Komplexitäts– und Entscheidbarkeitsresultate für inverse Monoide mit idempotenter Präsentation

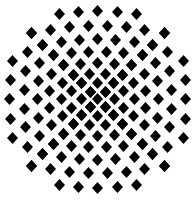
Von der Fakultät Informatik, Elektrotechnik und Informationstechnik der Universität Stuttgart zur Erlangung der Würde eines Doktors der Naturwissenschaften (Dr. rer. nat.) genehmigte Abhandlung

Vorgelegt von

Nicole Ondrusch
aus Leipzig

Hauptberichter:	Prof. Dr. Volker Diekert
Mitberichter:	Prof. Dr. Klaus-Jörn Lange
	Prof. Dr. Geraud Sénizergues

Tag der Einreichung: 2. Mai 2006
Tag der mündlichen Prüfung: 11. Oktober 2006



Universität Stuttgart
Institut für Formale Methoden der Informatik (FMI)
2006

Danksagung

Zunächst möchte ich mich bei Professor Volker Diekert und Markus Lohrey für die gute Zusammenarbeit und Unterstützung bei der Erstellung dieser Arbeit bedanken, auch gilt mein Dank Professor Geraud Sénizergues für die ideenreichen Gespräche und die Begutachtung der Arbeit. Ferner muss ich mich bei Professor Klaus-Jörn Lange für die Anfertigung des Gutachtens und besonders bei Professor Volker Claus bedanken.

In den letzten vier Jahren am Institut haben mich viele Kollegen und Freunde unterstützt. Hierfür und für die gemeinsame Arbeit möchte ich mich bedanken. Ein besonderer Dank gilt Professor Klaus Lagally, der mich in seine Abteilung aufgenommen und dafür gesorgt hat, dass ich neben der wissenschaftlichen Arbeit auch noch einiges über Betriebssysteme und Textsatzsysteme lerne.

Ein großes Dankeschön geht auch und vor allem an meine Familie mit Peter, Hendrik und Jonathan.

Inhaltsverzeichnis

Extended Abstract

We focus here on a special class of monoids – inverse monoids, which lie somewhere between monoids and groups. As groups arise naturally as bijections over a set, inverse monoids arise as monoids of partially defined injections over a set. We refer to [46] for detailed information.

The free inverse monoid $\mathrm{FIM}(\Gamma)$ over a set Γ is defined as the quotient of $(\Gamma \cup \Gamma^{-1})^*$ by (infinitely many) defining relations, also called the Vagner equations, $w = ww^{-1}w$, $ww^{-1}vv^{-1} = vv^{-1}ww^{-1}$, where $v, w \in (\Gamma \cup \Gamma^{-1})^*$.

We consider a special kind of inverse monoids. Our construction follows Birget and Rhodes [3, 4]. Let G be an infinite group. The elements of these inverse monoids, denoted by $\mathrm{IM}(G)$, are pairs (U, g) where U is a finite subset of G, g is an element of U and $1 \in U$. The multiplication of elements (U, g) and (V, h) of $\mathrm{IM}(G)$ is given by $(U, g)(V, h) = (U \cup gV, gh)$ and associativity and the Vagner equations are easily verified. The idempotents in this monoid are of the form $(U, 1)$. Let $P \subseteq \mathrm{IM}(G) \times \mathrm{IM}(G)$ be given by a (finite) set of idempotent pairs (e, e') in $\mathrm{IM}(G)$, this means that $e = (E, 1)$ and $e' = (E', 1)$ for some finite subsets $E, E' \subseteq G$. We call P a finite idempotent presentation over $\mathrm{IM}(G)$. This defines a quotient monoid $\mathrm{IM}(G)/P := \mathrm{IM}(G)/_{\cong_P}$ where $\cong_P$ is the smallest congruence generated by P.

The fact that for $(U, g) \in \mathrm{IM}(G)$ we require that $1 \in U$ is not essential, but following Margolis and Meakin, we concentrate on these monoids. In fact Margolis and Meakin [36] considered a special kind of these monoids where U is a connected subgraph of a Cayley graph of G, but it turns out that we are more flexible (we do not stick on the shape of the Cayley graph, so the construction does not depend on the generating set), if we do not pay attention to connectedness. Let $\mathrm{IM}(\Gamma, G)$ denote this submonoid of $\mathrm{IM}(G)$ which contains all elements $(U, g) \in \mathrm{IM}(G)$ where U is a connected subgraph of the Cayley graph of G w.r.t. the generating set Γ. We first focus on these inverse monoids $\mathrm{IM}(\Gamma, G)$. Let $\mathrm{FG}(\Gamma)$ be the free group generated by a finite set Γ. By Munn's theorem we

have $\mathrm{IM}(\Gamma, \mathrm{FG}(\Gamma)) = \mathrm{FIM}(\Gamma)$. Margolis and Meakin [37] generalized this result by considering a closure operation, $\mathrm{cl}_P(U)$, on elements (U, g) of $\mathrm{FIM}(\Gamma)$ w.r.t. P, where P is a finite set of idempotents in $\mathrm{IM}(\Gamma, G)$. More explicitly they get an inverse monoid where two elements (U, g) and (V, h) are equal if and only if $\mathrm{cl}_P(U) = \mathrm{cl}_P(V)$ and $g = h$. It turns out that this monoid is precisely the quotient monoid $\mathrm{IM}(\Gamma, G)/P := \mathrm{IM}(\Gamma, G)/_{\cong_P}$, where P is an idempotent presentation in $\mathrm{IM}(\Gamma, G)$ and $\cong_P$ the smallest congruence including P. We consider this monoid and denote it by $\mathrm{FIM}(\Gamma)/P$.

After some preliminaries we introduce the algebraic problems we are concerned here. First we are interested in solving the word problem for monoids $\mathrm{FIM}(\Gamma)/P$. The word problem for a monoid M is the question whether two given words represent the same element in M. In general the word problem is undecidable for finite presented monoids (Markov [39], Post [48]) and groups (Boone [8], Novikov [44]). This motivates a search for a class of monoids where the word problem is still decidable. Margolis and Meakin [37][1] have shown, that the word problem for monoids $\mathrm{FIM}(\Gamma)/P$ is decidable. They used a result from logic – Rabin's tree theorem. This leads to non-elementary complexity, so in [2, 37] the question for a better algorithm solving the word problem for this class of monoids is raised. We will show in Chapter 4 that this problem is decidable in linear time (on a RAM), while the uniform word problem is EXPTIME-complete. In the uniform word problem the idempotent presentation P is not fixed but part of the input.

Let from now on G be an infinite virtually free group and $P \subseteq \mathrm{IM}(G) \times \mathrm{IM}(G)$ an idempotent presentation. The above result can be generalized to $\mathrm{IM}(G)/P$. In Chapter 5 we give a direct proof for the decidability of word problem for $\mathrm{IM}(G)/P$. The proof is somewhat longer than the proof in Chapter 4, but does not use tree automata and other results, needed in Chapter 4 to prove decidability of the word problem for $\mathrm{FIM}(\Gamma)/P$.

In Chapter 6 we study a structure $\mathcal{C}(\mathrm{IM}(G)/P)$ with a predicate $\mathrm{reach}_L(x, y)$ for every regular language L, where two elements $x, y \in \mathrm{IM}(G)/P$ are in relation reach_L if and only if there is an element $w \in L$ such that $xw = y$ in $\mathrm{IM}(G)/P$. We show, that the first-order theory of this structure is decidable. The main part is to prove, that the predicate $\mathrm{reach}_L(x, y)$ can be transformed into an MSO-formula over the signature of the Cayley graph of G with respect to a generating set. We give two different proofs for this fact, where one uses MSO-transductions and results of Courcelle [16, 17, 18] while the other proof shows this fact from scratch using ideas of Kleene's proof of the fact that recognizable languages are rational.

[1] The result was announced by Margolis and Meakin at the international conference on semigroups in Szeged, Hungary in August 1987.

We use these results to prove in Chapter 7 the decidability of the generalized word problem for $\mathrm{IM}(G)/P$ (for G virtually free and P a finite idempotent presentation) and the decidability of the emptiness problem for Boolean combinations of rational sets of $\mathrm{IM}(G)/P$. This result goes beyond rational sets, because the family of rational sets of $\mathrm{FIM}(\Gamma)$ is not closed under finite intersection.

This work on inverse monoids was done with Volker Diekert and Markus Lohrey and some parts are published in a conference version in [33]. Some newer results in this thesis have been submitted.

Kapitel 1

Einführung

Algorithmische Fragestellungen von Problemen über algebraischen Strukturen sind ein Themengebiet der theoretischen Informatik mit engem Bezug zur Mathematik. Zu solchen Strukturen zählen Monoide und - als Spezialfall - inverse Monoide und Gruppen. Inverse Monoide erscheinen etwa als Transformationsmonoide kantenbeschrifteter (deterministischer und codeterministischer) Transitionssysteme. Genauer bildet jedes solche Transformationsmonoid ein inverses Monoid und umgekehrt definiert jedes inverse Monoid ein solches Transformationsmonoid.

Die Eigenschaften deterministisch und codeterministisch ergeben sich auf natürliche Weise aus den Forderungen, dass Systeme modelliert werden sollen, in denen durch eine Transaktion (wir werden dafür gleich Beispiele sehen) ein eindeutig bestimmter Zustand erreicht werden soll (Determinismus) und umgekehrt eine Aktion auch nur rückgängig gemacht werden kann, wenn sie zuvor auch durchgeführt wurde. Auch dies soll zu einem eindeutig bestimmten Zustand (Codeterminismus) führen.

Solche (deterministische und codeterministische) Transitionssysteme können etwa bei der *Modellierung von Steuerungsabläufen* eingesetzt werden. So kann zum Beispiel der Werkstückfluss in einer Montagelinie (eine Beschreibung der Steuerung einzelner Maschinen ist ebenso möglich) durch diese Systeme beschrieben werden. Technisch realisiert werden solche Ablaufsteuerungen häufig durch den Einsatz speicherprogrammierbarer Steuerungen (SPS oder englisch: Programmable Logic Controller, PLC). Die Zuständen beschreiben die entsprechenden, vom Werkstück angelaufenen, Stationen. Korrespondierende Aktionen werden nach Zuständen ausgelöst. So kann man sich an den Kantenbeschriftungen solche Aktionen wie das „Anziehen einer Schraube A“ vorstellen. Durch Ablaufen dieser

Kante wird ein Zustand „Werkstück mit angezogener Schraube A“erreicht. Offenbar ist hier erforderlich und gegeben, dass durch das Ausführen einer Aktion ein eindeutiger Zustand erreicht wird (Determinismus). Ebenso können nur Aktionen rückgängig gemacht werden (Anziehen einer Schraube), die zuvor durchgeführt worden. Auch hierfür wird ein eindeutiges Ergebnis (Codeterminismus) erwartet.

Ein weiteres einfaches Beispiel für den Einsatz dieser Transitionssysteme ist die Beschreibung der Arbeit eines gewöhnlichen Texteditors. So stellt man sich das Entlanglaufen einer Kante, die mit a beschriftet ist, etwa als die Eingabe eines a's in den Editor vor. Das Löschen (Zurücksetzen) eines a's (also das Zurücklaufen entlang einer a-Kante) ist offenbar nur möglich wenn man zuvor ein a geschrieben hat (mit einem a in diesen Zustand des Transitionssystem gelangen kann – diese mit a beschriftete Kante muss eindeutig sein, weswegen wir codeterministische Systeme verlangen). Umgekehrt muss natürlich auch die Eingabe eines a's eindeutig zu einem neuen Textdokument führen, weswegen deterministische Transitionssysteme zur Beschreibung erforderlich sind.

Für das Transformationsmonoid des Transitionssystems bedeuten diese Eigenschaften, dass, wird von einem beliebigen Zustand ausgehend ein Eingabestring s gelesen (dies endet wegen des Determinismus in einem eindeutigen Zustand) es einen (im Transformationsmonoid eindeutigen[1]) String s^{-1} gibt (wegen des Codeterminismus) so, dass nach Lesen von $ss^{-1}s$ der gleiche Zustand wie nach Lesen von s erreicht wird. Die Eingabestrings entsprechen also partiell definierten injektiven Abbildungen über einer (Zustands-)Menge und tatsächlich können alle inversen Monoide so realisiert werden.

Genauer heißt ein Monoid M *inverses Monoid*, falls es für alle $m \in M$ ein eindeutiges $m^{-1} \in M$ gibt so, dass $mm^{-1}m = m$ und $m^{-1}mm^{-1} = m^{-1}$. Statt die Existenz eines eindeutigen solchen $m \in M$ zu verlangen, kann man inverse Monoide auch über (Vagner-) Gleichungen definieren (und zu jedem $m \in M$ die Existenz eines $m^{-1} \in M$ verlangen so, dass die Gleichungen gelten):

$$\begin{aligned} mm^{-1}m &= m, \\ m^{-1}mm^{-1} &= m^{-1}, \\ mm^{-1}nn^{-1} &= nn^{-1}mm^{-1}, \end{aligned}$$

für alle $m, n \in M$. Es folgt, dass inverse Monoide eine Varietät bilden und dass freie Objekte existieren. Das *frei inverse Monoid* über einer endlichen Erzeugermenge Γ bezeichnen wir mit $\mathrm{FIM}(\Gamma)$. Inverse Monoide sowie ihre Verbindung

[1] Es mag mehrere Pfade geben, wenn dies jedoch in allen Zuständen der Fall ist, so sind die entsprechenden Elemente im Transformationsmonoid dieselben.

zur kombinatorischen Gruppentheorie und zur Automatentheorie, algorithmische Probleme und weitere Problemstellungen über inversen Monoiden wurden in den letzten Jahren vielfach untersucht [2, 5, 13, 14, 38, 59, 60, 63].

