mit $(B, C) \mapsto (B, C) \cdot a^- = (B \cdot a^- = A, C \cdot a^-)$. Wir finden ein Cover für jedes $g \in G_A$ beschrieben durch $cover(g) = a^- g a \in G_B$. Für eine beliebige Kante $e \in E_B$ gilt $\varphi(e \cdot cover(g)) = \varphi(e \cdot a^- g a) = (e \cdot a^- g) \cdot aa^- = e \cdot a^- g = \varphi(e) \cdot g$. Durch die Treue von (E_A, G_A) folgt die Teilbarkeit.
"$\succ$" lässt sich symmetrisch zeigen. □

Abgesehen von $|A| = |B|$ haben wir also eine Bijektion der Kanten von E_A und E_B der Knoten mit $A \mathcal{R} B$ und die Äquivalenzrelation $\mathcal{R}$ lässt sich auf natürliche Weise auf alle Kanten von $\mathcal{G}_{(X,S)}$ erweitern, da Kanten nur einen Vater–Knoten haben. Obige Verkettung von lokalen Transformationen ist die Motivation für den Namen Holonomie–Zerlegung.

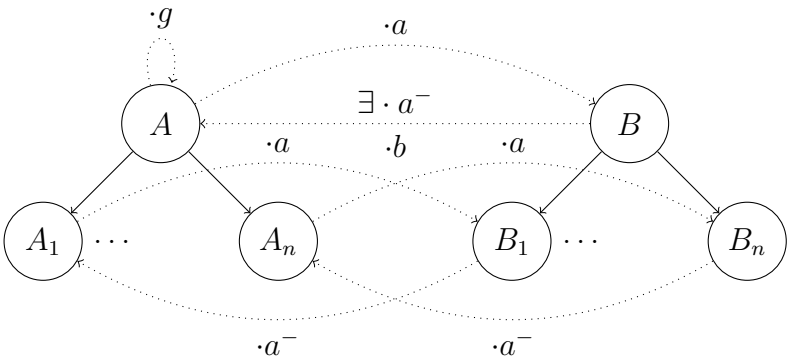

Abbildung 3.1: Bijektion zwischen Kanten E_A und E_B zweier Knoten mit $A \mathcal{R} B$.

Lemma 3.3: *Die Äquivalenzrelation $\mathcal{R}$ partitioniert die inneren Knoten von $\mathcal{G}_{(X,S)}$ in $V = X \dot\cup [X_1] \dot\cup \ldots \dot\cup [X_n]$ und die Kanten $E = [E_{X_1}] \dot\cup \ldots \dot\cup [E_{X_n}]$ mit $n \leq |S| + 1$. Weiter gibt es eine lineare Ordnung dieser Partitionen welche für alle $s \in S$ Beides*

$$\begin{aligned} |X_i| < |X_j| &\Rightarrow i < j \\ A \in [X_j] \text{ und } A \cdot s \in [X_i] &\Rightarrow i \leq j \end{aligned}$$

erfüllt.

Beweis: Die Repräsentanten X_i sein beliebig, aber von nun an fest. $X_n = X$ bezeichnet stets den maximalen Knoten im Graph. Durch Lemma 3.2 überträgt sich die Partition direkt auf die Kanten.

Wir sortieren die Klassen der Knoten topologisch, wobei wir zusätzlich zu den Kanten des Inklusionsgraph $\mathcal{G}_{(X,S)}$ auch Kanten der Form

$$E_S = \left\{ (A, B) \in V^2 \;\middle|\; \exists s \in S : A \cdot s = B \right\}$$

berücksichtigen. Da $|A \cdot s| \leq |A|$ existieren keine Kreise außerhalb einer Klasse. Für $A \in [X_i]$ und $B \in [X_j]$ mit $[X_i] \neq [X_j]$ existiert maximal eine Kante $(A, B) \in E_S$, da sonst $A \mathcal{R} B$. □

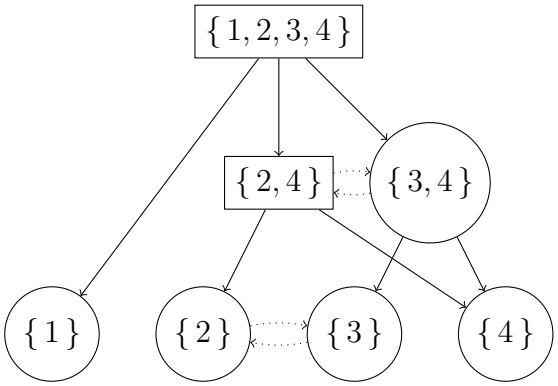

Abbildung 3.2: Inklusionsgraph der Beispielsprache von Kapitel 2. Die gewählten Repräsentanten sind als Rechtecke, übrigen Knoten als Kreise, Kanten als durchgezogene Pfeile und $\mathcal{R}$–Zusammenhänge als gepunktete Pfeile gezeichnet.

Lemma 3.4: *Es existieren eine injektive Abbildung c von Pfaden zu Kanten–Repräsentanten und eine inverse Abbildung d, welche für jeden Pfad $p_A = e_1 \dots e_l$ von $X = source(e_l)$ nach $A = target(e_1)$ Folgendes erfüllen:*

$$d(c(p_A)) = p_A.$$

Insbesondere existiert eine Abbildung von Suffixen zu Knoten $decode : E_{X_i} \times \dots \times E_{X_n} \to V$, die für alle Suffixe bis i Folgendes erfüllt:

$$decode(\gamma_{i+1} \dots \gamma_n) \in [X_j] \;\Rightarrow\; j \leq i.$$

Beweis: Sei $p_A = e_1 \dots e_l$ ein Pfad der $target(e_1) = A \in [X_i]$ mit dem maximalen Knoten $source(e_l) = X = X_n$ verbindet. Die Funktion c bildet jede Kante auf die Kante des Repräsentanten ab, wobei unbenutzte Klassen beliebig gewählt werden. Genauer, falls $[E_{X_k}]$ eine Kante e_j enthält, haben wir $source(e_j) = X_k \cdot a$ und wählen das Bild $\gamma_k = e_j \cdot a^-$. Anderenfalls wählen wir γ_k beliebig.

$$c : e_1 \dots e_l \mapsto \gamma_{i+1} \dots \gamma_n$$

Sei die Funktion $target$ nun auf Pfade erweitert. Wir definieren die Funktion d induktiv auf Suffixen:

$$d(\gamma_i \dots \gamma_n) = \begin{cases} \gamma_n & , \text{falls } i = n \\ (\gamma_i \cdot a)\ d(\gamma_{i+1} \dots \gamma_n) & , \text{falls } target(d(\gamma_{i+1} \dots \gamma_n)) = X_i \cdot a \\ d(\gamma_{i+1} \dots \gamma_n) & , \text{sonst} \end{cases}$$

Da p_A zusammenhängend war, liefert eine Induktion über die Suffixlänge den identischen, verbundenen Pfad. Der mittlere Fall in der Abbildung d stellt die Verbindung zwischen ausgewerteten Suffixen mit steigender Länge sicher.

Und wir definieren die Abbildung $decode(\gamma_i \dots \gamma_n) = target(d(\gamma_i \dots \gamma_n))$ und es gilt:

$$decode(c(p_A)) = A.$$

□

Beispiel 3.1
Wir betrachten obigen Inklusionsgraph. Durch $\mathcal{R}$ haben wir die folgende Partition und wählen Repräsentanten X_i.

$$\begin{aligned} V &= \{\{4\},\{2\},\{3\},\{1\}\} \dot\cup \{\{2,4\},\{3,4\}\} \dot\cup \{\{1,2,3,4\}\} \\ X_1 &= \{2,4\} \\ X_2 &= \{1,2,3,4\} \end{aligned}$$