So wie sich alle Gruppen als bijektive Abbildungen einer Menge beschreiben lassen sind inverse Monoide gerade die Monoide der partiellen injektiven Abbildungen einer Menge G. In dieser Arbeit ist G eine unendliche Gruppe. Für jede endliche Teilmenge U von G können wir nun eine (fast überall definierte) injektive Abbildung von $G \backslash U$ durch

$$(U, g) : \ x \mapsto g^{-1}x,$$

angeben. Die partiellen Abbildungen vom Typ (U, g) definieren ein inverses Monoid $\mathcal{M}$, die Multiplikation zweier Elemente (U, g) und (V, h) aus $\mathcal{M}$ ist gegeben durch

$$(U, g)(V, h) = (U \cup gV, gh).$$

Das neutrale Element ist $(\emptyset, 1)$. Wir betrachten hier jedoch die Lokalisierung (siehe auch Birget, Rhodes [3, 4]) dieses Monoids $\mathcal{M}$ an dessen Idempotenten $(\{1\}, 1)$ dies ist ein Monoid mit Elementen der Form $(U \cup \{1, g\}, g)$ für alle $(U, g) \in \mathcal{M}$. Mit anderen Worten, wir erhalten ein Monoid in dem für Elemente (V, h) gilt, dass $1, h \in V$. Das neutrale Element ist jetzt $(\{1\}, 1)$. Für eine unendliche Gruppe G bezeichnen wir dieses Monoid mit $\mathrm{IM}(G)$.

Betrachten wir Elemente (U, g) mit zusammenhängender Teilmenge U des Cayleygraphen $\mathcal{C}(G, \Gamma)$ der Gruppe G mit $1 \in U$ und $g \in U$ so erhalten wir die von Margolis und Meakin [36, 37] gegebene Konstruktion inverser Monoide $\mathrm{IM}(\Gamma, G)$. Diese ist jedoch abhängig von der Erzeugermenge Γ der Gruppe G.

Wir interessieren uns für eine Klasse inverser Monoide, die wiederum zwischen inversen Monoiden und Gruppen liegt: Eine Kongruenz ρ auf einem Monoid M heißt Gruppenkongruenz, wenn M/ρ eine Gruppe ist. Für inverse Monoide M ist eine Kongruenz $\rho \subseteq M \times M$ genau dann eine Gruppenkongruenz, wenn ρ alle Paare (im Allgemeinen unendlich viele) von Idempotenten aus M umfasst. Bei den hier betrachteten inversen Monoiden werden nun nur endlich viele Gleichungen zwischen Idempotenten zugelassen, weswegen wir diese Monoide als *inverse Monoide mit (endlich) idempotenter Präsentation* bezeichnen. Ist P eine endliche Menge von Gleichungen zwischen Idempotenten aus $\mathrm{IM}(G)$ (eine idempotente Präsentation) und $\cong_P$ die kleinste von P erzeugte Kongruenz so heißt das Quotientenmonoid $\mathrm{IM}(G)/_{\cong_P}$ inverses Monoid mit idempotenter Präsentation. Diese algebraische Struktur, die wir kurz mit $\mathrm{IM}(G)/P$ bezeichnen, werden wir für endlich erzeugte virtuell freie Gruppen G untersuchen. Eine Gruppe heißt virtuell frei, wenn sie eine nicht-triviale freie Untergruppe von endlichem Index besitzt.

Ebenso können wir ein Monoid $\mathrm{IM}(\Gamma, G)/P$ definieren (mit Idempotenten aus $\mathrm{IM}(\Gamma, G)$). Ist G eine freie Gruppe, so ist $\mathrm{IM}(\Gamma, G) = \mathrm{FIM}(\Gamma)$ (Munn, [43]) und $\mathrm{IM}(\Gamma, G)/P = \mathrm{FIM}(\Gamma)/P$ (Margolis, Meakin [37]). Aus diesen Resultaten folgt die Entscheidbarkeit des Wortproblems für $\mathrm{FIM}(\Gamma)$ und des (uniformen) Wortproblems[2] für $\mathrm{FIM}(\Gamma)/P$. Einen alternativen Beweis der Entscheidbarkeit des (uniformen) Wortproblems für $\mathrm{FIM}(\Gamma)/P$ gibt Silva [59]. Das *Wortproblem* für ein Monoid M ist die Frage, ob zwei gegebene Wörter das gleiche Element in M repräsentieren. Beim uniformen Wortproblem für $\mathrm{FIM}(\Gamma)/P$ ist die idempotente Präsentation P nicht wie beim Wortproblem für $\mathrm{FIM}(\Gamma)/P$ fest, sondern Teil der Eingabe. Im Allgemeinen ist das Wortproblem für endlich präsentierte Monoide (Markov [39], Post [48]) und Gruppen (Boone [8], Novikov [44]) unentscheidbar.

Der Beweis von Margolis und Meakin für die Entscheidbarkeit des Wortproblems von $\mathrm{FIM}(\Gamma)/P$ nutzt ein Resultat aus der Logik – Rabins Baumtheorem. Dies führt zu nichtelementarer Komplexität, weswegen in [2, 37] die Frage nach einem besseren Algorithmus für das Wortproblem für diese Klasse von Monoiden gestellt wird (siehe [33]). Wir werden in Kapitel 4 zeigen, dass dieses Problem in Linearzeit (auf einer RAM) lösbar ist, das uniforme Wortproblem jedoch EXPTIME-vollständig ist.

Wir nutzen für den Beweis der Lösbarkeit des Wortproblems für $\mathrm{FIM}(\Gamma)/P$ eine Reihe von Resultaten und Konstrukte wie etwa Baumautomaten, so dass sich die Frage nach einem direkten Beweis stellt. Wir stellen einen direkten Beweis für das allgemeinere Problem der Lösbarkeit des Wortproblems in Linearzeit (auf einer RAM) für $\mathrm{IM}(G)/P$ mit G virtuell frei in Kapitel 5 vor.

Das *verallgemeinerte Wortproblem* für ein Monoid M ist die Frage, ob das durch ein gegebenes Wort u repräsentierte Element in M in dem von den durch die gegebenen Wörter $u_1, \ldots, u_n$ repräsentierten Elementen erzeugten Untermonoid von M liegt. Die Entscheidbarkeit des verallgemeinerten Wortproblems für inverse Monoide $\mathrm{FIM}(\Gamma)/P$ und $\mathrm{IM}(G)/P$ für virtuell freie Gruppen g folgt als Korollar aus einem allgemeineren Resultat. Wir betrachten relationale Strukturen $\mathcal{C}(M)$. Diese Strukturen enthalten für jede raionale Sprache $L \subseteq \mathrm{RAT}(M)$ ein Prädikat reach_L. Hierbei stehen zwei Elemente u, v eines Monoids M genau dann in der Relation reach_L, wenn es ein $w \in L$ mit $uw = v$ in M gibt. Wir zeigen, dass die FO-Theorie dieser relationalen Struktur für $M = \mathrm{IM}(G)/P$ mit G virtuell frei (und mit den gleichen Methoden auch für $M = \mathrm{FIM}(\Gamma)/P$) entscheidbar ist.

Aus diesem Ergebnis lässt sich neben der Entscheidbarkeit des verallgemeinerten Wortproblems für $\mathrm{IM}(G)/P$ leicht die Entscheidbarkeit des Leerheitsproblems

[2] Die Entscheidbarkeit des Wortproblems für $\mathrm{FIM}(\Gamma)/P$ wurde von Margolis und Meakin bereits auf der international conference on semigroups in Szeged, Ungarn, im August 1987 angekündigt.

für eine boolesche Kombination von rationalen Mengen aus $\mathrm{IM}(G)/P$ folgern. Dieses Leerheitsproblem ist für jedes endlich erzeugte Monoid M für dass die Menge der rationalen Mengen von M eine effektive boolesche Algebra bildet entscheidbar. Jedoch gilt im Fall $M = \mathrm{FIM}(\Gamma)$, dass die Familie der rationalen Mengen von M keine boolesche Algebra bildet. Genauer, sie ist nicht abgeschlossen unter endlichem Durchschnitt.

Die Beweise der genannten Resultate (siehe auch [33]) nutzen verschiedene Techniken und Methoden aus der theoretischen Informatik, so zum Beispiel die Übersetzung von MSO-Formeln in Baumautomaten. Diese Automaten arbeiten auf (unendlichen) Bäumen und spielen etwa in der Verifikation unendlicher Systeme eine Rolle. Die Konzepte dazu werden in den Abschnitten 2.3 und 2.4 des Kapitels 2 vorgestellt.

Zum Beweis der oberen Schranke für das uniforme Wortproblem reduzieren wir dieses auf ein Model-Checking Problem für den modalen μ-Kalkül und nutzen dann ein Resultat aus dem Bereich des Model-Checkings [28, 69]. Der modale μ-Kalkül [65] ist eine Erweiterung der modalen Logik durch Fixpunkt-Operatoren. Verwendet wird er vor allem zur Verifikation endlicher Transitionssysteme. Die entsprechenden Notationen und Definitionen führen wir zu Beginn des Abschnitts 4.2 ein. Zum Beweis der unteren Schranke nutzen wir die Tatsache, dass EXPTIME gleich APSPACE, der Klasse aller Probleme, die in polynomieller Zeit von einer alternierenden Turingmaschine erkannt werden, ist. Die Konfigurationen einer solchen Turingmaschine sind dann Basis für eine „Codierung“ der Berechnung einer alternierenden Turingmaschine durch den Prozess der Abschlussbildung eines Munnbaums (Darstellung eines Elements aus $\mathrm{FIM}(\Gamma)$). Die Definition von alternierenden Turingmaschinen sowie Baumautomaten werden in Abschnitt 2.5 gegeben.

Für den Beweis der Entscheidbarkeit der FO-Theorie von $\mathcal{C}(\mathrm{IM}(G)/P)$ nutzen wir Resultate aus der Logik, hier vor allem Rabins Baumtheorem und den Begriff der MSO-Transduktion. Die Grundlagen dazu sowie für alle weiterführenden Kapitel werden im Kapitel 2 eingeführt. Kapitel 3 befasst sich mit Grundlagen und allgemeinen Konstruktionen inverser Monoide. Hier werden die in dieser Arbeit behandelten Strukturen ausführlich vorgestellt und erste Resultate bewiesen. Die oben erwähnten algorithmischen Probleme werden im Kapitel 2 behandelt und notwendige und mehrfach vorkommende Konzepte für Beweise ausgeführt. Die folgenden Kapitel widmen sich dann den weiteren Beweisen der obigen Ergebnisse.

Wesentliche Ergebnisse dieser Dissertation entstammen einer Zusammenarbeit mit Markus Lohrey und erschienen in [33] als Konferenzartikel. Eine ausführ-

liche Zeitschriftenversion dieses Artikels, die auch neue Ergebnisse aus dieser Arbeit beinhaltet, wurde zur Veröffentlichung eingereicht.

Kapitel 2

Definitionen, Notationen und allgemeine Grundlagen

In diesem Kapitel werden Definitionen wiederholt und im Folgenden wichtige Notationen einführt. Auch geben wir bekannte Resultate an, die im Weiteren benötigt werden.

2.1 Monoide und Cayleygraphen

Sei Γ eine endliche Menge, wir werden die Elemente aus Γ mit kleinen Buchstaben (etwa $a, b, a_1, a_2, \ldots$) bezeichnen. Sei $\Gamma^{-1} = \{a^{-1} \mid a \in \Gamma\}$ eine zu Γ in 1–1-Beziehung stehende disjunkte Menge. Für alle $a^{-1} \in \Gamma^{-1}$ definieren wir $(a^{-1})^{-1} = a$. Damit ist $^{-1}$ eine Involution die wir durch $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ mit $a_i \in \Gamma \cup \Gamma^{-1}$ und $\epsilon^{-1} = \epsilon$ (wobei wir mit ϵ das leere Wort in $(\Gamma \cup \Gamma^{-1})^*$ bezeichnen) auf Wörter aus $(\Gamma \cup \Gamma^{-1})^*$ fortsetzen können. Die Länge n eines Wortes $w = a_0 \cdots a_n$, $a_i \in \Gamma \cup \Gamma^{-1}$, notieren wir mit $|w|$.

Sei $(M, \circ, 1)$ ein Monoid mit Operation $\circ$ und neutralem Element 1. Ist beides aus dem Zusammenhang klar oder unerheblich, so schreiben wir statt $(M, \circ, 1)$ lediglich M. Ein von einer Menge $\Sigma \subseteq M$ erzeugtes Monoid M heißt endlich erzeugt, falls Σ endlich ist. Dies sei von nun an der Fall.

Die freie Gruppe, FG(Γ), auf der Erzeugermenge Γ ist der Quotient $(\Gamma \cup \Gamma^{-1})^*/\gamma_c$, wobei $\gamma_c \subseteq (\Gamma \cup \Gamma^{-1})^* \times (\Gamma \cup \Gamma^{-1})^*$ die kleinste Kongruenz ist, die alle Paare

(aa^{-1}, ϵ) und $(a^{-1}a, \epsilon)$ mit $a \in \Gamma$ enthält. Den kanonischen surjektiven Homomorphismus $(\Gamma \cup \Gamma^{-1})^* \to \mathrm{FG}(\Gamma)$ bezeichnen wir mit γ .

Ist $g \in \mathrm{FG}(\Gamma)$ so schreiben wir $|g|$ für die Länge des reduzierten, g repräsentierenden Wortes.

Sei M ein Monoid mit Erzeugermenge Σ, der (Rechts-)Cayleygraph $\mathcal{C}(M, \Sigma)$ des Monoids M bezüglich Σ enthält alle Elemente von M als Knoten und besitzt genau dann eine mit $a \in \Sigma$ markierte Kante von $m_1 \in M$ nach $m_2 \in M$ wenn gilt $m_1\gamma(a) = m_2$:

$$\mathcal{C}(M, \Sigma) = (M, (\{(m_1, m_2) \in M \times M \mid m_1\gamma(a) = m_2\})_{a\in\Sigma}, 1)$$

Cayleygraphen wurden und werden insbesondere in der Gruppentheorie viel studiert (siehe etwa [57]) und sind ein wichtiges Instrument der kombinatorischen Gruppentheorie [34], aber auch in anderen Bereichen der Mathematik und theoretischen Informatik finden sie Anwendung [41, 42].