Wir codieren nun den Pfad $p_{\{3\}} = (34,3)(1234,34)$. Es gilt $\{3,4\} = X_1 \cdot s_5$ und $X_1 = \{3,4\} \cdot s_4$. Außerdem ist $s_5^- = s_4$ und wir erhalten relativ zu den Repräsentanten den Pfadcode

$$c(p_{\{3\}}) = ((34,4) \cdot s_5^-)(1234,34) = (24,2)(1234,34) = \gamma$$

Wir berechnen nun $d(\gamma)$. Da $target(d(\gamma_2)) = \{3,4\} = X_1 \cdot s_5$ erhalten wir

$$d(\gamma) = ((24,2) \cdot s_5)(1234,34) = (34,3)(1234,34)$$

Und $decode(\gamma) = \{3\}$.

3.2 Varianten der Holonomie–Zerlegung

Die Hauptidee um Zerlegungen von rechts–Wirkungen in dieser Anschauung zu beweisen ist Mikrokomponenten, wie (E_A, G_A), und ihre Isomorphien "$\approx$" zu benutzen. Ähnlich wie bei Weichen in einem Schienennetz wird durch lokale Manipulationen ein Pfad mit Ziel $x \cdot s$ generiert.

Satz 3.5 (Holonomie–Zerlegung[10])**:** *Sei (X,S) eine Transformations–Halbgruppe, dann gilt*

$$(X,S) \prec_\varphi \overline{(E_{X_1}, G_{X_1})} \wr \dots \wr \overline{(E_{X_n}, G_{X_n})} \ ,$$

wobei alle $n \leq |S|+1$ Faktoren treu sind. Jeder Gruppenfaktor ist entweder leer $G_{X_i} = \emptyset$ oder eine Untergruppe $G_{X_i} \subseteq S$. Letzterenfalls ist (E_{X_i}, G_{X_i}) eine Transformations–Gruppe.

Das Hauptresultat dieser Arbeit ist der folgende Beweis.

Beweis: Sei $\mathcal{G}_{(X,S)} = (V,E)$ und E_{X_i} , die Kanten von Repräsentant i, angeordnet wie in Lemma 3.3 beschrieben. Nach Lemma 3.4 ist $\varphi = decode$ eine Surjektion von

$\prod_{i=1}^{n} E_{X_i}$ nach X. Für den Beweis genügt es ein Cover anzugeben, welches einen Pfad von X nach x zu einem Pfad von X nach $x \cdot s$ für ein gegebenes $s \in S$ transformiert.

Seien $x = A_1 \subsetneq \ldots \subsetneq A_{l+1} = X$ die Knoten solch eines gegebenen Pfades $p = e_1 \ldots e_l$. Anstatt nun einen beliebigen Pfad nach $x \cdot s$ zu erhalten, wird dieser Beweis einen eindeutigen Pfad rekonstruieren, der zumindest alle Bilder $x \cdot s = A_1 \cdot s \subseteq \ldots \subseteq A_{l+1} \cdot s \subseteq X$ enthält. Wir fixieren nun für jedes Paar von Knoten $C, D \in V$ mit $C \supsetneq D$ unabhängig von s oder p exakt einen, jedoch beliebigen, verbindenden Pfad. Dadurch ist der zu rekonstruierende Pfad $p' = e'_1 \ldots e'_m$ mit Ziel $x \cdot s$ eindeutig.

Durch die Abbildung $cover : S \to \prod_{i=1}^{n} \left\{ \overline{E_{X_i}} \cup G_{X_i} \right\}^{E_{X_{i+1}} \times \ldots \times E_{X_n}}$ wird für jedes $s \in S$ ein Cover angegeben. Wir definieren die Abbildung *cover* komponentenweise und bezeichnen abkürzend mit $A = decode(\gamma_{i+1} \ldots \gamma_m)$, wobei $\gamma_i \in E_{X_i}$, den bis i kleinsten Knoten des ursprünglichen Pfades und mit $p'|_{A \cdot s}$ den Suffix von p' bis Knoten $A \cdot s$.