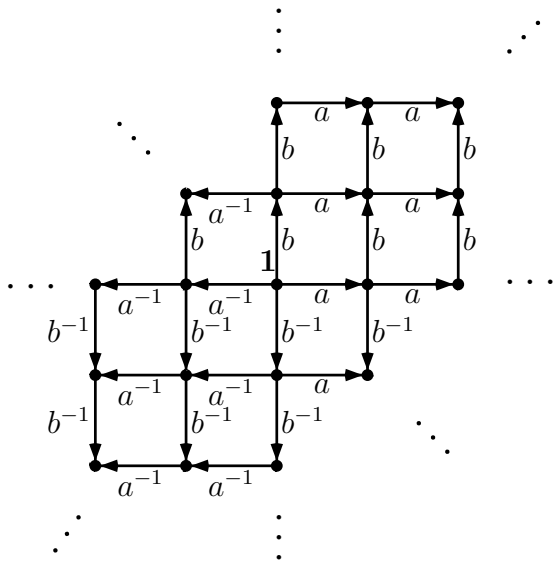
Cayleygraphen von Monoiden sind weniger umfangreich studiert und wurden in neuerer Zeit betrachtet, siehe zum Beispiel [25, 26, 27, 71]. Cayleygraphen von automatischen Monoiden werden in [61, 62] untersucht.

Wir bezeichnen mit $\mathcal{C}(\Gamma)$ den Cayleygraph der freien Gruppe $\mathrm{FG}(\Gamma)$ bezüglich der Erzeugermenge Γ.

Im Cayleygraph von $\mathrm{FG}(\Gamma)$ (oder allgemein im Cayleygraph einer Gruppe), gibt es genau dann eine mit $a \in \Gamma \cup \Gamma^{-1}$ markierte Kante von $g_1 \in \mathrm{FG}(\Gamma)$ nach $g_2 \in \mathrm{FG}(\Gamma)$, wenn $g_1\gamma(a) = g_2$ und damit $g_2\gamma(a^{-1}) = g_1$. Mit anderen Worten, es gibt ebenso eine (mit a^{-1} markierte) Kante von g_2 nach g_1. Wir werden in der graphischen Darstellung nur eine Kante $g_1 \xrightarrow{a} g_2$ mit Markierung $a \in \Gamma$ angeben, die andere Kante nehmen wir implizit an.

Beispiel 2.1.1 *Sei $\Gamma = \{a, b\}$. Sei $G = \mathbb{Z} \times \mathbb{Z} = (\Gamma \cup \Gamma^{-1})^*/\zeta$, wobei $\zeta = \gamma \cup \eta$ und η sei die kleinste Kongruenz, die alle Paare (ab, ba) mit $a, b \in \Gamma \cup \Gamma^{-1}$ enthält.*

Ein Ausschnitt aus dem Cayleygraphen von $\mathcal{C}(G, \Gamma \cup \Gamma^{-1})$ sieht dann folgendermaßen aus:



Diese Struktur (Gitter) des Cayleygraphen $\mathcal{C}(G, \{a, b\})$ von $G = \mathbb{Z} \times \mathbb{Z}$ wird in Zusammenhang mit MSO-Logik auf Cayleygraphen im Abschnitt 6.3 wieder eine Rolle spielen.

Die Form des Cayleygraphen eines Monoids M ist abhängig von der gewählten Präsentation. Wir sehen später (nächster Abschnitt bzw. Abschnitt 2.6), dass dieses Aussehen jedoch auf die Entscheidbarkeit gewisser Logiken über der Signatur eines Cayleygraphen keinen Einfluss hat. Die Grundlagen hierzu stellen wir im folgenden Abschnitt vor.

2.2 Logik

Für weiterführende Ergebnisse und Definitionen zu diesem Abschnitt siehe etwa [22].

Sei S eine Menge. Eine Signatur SIG ist eine abzählbare Menge relationaler Symbole $R \in \mathsf{SIG}$, denen jeweils eine Stelligkeit n_R zugeordnet ist. Eine (relationale) Struktur ist ein Tupel

$$\mathcal{S} = (S, (R^{\mathcal{S}})_{R \in \mathsf{SIG}})$$

über der Domäne (Grundmenge) S mit n_R-stelligen Relationen $(R^{\mathcal{S}})_{R \in \mathsf{SIG}}$. Hierbei interpretiert eine solche Relation $R^{\mathcal{S}}$ über der Grundmenge S entsprechend das relationale Symbol $R \in \mathsf{SIG}$ in der Struktur $\mathcal{S}$.

Wir nehmen an, dass jede Signatur das Gleichheitssymbol $=$ enthält und $=^{\mathcal{S}}$ die Identität(srelation) auf S ist. Konstanten $c \in S$ können als unäre Relation $\{c\}$ codiert werden. Zur Abkürzung werden wir $R^{\mathcal{S}}$ auch einfach mit R bezeichnen.

Die Einschränkung einer Struktur $\mathcal{S}$ auf einen Teilbereich der Domäne $S' \subseteq S$ ist wieder eine Struktur über derselben Signatur und definiert durch:

$$\mathcal{S}|_{S'} = (S', (R^{\mathcal{S}} \cap (S')^{n_R}))$$

wobei n_R die Stelligkeit der Relation R sei. Wir bezeichnen mit RS(SIG) die Menge aller relationalen Strukturen über einer Signatur SIG.

Beispiel 2.2.1 *Sei M ein Monoid. Der Cayleygraph*

$$\mathcal{C}(M, \Sigma) = (M, (\{(m_1, m_2) \in M \times M \mid m_1\gamma(a) = m_2\})_{a\in\Sigma}, 1)$$

von M bezüglich der Erzeugermenge Σ ist eine relationale Struktur deren Grundmenge alle Elemente des Monoids M enthält. Die Signatur von $\mathcal{C}(M, \Sigma)$ enthält binäre Symbole für die Kantenrelationen und ein unäres Symbol für die Auszeichnung des speziellen, mit $1 \in M$ markierten, Knotens im Graphen.

Beispiel 2.2.2 *Sei Γ eine endliche Menge und T_Γ die folgende Struktur:*

$$T_\Gamma = ((\Gamma \cup \Gamma^{-1})^*, \{r_a \mid a \in \Gamma \cup \Gamma^{-1}\}, \epsilon)$$

wobei $r_a : (\Gamma \cup \Gamma^{-1})^* \to (\Gamma \cup \Gamma^{-1})^*$ die Rechtsmultiplikation in $(\Gamma \cup \Gamma^{-1})^*$ ist. Mit anderen Worten $ur_a = ua$ für alle $u \in (\Gamma \cup \Gamma^{-1})^*$, $a \in \Gamma \cup \Gamma^{-1}$. Aufgefasst als Graph mit Kanten entsprechend r_a ist

$$T_\Gamma = ((\Gamma \cup \Gamma^{-1})^*, (\{(u_1, u_2) \in (\Gamma \cup \Gamma^{-1})^* \times (\Gamma \cup \Gamma^{-1})^* \mid u_1 a = u_2\})_{a\in\Gamma\cup\Gamma^{-1}}, \epsilon)$$

der Cayleygraph des freien Monoids $(\Gamma \cup \Gamma^{-1})^*$.

Sei var eine (abzählbar unendliche) Menge von Variablen erster Stufe (englisch: first-order) bzw. VAR eine (abzählbar unendliche) Menge von Variablen zweiter Stufe (englisch: second-order). Wir werden Variablen erster Stufe mit kleinen Buchstaben ($x, y, z, \ldots$) und Variablen zweiter Stufe mit großen Buchstaben (etwa $X, Y, Z, \ldots$) bezeichnen.

Eine MSO-Formel (von englisch: monadic second-order) über der Signatur SIG ist eine Formel φ gebildet:

- aus atomaren Formeln $R(x_1, \ldots, x_{n_R})$; mit $R \in$ SIG, $x_1, \ldots, x_{n_R} \in$ var sowie

- aus atomaren Formeln $x \in X$; wobei $x \in \mathsf{var}$ und $X \in \mathsf{VAR}$ unter Verwendung von
- booleschen Operationen $\neg$, $\wedge$ und $\vee$ sowie
- Quantifizierungen ($\forall$, $\exists$) über Variablen aus var bzw. VAR.

Eine FO-Formel (von englisch: first-order) über SIG ist eine MSO-Formel φ in der keinerlei Variablen aus VAR vorkommen. Mit anderen Worten, φ enthält keinerlei atomare Teilformeln wie im zweiten Punkt.

Eine Variable heißt frei in einer Formel φ, wenn sie nicht durch einen Quantor gebunden ist. Eine MSO-Formel ohne freie Variablen heißt MSO-Satz. Ist $\varphi(x_1, \ldots, x_n, X_1, \ldots, X_m)$ eine MSO-Formel in der höchstens freie Variablen erster Stufe aus der Menge $\{x_1, \ldots, x_n\} \subseteq \mathsf{var}$ bzw. freie Variablen zweiter Stufe aus der Menge $\{X_1, \ldots, X_m\} \subseteq \mathsf{VAR}$ vorkommen und $s_1, \ldots, s_n \in S$ sowie $S_1, \ldots, S_m \subseteq S$, dann bedeutet

$$\mathcal{S} \models \varphi(s_1, \ldots, s_n, S_1, \ldots, S_m)$$

dass φ in $\mathcal{S}$ wahr ist, falls die freien Variablen x_i (bzw. X_j) durch s_i (bzw. S_j) ersetzt werden.

Sei $\mathcal{S}$ eine Struktur. Die Menge aller MSO-Formeln φ ohne freie Variablen so, dass $\mathcal{S} \models \varphi$ heißt MSO-Theorie von $\mathcal{S}$ und wird mit $\mathrm{MSOTh}(\mathcal{S})$ bezeichnet. Analog wird die FO-Theorie $\mathrm{FOTh}(\mathcal{S})$ der Struktur $\mathcal{S}$ definiert.

Sei $\varphi(x_1, \ldots, x_n, X_1, \ldots, X_m)$ und $Y \in \mathsf{VAR} \setminus \{X_1, \ldots, X_m\}$. Dann definieren wir $\varphi|_Y(x_1, \ldots, x_n, X_1, \ldots, X_m, Y)$ induktiv durch Einschränken aller Quantoren in der Formel φ auf die Menge Y. Wir erhalten für alle Teilmengen $S' \subseteq S$ und alle $s_1, \ldots, s_n \in S'$ sowie $S_1, \ldots, S_m \subseteq S'$:

$$\mathcal{S}|_{S'} \models \varphi(s_1, \ldots, s_n, S_1, \ldots, S_m) \Leftrightarrow \mathcal{S} \models \varphi|_Y(s_1, \ldots, s_n, S_1, \ldots, S_m).$$

Wir benötigen folgenden

Satz 2.2.3 ([30]) *Sei M ein endlich erzeugtes Monoid. Seien Σ_1 und Σ_2 zwei endliche Erzeugermengen von M. Dann ist die FO-Theorie (bzw. die MSO-Theorie) des Cayleygraphen $\mathcal{C}(M, \Sigma_1)$ mit logarithmischen Platz reduzierbar auf die FO-Theorie (bzw. MSO-Theorie) des Cayleygraphen $\mathcal{C}(M, \Sigma_2)$.*

Mit anderen Worten, die Entscheidbarkeit der MSO-Theorie bzw. FO-Theorie des Cayleygraphen $\mathcal{C}(M, \Sigma)$ eines Monoids M bezüglich Erzeugermenge Σ hängt nicht von dieser ab. Wir werden deshalb im Folgenden von der Entscheidbarkeit von MSO- (FO-) Theorie des Cayleygraphen eines Monoids sprechen.

2.3 MSO-Formeln über Graphen

Wir nutzen an verschiedenen Stellen die Entscheidbarkeit der MSO-Theorie über dem Cayleygraph der freien Gruppe $\mathcal{C}(\Gamma)$ (Theorem 2.4.4), um, zum Beweis von Entscheidbarkeitsresultaten für (WP) und (GWP), gewisse Formeln in MSO-Formeln über der Signatur gerichteter Graphen (etwa $\mathcal{C}(\Gamma)$) zu übersetzen.

In diesem Abschnitt geben wir entsprechende Hilfsformeln an, auf die wir immer wieder zurückgreifen werden. Zunächst einige allgemeine Formeln über der Signatur E eines Graphen $G = (V, E)$.

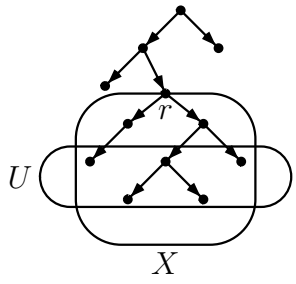
Sei $G = (V, E)$ ein gerichteter Graph, dann gibt es eine Formel $\mathrm{reach}(x, y)$ so, dass für Knoten $s, t \in V$ gilt $G \models \mathrm{reach}(s, t)$ genau dann, wenn es einen Pfad von s nach t in G gibt. Genauer ist $\mathrm{reach}(x, y)$ die folgende Formel:

$$\forall X : ((x \in X \wedge \forall u, v : (u \in X \wedge E(u, v) \Rightarrow v \in X)) \Rightarrow y \in X)$$

Mit dieser MSO-Formel ist es jetzt einfach, in MSO über der Signatur E auszudrücken, dass eine Menge von Knoten in $G = (V, E)$ zusammenhängend bzw. stark zusammenhängend ist.