$$cover_i(s, (\gamma_{i+1} \ldots \gamma_m)) = \begin{cases} \alpha_1 s \alpha_2^- & , \text{ falls } A = X_i \cdot \alpha_1 \text{ und } A \cdot s = X_i \cdot \alpha_2 \\ \overline{(C, D) \cdot \alpha^-} & , \text{ falls } [E_{X_i}] \cap p'|_{A \cdot s} = (C, D) \text{ mit } C = X_i \cdot \alpha \\ \text{beliebig} & , \text{ sonst} \end{cases}$$

Da p' ein Pfad ist, enthält jede Äquivalenzklasse $[E_{X_i}]$ maximal eine zu belegende Kante. Wir zeigen nun, dass nach dem Update genau diese belegt wird. Noch immer sei $A = decode(\gamma_{i+1} \ldots \gamma_n)$ und j durch $A \cdot s \in [X_j]$ gegeben. Durch die Anordnung der Repräsentanten (Lemma 3.3) haben wir zwei Fälle:

- $j = i$: Damit gilt $A = X_i \cdot \alpha_1$ und $A \cdot s = X_i \cdot \alpha_2$ und s wirkt als Kanten–Bijektion in $[E_{X_i}]$. Es gilt $e = (A, C) \in p \;\Rightarrow\; (A \cdot s, C \cdot s) = e' \in p'$ und es folgt:

$$\begin{aligned} \gamma_i &= \gamma_i \cdot cover_i(s, (\gamma_{i+1} \ldots \gamma_n)) \\ &= \gamma_i \cdot \alpha_1 s \alpha_2^- \\ &= (e \cdot \alpha_1^-) \cdot \alpha_1 s \alpha_2^- \\ &= (e \cdot s) \cdot \alpha_2^- = e' \cdot \alpha_2^- \end{aligned}$$

- $j < i$: Durch die Eindeutigkeit enthält $[E_{X_i}]$ maximal eine Kante $(C, D) = e' \in p'$. Wir haben $C = X_i \cdot \alpha$ und es folgt:

$$\begin{aligned} \gamma'_i &= \gamma_i \cdot cover_i(s, (\gamma_{i+1} \ldots \gamma_n)) \\ &= \gamma_i \cdot \overline{(C, D) \cdot \alpha^-} = e' \cdot \alpha^- \end{aligned}$$

Da jede notwendige Klasse den Code der jeweiligen Kante von p' belegt, ist $\varphi = decode$ eine Überdeckung. □

Wir wollen dies nun mit dem Beweis von Eilenberg[3, p.33-57] vergleichen, der Grundlage für unseren Beweis ist. Hierin wird eine, zu Beginn triviale, relationale Überdeckung φ und Cover, zusammen induktiv verfeinert bis diese eine Überdeckung sind. In unserer Notation lässt sich der Prozess entkoppelt darstellen. Die Funktion *decode* stimmt

mit der verfeinerten Relation φ überein, jedoch drückt sich das dort generierte Cover in unserer Notation wie folgt aus:

$$cover_i(s,(\gamma_{i+1}\dots\gamma_m)) = \begin{cases} \alpha_1 s \alpha_2^- & \text{, falls } A = X_i\cdot\alpha_1 \text{ und } A\cdot s = X_i\cdot\alpha_2 \\ \overline{(C,D)\cdot\alpha^-} & \text{, falls } \exists j > i: \\ & decode(\gamma|_j \cdot cover(s,(\gamma_{j+1}\dots\gamma_n))) = C \\ & \text{mit } C = X_i\cdot\alpha \\ & \text{und } (C,D)\in[E_{X_i}] \text{ beliebig mit } D \supseteq A\cdot s \\ \text{beliebig} & \text{, sonst} \end{cases}$$

Durch die beliebige Wahl und anschließende sukzessive Rekonstruktion der Ergebnisse mit höherem Index wird dort ein beliebiger Pfad mit Ziel $x\cdot s$ als Ergebnis von $\gamma\cdot cover(s)$ erzeugt.