Nun nutzen wir mit Königs Lemma einen Standardtrick (siehe etwa [50]), um die Endlichkeit einer Menge $U \subseteq V$ in einem Baum $T = (V, E)$ von endlichem Grad auszudrücken.

Dazu bilden wir den „Zusammenhangsabschluss“ von U bezüglich eines Knotens r in $T = (V, E)$. Dies ist die kleinste zusammenhängende Menge von Knoten in $T = (V, E)$, die U und r enthält. Genauer geben wir eine Formel zsh-cl(r, U, X) an, mit $T \models \mathrm{zsh-cl}(r, U, X)$ genau dann wenn X den Abschluss von U bis zum Knoten r enthält (alle Knoten oberhalb von U bis zum Knoten r).



Um $\mathrm{zsh-cl}(r, U, X)$ zu formulieren nutzen wir wieder $\mathrm{reach}(x, y)$ um die Existenz eines endlichen Pfades auszudrücken. Genauer sei $N(x)$ die Menge aller Nachbarknoten von x in $T = (V, E)$ und sei $\mathrm{epfad}(x, y, X)$ folgende Formel

$$\begin{aligned}\mathrm{epfad}(x, y, X) \;:=\; & (X = \{x\} \wedge x = y) \;\vee\; (x \neq y \;\wedge\; x, y \in X \;\wedge \\ & |N(x) \cap X| = |N(y) \cap X| = 1 \;\wedge \\ & \forall z \in X \setminus \{x, y\} : |N(z) \cap X| = 2 \;\wedge \\ & \forall z \in X : \mathrm{reach}|_X(x, z, X)).\end{aligned}$$

Dann ist $T \models \mathrm{epfad}(x, y, X)$ genau dann, wenn X ein endlicher Pfad von x nach y ist. Damit erhalten wir

$$\mathrm{zsh-cl}(r, U, X) := \forall x : \ (x \in X \Leftrightarrow \exists y \in U \exists Y : (\mathrm{epfad}(r, y, U) \wedge x \in Y)).$$

Offenbar ist U endlich, wenn der Abschluss X dies ist.

Nach dem Lemma von König ist nun (da T und damit X endlichen Grad hat) X endlich, falls es keinen unendlichen Pfad in X gibt. Um dies auszudrücken benötigen wir folgende Formel:

$$\begin{aligned} \omega\mathrm{pfad}(x, X) \ := \ & x \in X \ \wedge \ |N(x) \cap X| = 1 \ \wedge \\ & \forall y \in X \setminus \{x\} : |N(y) \cap X| = 2 \ \wedge \\ & \forall y \in X : \mathrm{reach}|_X(x, y, X). \end{aligned}$$

Insgesamt erhalten wir

Bemerkung 2.3.1 $T \models \mathrm{endlich}(U)$*, mit*

$$\mathrm{endlich}(U) := \exists r \exists X : \ \mathrm{zsh-cl}(r, U, X) \wedge \nexists Z : \ (\omega\mathrm{pfad}(r, Z) \wedge Z \subseteq X)$$

genau dann, wenn U eine endliche Menge von Knoten in T ist.

2.4 Baumautomaten und MSO-Logik

Die (unendliche) Baumstruktur des Cayleygraphen $\mathcal{C}(\Gamma)$ der freien Gruppe wird in dieser Arbeit an vielen Stellen eine wesentliche Rolle spielen. Hilfreich sind hier endliche Automaten auf unendlichen Bäumen – ω-Baumautomaten – und MSO-Logik über der Signatur von unendlichen Bäumen.

Büchi [9] und Elgot [20] waren die ersten, die einen Zusammenhang zwischen Logik und endlichen Automaten erkannten:

Theorem 2.4.1 ([9],[20]) *Sei Σ eine endliche Menge und $L \subseteq \Sigma^*$ eine Sprache endlicher Wörter. Dann ist L genau dann regulär wenn L MSO-definierbar über der Signatur endlicher Wörter ist. Beide Transformationen (von Automaten zu MSO-Formeln und umgekehrt) sind effektiv.*

Diese Äquivalenz lässt sich ebenfalls (Büchi [10]) für MSO über unendlichen Wörtern zeigen (ω-Automaten).

1969 konnte Rabin [50] schließlich das Resultat auf (unendliche) Bäume erweitern. Um dieses Resultat anzugeben benötigen wir folgendes Wissen über Bäume und Automaten. Wir betrachten endliche ω-Baumautomaten, die top-down auf unendlichen Bäumen arbeiten. Es gibt (wie auch bei ω-Automaten) verschiedene Akzeptanzbedingungen (Muller, Street, Rabin siehe [66]). Da es hier darauf jedoch nicht ankommt, werden wir auf dies nicht näher eingehen. Wir verwenden die Muller-Akzeptanzbedingung.

Definition 2.4.1 *Ein (top-down) ω-Baumautomat ist ein Tupel*

$$\mathcal{A} = (Q, \Sigma, \Delta, q_0, \mathcal{F}),$$

mit einer Menge Q von Zuständen, einem Alphabet Σ, Transitionsrelation $\Delta \subseteq Q \times \Sigma \times Q^{2|\Gamma|}$ sowie $q_0 \in Q$ und $\mathcal{F} \subseteq 2^Q$.

Ein Lauf des Automats $\mathcal{A}$ auf einem (unendlichen) Baum

$$((\Gamma \cup \Gamma^{-1})^*, (r_a)_{a \in \Gamma \cup \Gamma^{-1}}, \lambda)$$

der Knotenmarkierung $\lambda : (\Gamma \cup \Gamma^{-1})^* \to \Sigma$ ist ein (unendlicher) Baum $((\Gamma \cup \Gamma^{-1})^*, (r_a)_{a \in \Gamma \cup \Gamma^{-1}}, \lambda_Q)$ mit Knotenmarkierung $\lambda_Q : (\Gamma \cup \Gamma^{-1})^* \to Q$ so, dass $\lambda_Q(\epsilon) = q_0$ und

$$(\lambda_Q(w), \lambda(w), (\lambda_Q(wa))_{a \in \Gamma \cup \Gamma^{-1}}) \in \Delta$$

für alle $w \in (\Gamma \cup \Gamma^{-1})^*$.

Ein Lauf $((\Gamma \cup \Gamma^{-1})^*, (r_a)_{a \in \Gamma \cup \Gamma^{-1}}, \lambda_Q)$ heißt erfolgreich, wenn es einen Pfad in $((\Gamma \cup \Gamma^{-1})^*, (r_a)_{a \in \Gamma \cup \Gamma^{-1}}, \lambda_Q)$ gibt, bei welchem die Menge aller Zustände, deren Knoten unendlich oft durchlaufen werden, eine Teilmenge von $\mathcal{F}$ ist.

Wir können nun das Resultat von Rabin angeben.

Theorem 2.4.2 ([50]) *Zu jeder MSO-Formel φ über der Signatur $\mathsf{SIG} = (\{r_a \mid a \in \Gamma \cup \Gamma^{-1}\}, \epsilon))$ eines Baums T kann (effektiv) ein Baumautomat $\mathcal{A}$ mit der Eigenschaft*

$$T \models \varphi \Leftrightarrow \mathcal{A} \text{ akzeptiert den Baum } T$$

angegeben werden.

Eine Folgerung aus Theorem 2.4.2 ist ein berühmtes Entscheidbarkeitsresultat von Rabin: wenden wir Theorem 2.4.2 auf einen MSO-Satz φ an, so liefert dies einen Baumautomat mit akzeptierendem Lauf auf einem Baum T genau dann, wenn φ auf T (als relationale Struktur) wahr ist. Rabins Basistheorem (siehe [51]) besagt nun, dass die Existenz eines solchen Laufs effektiv entschieden werden kann. Wir erhalten:

Theorem 2.4.3 (Rabins Baumtheorem, [50]) *Für jede abzählbare Menge Γ ist die MSO-Theorie von T_Γ, $\mathrm{MSOTh}(T_\Gamma)$, entscheidbar.*

Aus diesem Resultat kann (siehe dazu etwa [37]) das folgende Ergebnis von Muller und Schupp ([42]) hergeleitet werden. Hierzu wird MSOTh($\mathcal{C}(\Gamma)$) auf MSOTh(T_Γ) reduziert. Da wir genau diese Methoden auch später in Beweisen benötigen möchten wir hier kurz die Ansätze skizzieren. Wesentliche Idee ist (semantische Interpretation siehe [37, 52] oder auch Kapitel 6), $\mathrm{FG}(\Gamma)$ durch die Menge

$$\mathrm{IRR}(\Gamma) = \{r(w) \mid w \in (\Gamma \cup \Gamma^{-1})^*\}$$

der reduzierten Wörter zu repräsentieren, um darin die Relationen von $\mathcal{C}(\Gamma)$ durch MSO-definierbare Relationen in $(\Gamma \cup \Gamma^{-1})^*$ zu beschreiben. Genauer möchten wir für jede MSO-Formel φ über der Signatur von $\mathcal{C}(\Gamma)$ effektiv eine MSO-Formel $\hat{\varphi}$ über der Signatur von T_Γ konstruieren so, dass

$$\mathcal{C}(\Gamma) \models \varphi \text{ genau dann wenn } T_\Gamma \models \hat{\varphi}.$$

Durch Darstellung der Signatur von $\mathcal{C}(\Gamma)$ durch MSO-definierbare Relationen der Signatur von T_Γ kann dann $\hat{\varphi}$ auf natürliche Weise induktiv aus φ definiert werden.

Für ein $a \in \Gamma \cup \Gamma^{-1}$ sei $\mathrm{IRR}(\Gamma)_a$ die Menge der irreduziblen Wörter, die nicht mit einem a enden.

Bemerkung 2.4.1 *Offenbar ist $\mathcal{C}(\Gamma)$ isomorph zu folgender Struktur:*

$$(\mathrm{IRR}(\Gamma), (\{(u, ua) \mid u \in \mathrm{IRR}(\Gamma)_{a^{-1}}\} \cup \{(ua^{-1}, u) \mid u \in \mathrm{IRR}(\Gamma)_a\})_{a \in \Gamma \cup \Gamma^{-1}}, \epsilon)$$

Nun ist $\mathrm{IRR}(\Gamma)$ eine reguläre Teilmenge von $(\Gamma \cup \Gamma^{-1})^*$ und damit wegen Theorem 2.4.2 MSO-definierbar in T_Γ, letztlich also $\mathcal{C}(\Gamma)$ in T_Γ MSO-definierbar.

Ist nun eine Formel φ über der Signatur von $\mathcal{C}(\Gamma)$ gegeben, so erhält man $\hat{\varphi}$ durch Relativieren aller Quantoren auf die Menge $\mathrm{IRR}(\Gamma)$ und durch Ersetzen aller Terme, die Relationen aus $\mathcal{C}(\Gamma)$ enthalten, durch entsprechende Terme mit Relationen

aus $((\{(u, ua) \mid u \in \mathrm{IRR}(\Gamma)_{a^{-1}}\} \cup \{(ua^{-1}, u) \mid u \in \mathrm{IRR}(\Gamma)_a\})_{a \in \Gamma \cup \Gamma^{-1}}, \epsilon)$ also solchen aus T_Γ. Dies ist möglich da mit Bemerkung 2.4.1 die Relationen in $\mathcal{C}(\Gamma)$ als Relationen in T_Γ MSO-definiert werden können.

Wir erhalten zusammen mit Rabins Baumthorem 2.4.3:

Theorem 2.4.4 ([42]) *Für jede endliche Menge Γ ist die MSO-Theorie des Cayleygraphen der freien Gruppe, $\mathrm{MSOTh}(\mathcal{C}(\Gamma))$, entscheidbar.*

Theorem 2.4.4 ist ein wichtiges Hilfsmittel zum Beweis weiterer Entscheidbarkeitsresultate (hier in Kapitel 4 und 6). Jedoch ist die Komplexität der MSO-Theorie $\mathrm{MSOTh}(\mathcal{C}(\Gamma))$ nicht elementar (jeder Algorithmus, der $\mathrm{MSOTh}(\mathcal{C}(\Gamma))$ entscheidet ist nicht elementar, also nicht durch einen Exponenten-Turm fester Höhe beschränkt), da bereits die MSO-Theorie der Struktur $(\mathbb{Z}, +)$ (relationale Struktur mit Nachfolger-Funktion und der Menge der ganzen Zahlen $\mathbb{Z}$ als Grundmenge) nicht elementar ist [40].

2.5 Automaten und Komplexität

Wir wiederholen hier kurz die wichtigsten Begriffe und verweisen an entsprechender Stelle auf weiterführende Literatur. Zur Definition von Zeitschranken und Platzschranken, sowie zu weiteren Begriffen der Komplexitätstheorie siehe etwa [45, 53]. Wir verwenden den Ausdruck „in Linearzeit“ synonym für „in Linearzeit auf einer RAM“. Eine RAM (Registermaschine) kann auf einer Turingmaschine simuliert werden, wobei jedoch ein logarithmischer Faktor in der Laufzeit hinzukommt.

Eine alternierende Turingmaschine (siehe [12]) ist eine nicht-deterministische Turingmaschine T mit zwei Arten von Zuständen:

- existentielle Zustände ($Q_\exists$) und
- universelle Zustände ($Q_\forall$).

Genauer ist

$$T = (Q, \Sigma, \delta, q_0, q_f)$$

mit Zustandsmenge Q, wobei $Q = Q_\exists \cup Q_\forall \cup \{q_f\}$ disjunkte Vereinigung, Bandalphabet Σ, Übergangsfunktion δ sowie Anfangszustand q_0 und Endzustand q_f. Wir können annehmen, dass T keine Übergänge aus dem Endzustand q_f heraus machen kann.

Eine Konfiguration C von T im Zustand q heißt akzeptierend, wenn

- $q = q_f$, oder
- $q \in Q_\exists$ und es gibt eine akzeptierende Nachfolgekonfiguration von C oder
- $q \in Q_\forall$ und alle Nachfolgekonfigurationen von C sind akzeptierend.