Zusammen mit den grundlegenden Zerlegungen von Konstanten und Gruppen aus Kapitel 2 impliziert das Holonomie–Theorem 3.5 bereits die Krohn–Rhodes Zerlegung. Durch den Inklusionsgraph ist die Abschätzung für die Anzahl der Faktoren besonders leicht.

Korollar 3.6 (Krohn/Rhodes[7])**:** *Jede treue Transformations–Halbgruppe (X,S) teilt ein Kranzprodukt der Form*

$$(X_1,M_1)\wr\dots\wr(X_n,M_n)$$

wobei jeder der n Faktoren (X_i,M_i) entweder gleich $(\{x_0,x_1\},U_2)$ oder gleich (G,G) ist, und G ist eine nicht–triviale einfache Gruppe, die S teilt. Außerdem ist die Anzahl der Faktoren durch $n < c\ |S|\ log_2(|S|+|X|)$ beschränkt.

Beweis: Wir nutzen die Transitivität von Überdeckungen $\prec_\varphi$ um die Faktoren $\overline{(E_A,G_A)}$ die in der Holonomie–Zerlegung vorkommen weiter zu vereinfachen. Durch Lemma 2.2 und die Treue eines solchen Faktors haben wir $\overline{(E_A,G_A)} \prec (E_A,U_{E_A})\wr(G_A,G_A)$. Außerdem lässt sich der Konstanten–Faktor mit Lemma 2.3 in ein direktes Produkt von $\lceil log_2(|E_A|)\rceil$ Faktoren der Form $(\{x_0,x_1\},U_2)$ zerlegen, was ein Spezialfall des Kranzprodukts ist. Durch Korollar 2.5 teilt der Gruppen–Faktor ein Produkt $(G_1,G_1)\wr\dots\wr(G_m,G_m)$, wobei $m \le \lceil log_2(|G_A|)\rceil$ und alle G_i sind einfach und teilen G_A. Für n erhalten wir die folgende Abschätzung:

$$\begin{aligned} n &\le \sum_{i=1}^{|S|+1} \lceil log_2(|E_{X_i}|)\rceil + \lceil log_2(|G_{X_i}|)\rceil \\ &\le \sum_{i=1}^{|S|+1} \lceil log_2(|E|)\rceil + \lceil log_2(|S|)\rceil \end{aligned}$$

$$
\begin{aligned}
&\leq (|S|+1)\Big(2 + log_2(|E|) + log_2(|S|)\Big) \\
&\leq (|S|+1)\Big(2 + log_2\big((|S|+1)(|S|+|X|)\big) + log_2(|S|)\Big) \\
&\leq (|S|+1)\Big(2 + log_2(|S|+1) + log_2(|S|+|X|) + log_2(|S|)\Big) \\
&\leq c\ |S|\ log_2(|S|+|X|).
\end{aligned}
$$

□

3.3 Beispiel einer Zerlegung

Wir geben hier eine Holonomie–Zerlegung an. Die Transformations–Halbgruppe $(X,S) = (\{\,1,2,3,4\,\}, Synt^+(L))$ unserer Beispielsprache $L = (a|b)^*(aa|bb)(a|b)^*$ von Kapitel 2 teilt folglich ein Produkt von

$$
\begin{aligned}
(X,S) &\prec \overline{(E_{X_1}, G_{X_1})} \wr \overline{(E_{X_2}, G_{X_2})} \qquad \text{mit} \\
G_{X_2} \cup \overline{E_{X_2}} &= \emptyset \cup \Big\{\, \overline{(1234,1)}, \overline{(1234,24)}, \overline{(1234,34)} \,\Big\} \\
G_{X_1} \cup \overline{E_{X_1}} &= \{\, s_3 \,\} \cup \Big\{\, \overline{(24,2)}, \overline{(24,4)} \,\Big\}
\end{aligned}
$$

Wir geben außerdem noch jeweils die Urbilder von $\varphi = decode$ an.