Ein Eingabewort wird von T akzeptiert, wenn die entsprechende Anfangskonfiguration akzeptierend ist. Die Klasse aller Probleme, die von einer alternierenden Turingmaschine mit polynomiellem Platz akzeptiert werden, APSPACE, ist gleich der Klasse alle in exponentieller Zeit lösbaren Probleme, EXPTIME, (siehe [12]).

2.6 Das Wortproblem

Eines der klassischen algebraischen Probleme ist das Wortproblem, die Frage, ob zwei Wörter in einer gegebenen algebraischen Struktur das gleiche Element repräsentieren. Sei M ein beliebiges Monoid mit Erzeugermenge Σ, sei $h : \Sigma^* \to M$ der kanonische surjektive Homomorphismus.

Das Wortproblem (WP) für M bezüglich der Erzeugermenge Σ ist das folgende Problem:

(WP) EINGABE: Zwei Wörter $u, v \in \Sigma^*$.
AUSGABE: Ist $u = v$ in M? (Das heißt, gilt $h(u) = h(v)$?)

Wie auch die Entscheidbarkeit (Komplexität) von FO-Logik und MSO-Logik über der Signatur eines Cayleygraphen $\mathcal{C}(M, \Sigma)$ unabhängig von der Erzeugermenge Σ des Monoids M ist (Satz 2.2.3), gilt dies auch für das Wortproblem, weswegen wir im Folgenden von dem Wortproblem für ein Monoid M, unabhängig von der Erzeugermenge Σ sprechen:

Satz 2.6.1 *Sei M ein endlich erzeugtes Monoid mit Erzeugermengen Σ_1 bzw. Σ_2. Dann ist das Wortproblem von M bezüglich Σ_1 mit logarithmischen Platz auf das Wortproblem von M bezüglich Σ_2.*

Beweis: Sei $\Sigma_1 = \{a_1, \ldots, a_n\} \subseteq M$ und $\Sigma_2 = \{b_1, \ldots, b_m\} \subseteq M$. Dann gibt es für alle b_j (da Σ_1 Erzeugermenge) $a_{i_1}, \ldots, a_{i_j}$ mit $b_j = a_{i_1} \cdots a_{i_j}$ in M, weswegen alle Wörter in Σ_2 als solche in Σ_1 mit ebendieser Darstellung aufgefasst werden können. □

Das Wortproblem geht zurück auf Dehn, der dieses Problem 1911 formulierte. Im Allgemeinen ist das Wortproblem für endlich präsentierte Monoide (Markov [39], Post [48]) und Gruppen (Boone [8], Novikov [44]) unentscheidbar.

Lipton und Zalcstein [32] erweiterten ein Resultat von Rabin und zeigten, dass das Wortproblem für Matrixgruppen (und Halbgruppen) über Körpern mit Charakteristik 0 in logarithmischen Platz entscheidbar ist. Da freie Gruppen in Matrixgruppen über $\mathbb{Q}$ eingebettet werden können, folgt, dass das Wortproblem für freie Gruppen in logarithmischen Platz lösbar ist. Weitere Ergebnisse finden sich zum Beispiel in [64, 70].

Offenbar folgt aus der Entscheidbarkeit der FO-Theorie des Cayleygraphen eines Monoids M auch die Entscheidbarkeit des Wortproblems von M. Auf der anderen Seite gibt es endlich präsentierte Monoide mit entscheidbarem Wortproblem aber unentscheidbarer FO-Theorie, siehe [30]. Im besonderen Fall der Gruppe ist jedoch das Wortproblem einer endlich präsentierten Gruppe genau dann entscheidbar, wenn der Cayleygraph der Gruppe entscheidbare FO-Theorie hat, siehe [29].

In der kombinatorischen Gruppentheorie [24] ist man ferner daran interessiert, ob zwei Untergruppen einer Gruppe gleich sind, mit anderen Worten, ob alle Untergruppenelemente der einen Gruppe in der anderen enthalten sind. Kann man dieses Problem lösen, so kann man durch die Frage ob uv^{-1} in der von der 1 der Gruppe erzeugten Untergruppe liegt, auch das Wortproblem für diese Gruppe entscheiden. Dies motiviert das verallgemeinerte Wortproblem (generalized word problem – (GWP)), diese Notation aus der Gruppentheorie wurde für Monoide übernommen [7]. Sei M ein Monoid mit Erzeugermenge Σ und $h : \Sigma^* \to M$ der kanonische surjektive Homomorphismus. Wir definieren das verallgemeinerte Wortproblem von M bezüglich Σ:

(GWP)	EINGABE:	Wörter $u, u_1, \ldots, u_n \in \Sigma^*$.
	AUSGABE:	Liegt $h(u)$ in dem von $h(u_1), \ldots, h(u_n)$ erzeugten Untermonoid von M?

Das Problem (WP) lässt sich von (GWP) strikt trennen, so gibt es Gruppen (hyperbolische Gruppen, siehe [21]) mit entscheidbarem Wortproblem (das Wortproblem jeder hyperbolischen Gruppe ist entscheidbar [21]) aber unentscheidbarem verallgemeinerten Wortproblem (es gibt eine hyperbolische Gruppe, für welche (GWP) unentscheidbar ist [54]).

Wir werden uns mit dem Wortproblem und dem verallgemeinerten Wortproblem von inversen Monoiden mit idempotener Präsentation $\mathrm{FIM}(\Gamma)/P$ beschäftigen. Für solche Monoide folgt mit Lemma 3.5.3 aus der Entscheidbarkeit des verallgemeinerten Wortproblems die Entscheidbarkeit des Wortproblems. Ein allgemeines Resultat in dieser Form ist uns nicht bekannt.

Kapitel 3

Inverse Monoide

3.1 Definitionen

Wir geben hier diejenigen Grundbegriffe an, die wir im Weiteren benötigen. Eine umfassende Darstellung inverser Monoide sowie deren Verbindung zu anderen Teilen der Mathematik findet sich etwa in den Büchern [31] und [46].

Es gibt eine Reihe äquivalenter Definitionen inverser Monoide. Eine, oft verwendete, charakterisiert frei inverse Monoide über Vagner-Gleichungen. Seien u, v Wörter in $(\Gamma \cup \Gamma^{-1})^*$, die Gleichungen

$$\begin{aligned} u &= uu^{-1}u \\ uu^{-1}vv^{-1} &= vv^{-1}uu^{-1} \end{aligned} \tag{3.1}$$

werden als Vagner-Gleichungen bezeichnet.

Die Klasse der inversen Monoide bildet eine Varietät von Algebren (bezüglich der Operationen Multiplikation, Inversenbildung und Auswahl der Identität), darin existieren freie Objekte – frei inverse Monoide. Das frei inverse Monoid mit Erzeugermenge Γ (als inverses Monoid) bezeichnen wir mit FIM(Γ).

Sei σ_c die kleinste Kongruenz, die die Vagner-Gleichungen erfüllt. Das frei inverse Monoid FIM(Γ) ist isomorph zu $(\Gamma \cup \Gamma^{-1})^*/\sigma_c$. Wir bezeichnen mit σ den kanonischen surjektiven Homomorphismus $\sigma : (\Gamma \cup \Gamma^{-1})^* \to \mathrm{FIM}(\Gamma)$. Weitere Charakterisierungen frei inverser Monoide findet man etwa in [56]. Von Scheiblich [55] wurde eine Konstruktion vorgestellt, die Inspiration für viele fortführende Darstellung (so auch diejenige, mit der wir hier arbeiten) war. Alle diese Ergebnisse

zielen auf die Anwendbarkeit auf bestimmte Problemstellungen ab. In [47] stellen Poliakova und Schein eine Darstellung vor, die Verallgemeinerung der bisherigen Konstruktionen sein soll.

Zur Lösung des Wortproblems für FIM(Γ) wurde von Munn [43] eine alternative Konstruktion frei inverser Monoide angegeben. Diese stellt die Elemente von FIM(Γ) als endliche Teilgraphen des Cayleygraphen $\mathcal{C}(\Gamma)$ der freien Gruppe (Munnbäume) dar.

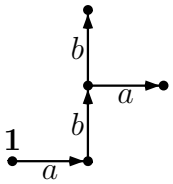
Genauer sei u ein Wort in $(\Gamma \cup \Gamma^{-1})^*$. Wir definieren den Munnbaum, MT(u) von u:

$$\mathrm{MT}(u) = \{\gamma(v) \in \mathrm{FG}(\Gamma) \mid \exists w \in (\Gamma \cup \Gamma^{-1})^* : u = vw\}.$$

Wir können $\mathrm{MT}(u)$ als Teilbaum von $\mathcal{C}(\Gamma)$, der alle Knoten aus $\mathrm{MT}(u)$ enthält auffassen. Mit anderen Worten, $\mathrm{MT}(u)$ ist der endliche, zusammenhängende Teilgraph des Cayleygraphen $\mathcal{C}(\Gamma)$, der sämtliche Knoten von $\mathcal{C}(\Gamma)$ enthält, die auf dem Pfad, der in der 1 der freien Gruppe startet und bis zum Element $\gamma(u)$ läuft, liegen.

Es vereinfacht die Notation, sowohl den Teilbaum von $\mathcal{C}(\Gamma)$ als auch die Menge der entsprechende Knoten der freien Gruppe als Munnbaum zu bezeichnen. Da aus dem Zusammenhang stets klar sein wird, welche Struktur gemeint ist, werden wir dies beibehalten.

Beispiel 3.1.1 *Sei $u = abaa^{-1}bb^{-1}b^{-1}$, dann ist der Munnbaum $\mathrm{MT}(u)$ von u der folgende Baum:*



Mit $r(u)$ bezeichnen wir die reduzierte Form von u, also dasjenige Wort $v \in (\Gamma \cup \Gamma^{-1})^*$ mit $v = r(v) = r(u)$, welches keine Teilwörter der Form aa^{-1} bzw. $a^{-1}a$ für $a \in \Gamma$ enthält. Das reduzierte Wort $r(u)$ kann aus dem Wort u in linearer Zeit berechnet werden [6]. Offenbar (und dies wird im weiteren wichtig sein) sind für zwei Wörter $u, v \in (\Gamma \cup \Gamma^{-1})^*$ die reduzierten Wörter $r(v)$ und $r(u)$ genau dann gleich, wenn $\gamma(v) = \gamma(u)$. Dies rechtfertigt die Notation $r(u)$ im entsprechenden Kontext auch als Element in $\mathrm{FG}(\Gamma)$ aufzufassen. Im Beispiel 3.1.1 ist $r(u) = a$.

Das folgende Theorem von Munn [43] impliziert die Entscheidbarkeit des Wortproblems (siehe Abschnitt 2.6) für frei inverse Monoide.

Theorem 3.1.1 (Munn's Theorem, [43]) *Seien $u, v \in (\Gamma \cup \Gamma^{-1})^*$. Dann ist*

$$\sigma(u) = \sigma(v) \text{ genau dann, wenn } \mathrm{MT}(u) = \mathrm{MT}(v) \text{ und } \gamma(u) = \gamma(v).$$

Damit kann jedes Element aus FIM(Γ) durch ein Tupel $(\mathrm{MT}(u), \gamma(u))$ dargestellt werden. Ist T ein endlicher zusammenhängender Teilbaum von $\mathcal{C}(\Gamma)$, der die $1 \in \mathrm{FG}(\Gamma)$ enthält und $g \in \mathrm{FG}(\Gamma)$ ebenfalls in T, so gibt es ein $u \in (\Gamma \cup \Gamma^{-1})^*$ (eigentlich unendlich viele) so, dass $(\mathrm{MT}(u), \gamma(u)) = (T, g)$. Wir identifizieren deshalb das Monoid FIM(Γ) mit der Menge $\{(\mathrm{MT}(u), \gamma(u)) \mid u \in (\Gamma \cup \Gamma^{-1})^*\}$ und der auf dieser Menge gegebenen Multiplikation:

$$(\mathrm{MT}(u), \gamma(u))(\mathrm{MT}(v), \gamma(v)) = (\mathrm{MT}(u) \cup \gamma(u)\mathrm{MT}(u), \gamma(uv)),$$

wobei $\gamma(u)\mathrm{MT}(u) = \{\gamma(u)g \mid g \in \mathrm{MT}(u)\}$ mit Multiplikation in FG(Γ) und uv Konkatenation in $(\Gamma \cup \Gamma^{-1})^*$.

3.2 E-unitäre inverse Monoide und $\mathrm{FIM}(\Gamma)/P$

Ein Element $e \in M$ heißt Idempotent, falls $e^2 = e$ in M. Die Menge der Idempotente eines Monoids M bezeichnen wir mit $E(M)$. Die zweite Vagner-Gleichung (3.1) impliziert, dass die Idempotente in inversen Monoiden kommutieren.

Die folgenden Definitionen motivieren die spezielle Klasse der hier betrachteten inversen Monoide.

Sei M ein Monoid, eine Kongruenz $\rho \subseteq M \times M$ heißt Gruppenkongruenz, falls M/ρ eine Gruppe ist.

Lemma 3.2.1 *Sei M ein inverses Monoid. Eine Kongruenz $\rho \subseteq M \times M$ ist genau dann eine Gruppenkongruenz, wenn für alle $e, f \in E(M)$ gilt: $(e, f) \in \rho$.*

Beweis: Offenbar ist ein inverses Monoid M genau dann eine Gruppe, wenn M genau ein Idempotent enthält. (Ist M eine Gruppe so folgt aus $m^2 = m$ schon $m = 1$, also enthält M nur ein Idempotent. Ist umgekehrt $m \in M$ und $m^{-1} \in M$ das (eindeutige) Element mit $m = mm^{-1}m$ und $m^{-1} = m^{-1}mm^{-1}$, dann ist, weil $1 \in M$ das einzige Idempotent und mm^{-1} sowie $m^{-1}m$ idempotent, $mm^{-1} = 1 = m^{-1}m$.)