$$
\begin{aligned}
decode^{-1}(1) &= \{\, (1234,1) \,\}\ , \\
decode^{-1}(2) &= \{\, (24,2)(1234,24) \,\}\ , \\
decode^{-1}(3) &= \{\, (24,2)(1234,34) \,\}\ , \\
decode^{-1}(4) &= \{\, (24,4)(1234,24), (24,4)(1234,34) \,\}
\end{aligned}
$$

Da dieses Beispiel nur für Zustand 4 mehrere Pfade besitzt genügt es hier nur $p_{\{\,1,2,3,4\,\},\{\,4\,\}} = (24,4)(1234,24)$ zusätzlich zu fixieren. Abschließend geben wir noch die Cover an:

$$
cover_1(s_1,(\gamma_2)) = \overline{(24,4)} \qquad cover_2(s_1,()) = \overline{(1234,24)}
$$

$$
cover_1(s_2,(\gamma_2)) = \begin{cases} \overline{(24,2)} & ,\text{falls } \gamma_2 = (1234,1) \\ \overline{(24,4)} & ,\text{falls } \gamma_2 = (1234,24) \\ s_5 s_2 s_4 = s_3 & ,\text{falls } \gamma_2 = (1234,34) \end{cases} \qquad cover_2(s_2,()) = \overline{(1234,24)}
$$

$$
cover_1(s_3,(\gamma_2)) = \begin{cases} \overline{(24,2)} & ,\text{falls } \gamma_2 = (1234,1) \\ s_3 & ,\text{falls } \gamma_2 = (1234,24) \\ \overline{(24,4)} & ,\text{falls } \gamma_2 = (1234,34) \end{cases} \qquad cover_2(s_3,()) = \overline{(1234,24)}
$$

$$cover_1(s_4,(\gamma_2)) = \begin{cases} \overline{(24,2)} & ,\text{falls } \gamma_2 = (1234,1) \\ \overline{(24,4)} & ,\text{falls } \gamma_2 = (1234,24) \\ s_5 s_4 1 = s_3 & ,\text{falls } \gamma_2 = (1234,34) \end{cases} \qquad cover_2(s_4,()) = \overline{(1234,24)}$$

$$cover_1(s_5,(\gamma_2)) = \begin{cases} \overline{(24,2)} & ,\text{falls } \gamma_2 = (1234,1) \\ 1 s_5 s_4 = s_3 & ,\text{falls } \gamma_2 = (1234,24) \\ \overline{(24,4)} & ,\text{falls } \gamma_2 = (1234,34) \end{cases} \qquad cover_2(s_5,()) = \overline{(1234,24)}$$

Das soll jedoch nicht heißen, dass man diese Sprache nicht in noch einfachere Komponenten zerlegen könnte.

4 Zusammenfassung

Diese Diplomarbeit beschäftigt sich mit einer intuitiven, aber trotzdem möglichst kompakten Darstellung der Holonomie–Zerlegung von Automaten, die ausschließlich elementare Mittel nutzt. In Kapitel 2 werden die Grundlagen zu Transformations–Halbgruppen, Divisionen und Überdeckungen dargestellt. Anders als bei vielen Arbeiten wird hier eine vektorielle Notation des Kranzprodukts verwendet, was sich als sehr nützlich für die konstruktive Definition einer Überdeckung erweist. Die Beweise dieses Kapitels sind nicht neu und können in vielen Standardwerken nachgelesen werden. Eine Ausnahme ist eventuell Lemma 2.3, welches das Transformations–Monoid $(\{0,\ldots,n-1\},U_n)$ in nur logarithmisch viele Flip–Flops $(\{0,1\},U_2)$ zerlegt. In Kapitel 3 wird der *Inklusionsgraph* einer Transformations–Halbgruppe eingeführt und die Kanten, die als Transformations–Gruppe operieren, sowie Isomorphien dieser werden beschrieben. Anschließend wird ein neuer Beweis für die Holonomie–Zerlegung gegeben, der das Cover für die Überdeckung konstruktiv angibt. Als Korollar erhalten wir die Krohn–Rhodes Zerlegung einer Transformations–Halbgruppe (X,S) mit nur maximal $c\cdot|S|\cdot log_2(|S|+|X|)$ Faktoren.