Auf der anderen Seite besitzt M/ρ genau dann genau eine idempotente ρ-Klasse (genau ein idempotentes Element), wenn alle Idempotente von M in einer ρ-Klasse liegen. Denn: jede idempotente ρ-Klasse in M/ρ enthält auch ein Idempotent aus M. Genauer, ist $(m, m^2) \in \rho$ und sei m' das eindeutige Inverse von m^2, so ist $e = mm'm$ das gesuchte Idempotent. □

Weiterhin kann man zeigen, dass der Schnitt von Gruppenkongruenzen wieder eine solche ist. Mit anderen Worten, es gibt eine minimale Gruppenkongruenz (der Schnitt aller Gruppenkongruenzen). Diese hat eine große Bedeutung bei der Betrachtung inverser Monoide. Hilfreicher ist jedoch die folgende Charakterisierung dieser Kongruenz. Wir bezeichnen mit $\leq$ die natürliche partielle Ordnung auf einem inversen Monoid M:

$$m \leq m' :\Leftrightarrow m = em'$$

für $m, m' \in M$ und ein Idempotent $e \in M$.

Lemma 3.2.2 *Die von $\leq$ induzierte Kongruenz $\iota_{c,M}$ (bzw. ι_c, falls M klar ist) auf M ist die minimale Gruppenkongruenz auf M. Genauer ist*

$$\iota_c = \{(m, m') \in M \times M \mid \exists n \in M : \ n \leq m, n \leq m'\}.$$

Die Gruppe M/ι_c heißt das maximal zu einer Gruppe homomorphe Bild von M.

Beweis: Es ist leicht zu zeigen, dass ι_c ein Äquivalenzrelation ist. Seien $e, f \in E(M)$. Da Idempotente kommutieren ist $efe = eff$ und damit ist per Definition von ι_c (weil $ef \in E(M)$ und damit $e'e = e'f$ für ein Idempotent e') $(e, f) \in \iota_c$. Wegen Lemma 3.2.1 ist M/ι_c eine Gruppe.

Wir müssen nun noch zeigen, dass ι_c minimal ist. Sei dazu ρ eine Gruppenkongruenz auf M und seien $(m_1, m_2) \in \iota_c$, es gibt also ein $e \in E(M)$ mit $em_1 = em_2$ in M, Gleichheit gilt dann offenbar auch für die entsprechenden ρ-Klassen: $(\rho e)(\rho m_1) = (\rho e)(\rho m_2)$. Nun ist S/ρ ein Gruppe, das einzige Idempotent (ρe) also die Identität und damit $(\rho m_1) = (\rho m_2)$, also $(m_1, m_2) \in \rho$ und $\iota_c \subseteq \rho$. □

Offenbar ist $\mathrm{FIM}(\Gamma)/\iota_c \cong \mathrm{FG}(\Gamma)$.

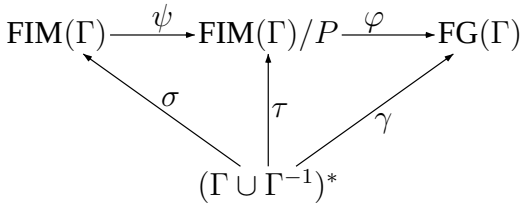
Sei M ein Monoid. M heißt E-unitär, falls für alle $m \in M$ mit $(m, e) \in \iota_c$ für ein $e \in E(M)$ gilt $m \in E(M)$. Es gibt eine Reihe von äquivalenten Beschreibungen für E-unitäre Monoide [46], wir werden an entsprechender Stelle die jeweils benötigte einführen. Aus den Resultaten von Munn folgt sofort, dass $\mathrm{FIM}(\Gamma)$ E-unitär ist.

Sei M ein Monoid mit Erzeugermenge Σ und $h : \Sigma^* \to M$ der kanonische surjektive Homomorphismus. Wir nennen eine endliche Menge $P \subseteq \Sigma^* \times \Sigma^*$ (endlich) idempotente Präsentation, wenn für alle $(e, f) \in P$ gilt, dass e und f Idempotente in M sind ($h(e)^2 = h(e)$ bzw. $h(f)^2 = h(f)$).

Sei P eine endlich idempotente Präsentation. Wir definieren

$$\mathrm{FIM}(\Gamma)/P = (\Gamma \cup \Gamma^{-1})^*/\tau_c,$$

wobei τ_c die kleinste Kongruenz ist, welche die Vagner-Gleichungen und P erfüllt. Wir bezeichnen im Weiteren den kanonischen Homomorphismus $(\Gamma \cup \Gamma^{-1})^* \to \mathrm{FIM}(\Gamma)/P$ mit τ. Insgesamt werden von nun an die Abbildungen zwischen den Monoiden wie folgt bezeichnet:



Wir beschäftigen uns speziell mit inversen Monoide der Form $\mathrm{FIM}(\Gamma)/P$, mit endlich idempotenter Präsentation P. Spezialfall dieser Klasse ist das frei inverse Monoid $\mathrm{FIM}(\Gamma)$ (falls $P = \emptyset$), ein weiterer Spezialfall ist $P = \{(e_i, 1) \mid i \in I\}$ für eine endliche Indexmenge I. Auf der anderen Seite wissen wir mit Lemma 3.2.1, dass falls für alle Idempotente e, f gilt $(e, f) \in P$ (unendliche Präsentation), das Monoid $\mathrm{FIM}(\Gamma)/P$ schon eine Gruppe ist.

Zur Verallgemeinerung des Resultats von Munn auf inverse Monoide $\mathrm{FIM}(\Gamma)/P$ mit idempotenter Präsentation P nutzen Margolis und Meakin [37] Vorarbeiten von Stephen [63] und erweitern die Idee der Munnbäume auf $\mathrm{FIM}(\Gamma)/P$. Wir geben in den nächsten Abschnitten eine Verallgemeinerung dieser Konstruktion wieder.

3.3 Eine allgemeine Konstruktion gewisser inverser Monoide

Zu jeder (unendlichen) Gruppe G, können wir ein inverses Monoid $\mathrm{IM}(G)$ auf folgende Weise konstruieren. Die Elemente von $\mathrm{IM}(G))$ sind

$$\mathrm{IM}(G) \quad = \quad \{(U, g) \mid U \subseteq G \text{ endlich}, \ 1, g \in U\}.$$

Die Multiplikation wird definiert durch

$$(U, g)(V, g') = (U \cup gV, gg').$$

Satz 3.3.1 ([36]) *Sei G eine Gruppe, dann ist $\mathrm{IM}(G)$ ein E-unitäres inverses Monoid mit maximal gruppenhomomorphen Bild G.*

Beweis: Die Assoziativität ist leicht nachzurechnen, ebenso die Vagner-Gleichungen mit $(U,g)^{-1} = (g^{-1}U, g^{-1})$. Neutrales Element ist $(\{1\}, 1)$.

Man zeigt leicht: Ein Monoid M ist E-unitär, falls für alle $m, m' \in M$ gilt ist $mm' = m$, dann ist $m' \in E(M)$. Nun sind Idempotente in $\mathrm{IM}(G))$ von der Form $(U, 1)$ und es ist

$$(U,g)(U',g) = (U \cup gU', gg') = (U,g),$$

dann muss $g' = 1$ sein. Damit ist $\mathrm{IM}(G))$ E-unitär.

Für die minimale Gruppenkongruenz ι_c gilt:

$$\begin{aligned}((U,g),(U',g')) \in \iota_c \quad \Leftrightarrow \quad & \exists \text{ Idempotent } (E,1): \\ & (E,1)(U,g) = (E,1)(U',g) \\ & \Leftrightarrow (E \cup U, g) = (E \cup U', g').\end{aligned}$$

Damit bildet $\iota : \mathrm{IM}(G) \to \mathrm{IM}(G)/\iota_c$ jedes (U,g) auf g ab und G ist maximal gruppenhomomorphes Bild von $\mathrm{IM}(G)$. □

Die obige Konstruktion folgt einer Konstruktion inverser Monoide die von Birget und Rhodes [3, 4] angegeben wurde.

Margolis und Meakin ([36, 37] verlangen in einer ähnlichen Konstruktion, dass U eine endliche, zusammenhängende Teilmenge des Cayleygraphen von G ist. Das erhaltene inverse Monoid ist abhängig von der Erzeugermenge Γ der Gruppe G. Wir bezeichnen dieses Monoid mit $\mathrm{IM}(\Gamma, G)$.

Bemerkung 3.3.1 *Sei $G = \mathrm{FG}(\Gamma)$ eine freie Gruppe. Betrachten wir nur Knotenmengen, die zusammenhängende Teilgraphen in $\mathcal{C}(\Gamma)$ bilden (Munnbäume), dann besagt Munns Theorem (3.1.1):*

$$\mathrm{IM}(\Gamma, G) = \mathrm{FIM}(\Gamma).$$

3.4 Idempotente Gleichungen in $\mathrm{IM}(G)$

Sei G eine unendliche, virtuell freie Gruppe.

Wir betrachten eine endliche Menge P idempotenter Gleichungen der Form

$$(E, 1) = (E', 1),$$

in $\mathrm{IM}(G)$ mit $E \subseteq E'$ (Wir können $E \subseteq E'$ annehmen, da die Gleichung $(E, 1) = (E', 1)$ offenbar äquivalent zu den beiden Gleichungen $(E, 1) = (E, 1)(E', 1)$ und $(E', 1) = (E, 1)(E', 1)$ ist). Wir sind interessiert am Quotientenmonoid

$$\mathrm{IM}(G)/_{\cong_P},$$

wobei $\cong_P$ die kleinste von P erzeugte Kongruenz ist. Wir schreiben im Weiteren statt $\mathrm{IM}(G)/_{\cong_P}$ einfach $\mathrm{IM}(G)/P$.

Offenbar impliziert $((U, g), (V, h)) \in \cong_P$, dass $g = h$ in G.

Wir definieren nun den Abschluss $\mathrm{cl}_P(V)$ einer Menge $V \subseteq G$ durch entsprechende Ersetzungsregeln. Hierbei notieren wir

$$U \underset{P}{\Rightarrow} V,$$

falls es für ein $p \in G$ ein $((E, 1), (E', 1))$ in P gibt, mit $pE \subseteq U$ und $V = U \cup pE'$.

Bemerkung 3.4.1 *Ist $U \underset{P}{\Rightarrow} V$ dann ist auch $((U, g), (V, g)) \in \cong_P$, für ein $g \in G$. Ist umgekehrt $(E, 1) = (E', 1)$ in P und $(U, g) = (X, p)(E, 1)(Y, y)$ sowie $(V, g) = (X, p)(E', 1)(Y, y)$, dann gilt $U = X \cup gE \cup gY$ und insbesondere $gE \subseteq U$. Weiterhin ist $V = U \cup gE'$ und damit $U \underset{P}{\Rightarrow} V$.*

Mit anderen Worten, ist $\overset{*}{\underset{P}{\Leftrightarrow}}$ der reflexive, symmetrische und transitive Abschluss von $\underset{P}{\Rightarrow}$, dann gilt für alle (U, g), (V, h) aus $\mathrm{IM}(G)$:

$$((U, g), (V, h)) \in \cong_P \text{ genau dann wenn } U \overset{*}{\underset{P}{\Leftrightarrow}} V \text{ und } g = h.$$

Falls $U \overset{*}{\underset{P}{\Rightarrow}} U'$ dann ist $(U \cup V) \overset{*}{\underset{P}{\Rightarrow}} U' \cup V$ für ein $V \subseteq G$. Ferner ist die Relation $\underset{P}{\Rightarrow}$ stark konfluent [1], mehr noch ist $V \underset{P}{\Rightarrow} U$ und $V \underset{P}{\Rightarrow} W$ dann gilt $U \underset{P}{\Rightarrow} U \cup W$ und $W \underset{P}{\Rightarrow} U \cup W$.

Wegen der Konfluenzeigenschaft [1] gilt für $U, V \subseteq G$ dass $U \overset{*}{\underset{P}{\Leftrightarrow}} V$ genau dann, wenn $U \overset{*}{\underset{P}{\Rightarrow}} W$ und $V \overset{*}{\underset{P}{\Rightarrow}} W$ für ein $W \subseteq G$.

Mit diesen Bemerkungen ist die Bildung des Abschlusses einer Menge U bezüglich P, definiert durch

$$\mathrm{cl}_P(U) = \bigcup \{W \mid U \overset{*}{\underset{P}{\Rightarrow}} W\},$$

wohldefiniert.

Es gilt die folgende Verallgemeinerung eines Theorems von Margolis und Meakin [37]:

Theorem 3.4.1 *Sei G eine unendliche Gruppe und $M = \mathrm{IM}(G)$. Sei P eine endlich idempotente Präsentation mit $E \subseteq E'$ für alle $((E,1),(E',1)) \in P$. Seien ferner $U, V \subseteq G$, $g, h \in G$. Dann sind äquivalent:*

(1) $(U, g) = (V, h)$ *in* M/P,

(2) $\mathrm{cl}_P(U) = \mathrm{cl}_P(V)$ *und* $g = h$,

(3) $U \subseteq \mathrm{cl}_P(V)$, $V \subseteq \mathrm{cl}_P(U)$ *und* $g = h$.

Beweis: Um die Richtung (1) nach (2) zu zeigen sei $(U, g) = (V, h)$ in M/P. Zunächst ist offenbar (siehe vorher) $g = h$ in G. Wegen Bemerkung 3.4.1 gilt zudem $U \overset{*}{\underset{P}{\Rightarrow}} W$ und $V \overset{*}{\underset{P}{\Rightarrow}} W$ für ein $W \subseteq G$ mit $U \cup V \subseteq W$.

Nun folgt wegen $U \overset{*}{\underset{P}{\Rightarrow}} W$ schon $\mathrm{cl}_P(W) \subseteq \mathrm{cl}_P(U)$ und ebenso gilt wegen $V \overset{*}{\underset{P}{\Rightarrow}} W$ schon $\mathrm{cl}_P(W) \subseteq \mathrm{cl}_P(V)$. Schließlich folgt aus $U \cup V \subseteq W$, dass $\mathrm{cl}_P(U) \subseteq \mathrm{cl}_P(W)$ und $\mathrm{cl}_P(V) \subseteq \mathrm{cl}_P(W)$.

Insgesamt also $\mathrm{cl}_P(U) = \mathrm{cl}_P(W) = \mathrm{cl}_P(V)$.

Die Richtung von (2) nach (3) ist trivial, da $U \subseteq \mathrm{cl}_P(U)$ und $V \subseteq \mathrm{cl}_P(V)$.

Bleibt noch zu zeigen, dass aus (3) die Aussage (1) folgt. Wähle dazu W_1 und W_2 so das $U \overset{*}{\underset{P}{\Rightarrow}} W_1$ mit $V \subseteq W_1$ und analog $V \overset{*}{\underset{P}{\Rightarrow}} W_2$ mit $U \subseteq W_2$.

Damit erhalten wir $W_1 \overset{*}{\underset{P}{\Rightarrow}} W_1 \cup W_2$ und $W_2 \overset{*}{\underset{P}{\Rightarrow}} W_1 \cup W_2$. Deswegen gilt insbesondere $U \overset{*}{\underset{P}{\Rightarrow}} W_1 \cup W_2$ und $V \overset{*}{\underset{P}{\Rightarrow}} W_1 \cup W_2$ und damit $(U, g) = (V, g)$ in M/P und wegen $g = h$ schließlich $(U, g) = (V, h)$ in M/P. □

Lemma 3.4.1 *Sei G eine unendliche Gruppe und $U, U' \subseteq G$. Dann ist $U \overset{*}{\underset{P}{\Leftrightarrow}} U'$ äquivalent zu den folgenden zwei Bedingungen:*

(1) $\exists V : U \overset{*}{\underset{P}{\Rightarrow}} V$ *und* $U' \subseteq V$ *und*

(2) $\exists V' : U' \overset{*}{\underset{P}{\Rightarrow}} V'$ *und* $U \subseteq V'$.

Beweis: Ist $U \overset{*}{\underset{P}{\Leftrightarrow}} U'$ dann gilt offenbar (1). Aussage (2) kann positiv mit $V = V'$, wobei $U \overset{*}{\underset{P}{\Rightarrow}} V$ und $U' \overset{*}{\underset{P}{\Rightarrow}} V$ beantwortet werden.

Umgekehrt sind (1) und (2) wahr mit V und V', dann ist $U \overset{*}{\underset{P}{\Rightarrow}} V \overset{*}{\underset{P}{\Rightarrow}} V \cup V'$ weil $U' \subseteq V$. Aus Symmetriegründen gilt $U' \overset{*}{\underset{P}{\Rightarrow}} V' \overset{*}{\underset{P}{\Rightarrow}} V \cup V'$ und damit $U \overset{*}{\underset{P}{\Leftrightarrow}} U'$. $\square$

Bemerkung 3.4.2 *Ist U zusammenhängende Teilmenge des Cayleygraphen $\mathcal{C}(G, \Gamma)$ und $1, g \in U$ für alle $(U, g) \in \mathrm{IM}(\Gamma, G)$ wird $\mathrm{IM}(\Gamma, G)$ erzeugt von den Elementen $(\{1, a\}, a)$ für alle $a \in \Gamma \cup \Gamma^{-1}$. Ist Γ endlich, so ist deshalb $\mathrm{IM}(\Gamma, G)$ endlich erzeugt. Dies ist im Allgemeinen für $\mathrm{IM}(G)$ nicht der Fall, da G unendlich ist. Sind nämlich $(U_i, g_i) \in \mathrm{IM}(G)$ endlich viele Elemente und ist g weder 1 noch eines der g_i, so kann $(\{1, g\}, g)$ nicht als Produkt in den (U_i, g_i) geschrieben werden.*

Eine Zentrale Rolle in dieser Arbeit spielt das schon von Margolis und Meakin [37] betrachtete inverse Monoid $\mathrm{FIM}(\Gamma)/P = \mathrm{IM}(\Gamma, \mathrm{FG}(\Gamma))/P$, mit endlich idempotenter Präsentation P, welches im nächsten Abschnitt ausführlicher dargestellt werden soll.

3.5 Das inverse Monoid $\mathrm{FIM}(\Gamma)/P$

Ist P wiederum eine Menge von Paaren (e, e'), wobei $e, e' \in \mathrm{IM}(\Gamma, G)$ idempotent sind, dann definiert $\mathrm{IM}(\Gamma \cup \Gamma^{-1}, G)/P$ ein weiteres Quotientenmonoid. Hierbei definiert die Inklusion $\mathrm{IM}(\Gamma, G) \subseteq \mathrm{IM}(G)$ eine kanonische Einbettung

$$\mathrm{IM}(\Gamma, G) \to \mathrm{IM}(G).$$

Seien E, E' endliche, zusammenhängende Teilmengen von G mit $1 \in E, E'$. Angenommen es ist $(U, f) = (X, g)(E, 1)(Y, h)$ wobei U zusammenhängend ist, dann folgt aus $U = X \cup gE \cup gY$, dass $g \in U$ und deshalb ist $U' = X \cup gE' \cup gY$ ebenfalls zusammenhängend. Das heißt, das Wortproblem von $\mathrm{IM}(\Gamma, G)/P$ kann reduziert werden auf das Wortproblem von $\mathrm{IM}(G)/P$.

Bemerkung 3.5.1 *Margolis und Meakin [37] beweisen Theorem 3.4.1 für den Spezialfall $M = \mathrm{FIM}(\Gamma)/P$. Ist I eine endliche Menge und*

$$P = \{(e_i, f_i) \mid i \in I\} \subseteq (\Gamma \cup \Gamma^{-1})^* \times (\Gamma \cup \Gamma^{-1})^*$$

eine idempotente Präsentation (wir können, wie oben, eine idempotente Präsentation P für die für alle $(e, f) \in P$ gilt $\mathrm{MT}(e) \subseteq \mathrm{MT}(f)$ annehmen) und sind $u, v \in (\Gamma \cup \Gamma^{-1})^*$, dann ist

$$u = v \text{ in } M \quad \text{genau dann, wenn} \quad \mathrm{cl}_P(\mathrm{MT}(u)) = \mathrm{cl}_P(\mathrm{MT}(v)) \text{ und } \gamma(u) = \gamma(v).$$

Man beachte, dass, da die Munnbäume $\mathrm{MT}(e)$, $\mathrm{MT}(f)$ und $\mathrm{MT}(u)$ zusammenhängend sind, auch $\mathrm{cl}_P(\mathrm{MT}(u))$ zusammenhängend ist.

Offenbar ist die Gleichung $\mathrm{cl}_P(\mathrm{MT}(u)) = \mathrm{cl}_P(\mathrm{MT}(v))$ äquivalent zu $\mathrm{MT}(u) \subseteq \mathrm{cl}_P(\mathrm{MT}(v)) \wedge \mathrm{MT}(v) \subseteq \mathrm{cl}_P(\mathrm{MT}(u))$.

Margolis und Meakin [37] nutzen Rabins Baumtheorem 2.4.4 um die Entscheidbarkeit des Wortproblems von $\mathrm{FIM}(\Gamma)/P$, für $P = \{(e_i, f_i) \mid i \in I\}$, I endlich, zu zeigen. Hierzu ist es notwendig, den Abschluss $\mathrm{cl}_P(V)$ einer Knotenmenge V in eine MSO-Formel über $\mathcal{C}(\Gamma)$ zu übersetzen. Da wir diese Formel (auch im allgemeineren Kontext der Signatur des Cayleygraphen der virtuell freien Gruppe) ebenso verwenden, geben wir sie hier an. Eine virtuell freie Gruppe meint hier und im Folgenden stets eine endlich erzeugte Gruppe mit einer nicht-trivialen freien Untergruppe von endlichem Index.

Lemma 3.5.1 *Sei G eine (endlich erzeugte) virtuell freie Gruppe, sei $\mathcal{C}$ der Cayleygraph von G und seien $V, X \subseteq G$. Ferner sei P eine endlich idempotente Präsentation in $\mathrm{IM}(G)$, wobei für alle $((E, 1), (E', 1)) \in P$ mit $E, E' \subseteq G$ gilt $E \subseteq E'$. Dann gibt es eine Formel $\mathrm{CL}_P(X, Y)$ über der Signatur von $\mathcal{C}$ mit $\mathcal{C} \models \mathrm{CL}_P(V, X)$, genau dann, wenn gilt $X = \mathrm{cl}_P(V)$.*

Beweis: Offenbar ist der Abschluss der Knotenmenge V bezüglich P die kleinste Menge $\mathrm{cl}_P(V)$, die V selbst enthält und die für alle $(e, e') := ((E, 1), (E', 1)) \in P$ und $v \in \mathrm{cl}_P(V)$ mit $vE \subseteq \mathrm{cl}_P(V)$ auch vE' enthält. Letzteres wird durch die Formel

$$\mathrm{cl}(V, X) := (V \subseteq X) \wedge \bigwedge_{(e,e') \in P} \forall v : \ (vE \subseteq X \Rightarrow vE' \subseteq X)$$

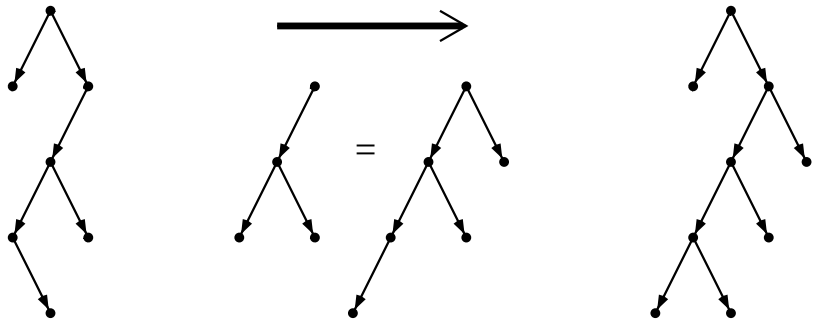
ausgedrückt. Insgesamt erhalten wir die Formel:

$$\mathrm{CL}_P(V, X) := \mathrm{cl}(V, X) \wedge \forall Z : \ (\mathrm{cl}(V, Z) \Rightarrow X \subseteq Z).$$

Mit anderen Worten $\mathcal{C} \models \mathrm{CL}_P(V, X)$ genau dann, wenn X der Abschluss von V in $\mathcal{C}$ ist. □ Seien hier alle Bezeichnungen wir in Bemerkung 3.5.1. Wir befassen uns mit Munnbäumen, also mit zusammenhängenden Teilbäumen des Cayleygraphen von $\mathrm{FG}(\Gamma)$.

Graphisch dargestellt ist jeder Ersetzungsschritt einfach das Ersetzen eines Teilbaums durch einen weiteren.

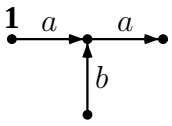
Bemerkung 3.5.2 *In jedem Ersetzungsschritt wird im bisher gebildeten Baum (ein Teilbaum des Cayleygraphen der entsprechenden freien Gruppe) ein neuer Teilbaum* $\mathrm{MT}(e)$ *gesucht und durch einen anderen Teilbaum* $\mathrm{MT}(f)$ *mit* $(e, f) \in P$ *ersetzt:*



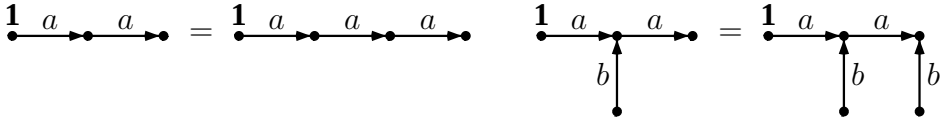
In der graphischen Darstellung von Munnbäumen behalten wir die Darstellung wie in Beispiel 3.1.1 bei. Die $1 \in \mathrm{FG}(\Gamma)$ wird dabei durch den Knoten $\mathbf{1}\bullet$ repräsentiert. Sofern erforderlich stehen die Erzeuger auf den Kanten, die Elemente neben den Knoten.

Das folgende Beispiel demonstriert den Abschluss eines Munnbaums.

Beispiel 3.5.2 *Sei* $\Gamma = \{a, b\}$ *und* $u = ab^{-1}baa^{-1}$. *Der Munnbaum von* u *ist folgender Graph*

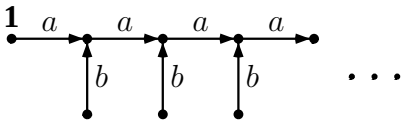


Sei ferner $P = \{(a^2a^{-2}, a^3a^{-3}), (a^2a^{-1}b^{-1}ba^{-1}, a^2b^{-1}ba^{-1}b^{-1}ba^{-1})\}$ *eine idempotente Präsentation. In Darstellung als Munnbäume sehen die Gleichungen aus* P *wie folgt aus:*



Wir erhalten den Abschluss des Munnbaums von u*:*

$$\mathrm{cl}_P(\mathrm{MT}(u)) = \{1\} \cup \{a^n \mid n \geq 1\} \cup \{a^n b^{-1} \mid n \geq 1\} :$$



Bemerkung 3.5.3 *Mit Bemerkung 3.5.1 folgt, dass* $\mathrm{FIM}(\Gamma)/P$ *E-unitär ist.*

Sei ι die minimale Gruppenkongruenz (Lemma 3.2.1). Alle E-unitäre inverse Monoide M erfüllen damit die Voraussetzungen des nachfolgenden Lemmas, falls $G = M/\iota$ torsionsfrei ist.