Ältere Beweise für das Krohn–Rhodes Theorem[7] sind algebraisch gehalten und benutzen neben Induktion über die Größe der Halbgruppe auch das nicht–triviale Trichotomie–Lemma von Krohn und Rhodes. Zeigers Beweis der Holonomie–Zerlegung [10] kommt ohne diese Induktion aus. Er verwendet aber, wie auch spätere Versionen[4], eine Mischung von automatentheoretischen und algebraischen Konzepten, um eine Relation genügend zu verfeinern. Die vollständige und rein algebraische Formulierung dieser Idee durch Eilenberg[3, p.33-57] ist aktuelle Arbeitsgrundlage. Allerdings verwendet diese Darstellung partiell definierte Überdeckungen, die aus einer gemeinsamen, induktiven Verfeinerung von relationaler Überdeckung und Cover hervorgeht. Dieser Ansatz ist nachvollziehbar, aber nur schwer verständlich, weshalb neuere Arbeiten einen intuitiveren Beweis suchen. Maler gibt beispielsweise einen neueren, induktiven Beweis in automatentheoretisch-algebraischer Notation[8]. Diese Beweise tendieren, wegen der Übertragung algebraischer Konzepte auf Automaten, dazu unübersichtlich zu wirken.

Der hier vorgestellte Beweis der Holonomie–Zerlegung argumentiert algebraisch anhand des Inklusionsgraphen. Dadurch ist es möglich eine Überdeckung direkt konstruktiv anzugeben. Auch die Formulierung des Covers ist so auf eine nicht–induktive Weise möglich. Außerdem werden keine tieferen algebraischen Konzepte benötigt. Die Formulierung als Graph ermöglicht gleichzeitig eine einfache Abschätzung der Faktorenzahl einer Krohn–Rhodes Zerlegung.

Literaturverzeichnis

[1] Volker Diekert, Manfred Kufleitner, and Benjamin Steinberg. The Krohn-Rhodes Theorem and Local Divisors. *Fundam. Inform.*, 116(1-4):65–77, 2012.

[2] Attila Egri-Nagy. *Algebraic Hierarchical Decomposition of Finite State Automata*. PhD thesis, University of Hertfordshire, 2005.

[3] S. Eilenberg. *Automata, Languages, and Machines*. Number Bd. 2 in Pure and applied mathematics. Academic Press, 1976.

[4] Abraham Ginzburg. *Algebraic theory of automata*. ACM monograph series. Academic Press, New York, NY, 1968.

[5] Mike Holcombe. Abstract machine models of cell metabolism. *SIGBIO Newsl.*, 12(2):14–17, June 1992.

[6] Kenneth Krohn, Rudolph Langer, and John Rhodes. Algebraic Principles for the Analysis of a Biochemical System. *J. Comput. Syst. Sci.*, 1(2):119–136, 1967.

[7] Kenneth Krohn and John Rhodes. Algebraic Theory of Machines. I. Prime Decomposition Theorem for Finite Semigroups and Machines. *Transactions of the American Mathematical Society*, 116:pp. 450–464, 1965.

[8] Oded Maler. On the Krohn-Rhodes Cascaded Decomposition Theorem. In Zohar Manna and Doron Peled, editors, *Time for Verification*, volume 6200 of *Lecture Notes in Computer Science*, pages 260–278. Springer Berlin / Heidelberg, 2010.

[9] Dominique Perrin and Jean-Éric Pin. *Infinite Words*, volume 141. Elsevier, 2004.

[10] Paul Zeiger. Yet another proof of the cascade decomposition theorem for finite automata. *Theory of Computing Systems*, 1:225–228, 1967. 10.1007/BF01703821.

Erklärung

Hiermit versichere ich, diese Arbeit
selbständig verfasst und nur die
angegebenen Quellen benutzt zu haben.

(Martin P. Seybold)