Lemma 3.5.3 *Sei* M *ein Monoid mit Erzeugermenge* Σ *und* $h : M \to G$ *ein Homomorphismus in eine torsionsfreie Gruppe* G *mit* $h^{-1}(1) = E(M)$*. Seien ferner* $u, v \in \Sigma^*$*. Dann gilt:*

$$\begin{aligned} u = v \text{ in } M \quad \Leftrightarrow \quad & u \in \{v^i \mid i \geq 0\} \text{ in } M \text{ und} \\ & v \in \{u^i \mid i \geq 0\} \text{ in } M \end{aligned}$$

Beweis: Die eine Richtung gilt trivialerweise, für die andere sei $u = v^m$ und $v = u^n$ in M für $m, n \geq 0$.

Falls $m = 0$, dann ist $u = 1$ und wegen $v = u^n$ auch $v = 1$ und damit $u = v$ in M.

Falls $m = 1$ ist ebenso $u = v$ in M. Analoges gilt für n.

Seien also $m, n > 1$. Dann ist $u^{mn} = u$ in M und weil h Homomorphismus ist, ist auch $u^{mn} = u$ in G und daher $u^{mn-1} = 1$ in G. Wegen $m, n > 1$ und G torsionsfrei ist daher $u = 1$ in G.

Daher ist wegen $h^{-1}(1) = E(M)$ das Element u ein Idempotent in M und wir erhalten $v = u^n = u$ in M, da $n > 1$. □

Kapitel 4

Die Komplexität des Wortproblems für $\mathrm{FIM}(\Gamma)/P$

Margolis und Meakin [37] nutzen in ihrem Beweis der Entscheidbarkeit des Wortproblems für inverse Monoide mit idempotenter Präsentation Rabins Baumtheorem. In [2, 37] wird die Frage nach einer besseren Komplexitätsschranke gestellt. Wir beweisen in diesem Kapitel, dass das Wortproblem für inverse Monoide $\mathrm{FIM}(\Gamma)/P$ in Linearzeit gelöst werden kann, das uniforme Wortproblem für diese Klasse von Monoiden jedoch EXPTIME-vollständig ist.

4.1 Das Wortproblem für $\mathrm{FIM}(\Gamma)/P$

Wir beweisen zunächst, dass das Wortproblem für $\mathrm{FIM}(\Gamma)/P$ in Polynomialzeit gelöst werden kann. In Theorem 4.1.1 modifizieren wir dann den angegebenen Algorithmus auf einen Linearzeitalgorithmus.

Satz 4.1.1 *Das Wortproblem für inverse Monoide $\mathrm{FIM}(\Gamma)/P$ mit endlicher idempotenter Präsentation kann in Polynomialzeit gelöst werden.*

Beweis: Das Wortproblem wird zunächst in eine MSO-Formel über der Signatur von T_Γ und schließlich darüber in einen Baumautomaten übersetzt. Dazu nutzen wir die Hilfsmittel aus Abschnitt 2.4.

Wegen Bemerkung 3.5.1 genügt es zu zeigen, dass für zwei Wörter $u, v \in (\Gamma \cup \Gamma^{-1})^*$ die Eigenschaften $\mathrm{MT}(u) \subseteq \mathrm{cl}_P(\mathrm{MT}(v))$ und $\gamma(u) = \gamma(v)$ in Polynomialzeit getestet werden kann. Das Wortproblem für $\mathrm{FG}(\Gamma)$ kann in Linearzeit gelöst werden [6], mit anderen Worten die Frage $\gamma(u) = \gamma(v)$ kann in Linearzeit entschieden werden und wir müssen zeigen, dass $\mathrm{MT}(u) \subseteq \mathrm{cl}_P(\mathrm{MT}(v))$ in Polynomialzeit entschieden werden kann.

Wegen Lemma 3.5.1 gibt es eine MSO-Formel $\mathrm{CL}_P(X, Y)$ über der Signatur von $\mathcal{C}(\Gamma)$ mit

$$\mathcal{C}(\Gamma) \models \mathrm{CL}_P(\mathrm{MT}(u), A) \text{ genau dann wenn } A = \mathrm{cl}_P(\mathrm{MT}(u)),$$

für alle Teilmengen $A \subseteq \mathrm{FG}(\Gamma)$. Die Eigenschaft $\mathrm{MT}(u) \subseteq \mathrm{cl}_P(\mathrm{MT}(v))$ kann damit in MSO über $\mathcal{C}(\Gamma)$ durch die Formel in-$\mathrm{cl}_P(X, Y)$ mit

$$\text{in-cl}_P(X, Y) := \exists Z : \mathrm{CL}_P(X, Z) \wedge Y \subseteq Z$$

beschrieben werden, genauer müssen wir deshalb zeigen, dass

$$\mathcal{C}(\Gamma) \models \text{in-cl}_P(\mathrm{MT}(u), \mathrm{MT}(v))$$

in Polynomialzeit entschieden werden kann.

Nun wenden wir die Ergebnisse aus Abschnitt 2.4 an. Zunächst repräsentiere die Menge U die Knoten des Munnbaums $\mathrm{MT}(u)$ in $(\Gamma \cup \Gamma^{-1})^*$, genauer sei

$$U = \{r(s) \mid \exists w \in (\Gamma \cup \Gamma^{-1})^* : u = sw\}.$$

Wegen Abschnitt 2.4 gibt es eine Formel $\psi_P(X, Y)$ über der Signatur von T_Γ mit $T_\Gamma \models \psi_P(U, V)$ genau dann wenn $\mathcal{C}(\Gamma) \models \text{in-cl}_P(\gamma(U), \gamma(V))$. Wir müssen nun zeigen, dass $T_\Gamma \models \psi_P(U, V)$ in Polynomialzeit getestet werden kann.

Dazu übersetzen wir die feste Formel (da P fest) $\psi_P(X, Y)$ in einen festen (top-down) ω-Baumautomaten $\mathcal{A}_P$. Dies geht mit Theorem 2.4.2 (zur genauen Konstruktion des Automats siehe Beweis dieses Theorem in [50].) Dieser Automat läuft auf einem mit Kantenmarkierung $\lambda : (\Gamma \cup \Gamma^{-1})^* \to \{0, 1\} \times \{0, 1\}$ versehenen ω-Baum (T_Γ, λ).

Wir erhalten einen Automat $\mathcal{A}_P$ mit $T_\Gamma \models \psi_P(U, V)$ genau dann, wenn $\mathcal{A}_P$, den ω-Baum

$$T_{U,V} = (T_\Gamma, \lambda) \text{ mit } \lambda(w) = (i, j)$$

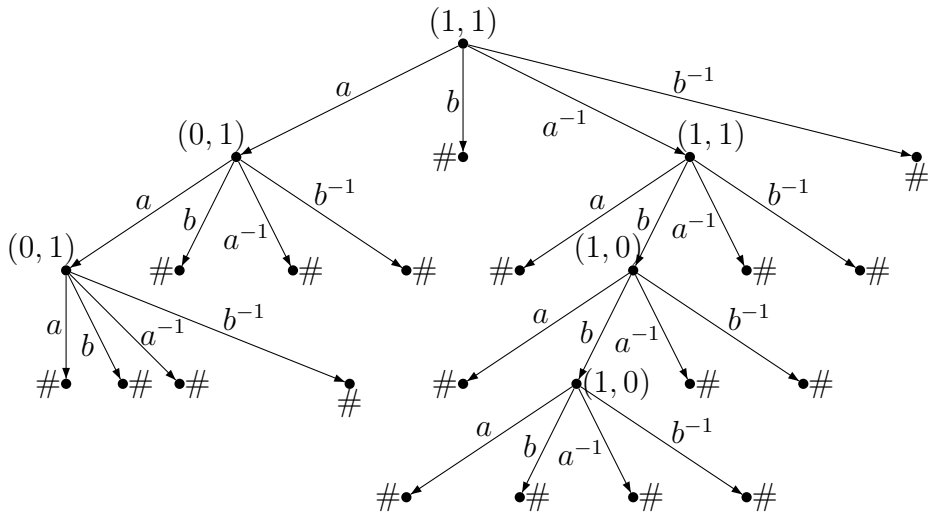
akzeptiert. Wobei $i = 1$ genau wenn $w \in U$ und $j = 1$ genau wenn $w \in V$, für alle $w \in (\Gamma \cup \Gamma^{-1})^*$.

Da $\psi_P(X, Y)$ eine feste MSO-Formel ist, ist auch $\mathcal{A}_P$ ein fester ω-Baumautomat.

Im letzten Schritt übersetzen wir $T_{U,V}$ in einen endlichen Baum. Die Idee ist, durch Streichen von Knoten, die nichts zum Erkennen beitragen einen endlichen Baum zu erhalten. Die Mengen U und V sind endlich, weshalb fast alle Knoten in $T_{U,V}$ Knotenmarkierung $(0, 0)$ ($(1, 0)$ nur, falls $w \in U$ und $(0, 1)$, nur, falls $w \in V$) haben.

Sei nun $B \in (\Gamma \cup \Gamma^{-1})^*$ die Menge aller Wörter der Form wa mit $w \in (\Gamma \cup \Gamma^{-1})^*$, $a \in \Gamma \cup \Gamma^{-1}$, $\lambda(wat) = (0, 0)$ für alle $t \in (\Gamma \cup \Gamma^{-1})^*$, jedoch $\lambda(w) \neq (0, 0)$.

Wir konstruieren einen endlichen Baum $T^{\text{fin}}_{U,V}$ aus dem unendlichen Baum $T_{U,V}$, indem wir jeden Knoten $w \in B$ zu einem Blatt mit Knotenmarkierung $\#$ machen. Hier ein Beispiel dieser Konstruktion. Sei $V = \{\varepsilon, a, aa, a^{-1}\}$ und $U = \{\epsilon, a^{-1}, a^{-1}b, a^{-1}bb\}$. Dann ist $T^{\text{fin}}_{U,V}$ der folgende endliche Baum:



Der Baum $T^{\text{fin}}_{U,V}$ ist endlich und kann aus U und V in polynomieller Zeit berechnet werden. Da der ω-Baumautomat $\mathcal{A}_P$ fest ist, können wir daraus einen festen Baumautomat $\mathcal{A}^{\text{fin}}_P$ konstruieren, der einen endlichen Baum $T^{\text{fin}}_{U,V}$ genau dann akzeptiert, wenn $\mathcal{A}_P$ den Baum $T_{U,V}$ akzeptiert.

Diese Konstruktion übernimmt im Wesentlichen alle Zustände und Übergänge des Baumautomats $\mathcal{A}_P$, mit der Ausnahme, dass der Automat $\mathcal{A}^{\text{fin}}_P$ genau dann in einem Blatt eines endlichen Baums im Zustand q akzeptiert, wenn $\mathcal{A}_P$, in Zustand q startend, den kompletten ω-Baum mit allen Knoten mit Knotenmarkierung $(0, 0)$ akzeptiert.

Da in polynomieller Zeit getestet werden kann, ob $\mathcal{A}^{\text{fin}}_P$ den Baum $T^{\text{fin}}_{U,V}$ akzeptiert folgt damit die Behauptung. □

Theorem 4.1.1 *Das Wortproblem für inverse Monoide $\mathrm{FIM}(\Gamma)/P$ mit endlich idempotenter Präsentation kann in Linearzeit gelöst werden.*

Beweis: Wir werden zeigen, dass der Algorithmus aus Satz 4.1.1 in Linearzeit durchgeführt werden kann. Zunächst bemerken wir, dass eine Zeigerdarstellung von $T^{\mathrm{fin}}_{U,V}$ in Linearzeit aus den Wörtern u und v konstruiert werden kann. Ferner benötigen wir den folgenden Standardalgorithmus für eine Zeigerdarstellung von $\mathrm{MT}(u)$:

$k := 1$; $c := 1$;
for all $a \in \Gamma \cup \Gamma^{-1}$: out$(1, a) :=$ nil;
for $i := 1$ to $|u|$ do
  if out$(c, u[i]) \neq$ nil then
    $c :=$ out$(c, u[i])$
  else
    $k := k + 1$;
    out$(c, u[i]) := k$;
    out$(k, u[i]^{-1}) := c$;
    for all $a \in (\Gamma \cup \Gamma^{-1}) \setminus \{u[i]^{-1}\}$: out$(k, a) :=$ nil;
    $c := k$
  endif
endfor

Im Algorithmus wird das Wort u einmal von links nach rechts abgelaufen, um den Munnbaum $\mathrm{MT}(u)$ aufzubauen. Dabei werden die Knoten des Baums mit Zahlen $\{1, \ldots, \ell\}$ durchnummeriert, hierbei ist ℓ der Wert der Variable k am Ende eines Laufes des Algorithmus.

In k wird der maximale bisher erzeugte Knoten gespeichert, die Variable c speichert den derzeitig bearbeiteten Knoten des Munnbaums (im bislang erzeugten Munnbaum). Ferner speichern wir in out(j, a) für jeden Knoten j denjenigen Knoten, der von j über eine mit a markierte Kante erreicht werden kann; dieser Knoten kann nil sein. Die lineare Laufzeit des Algorithmus folgt sofort.

Nach Ablauf des Algorithmus setzen wir den derzeitigen Knoten c auf die Wurzel 1 und lassen (ohne Veränderung der anderen globalen Variablen) den gleichen Algorithmus mit dem Wort v statt u laufen. Dies liefert offenbar eine Zeigerdarstellung von $\mathrm{MT}(u) \cup \mathrm{MT}(v)$.

Schließlich fügen wir für jeden Knoten $1 \leq i \leq k$ und jedes $a \in \Gamma \subseteq \Gamma^{-1}$ so, dass entweder out$(i, a) =$ nil (ein Blatt) oder out$(i, a) < i$ (auch ein Blatt im

ungerichteten Baum, die mit a markierte Kante aus i führt in den Baum zurück) einen neuen Knoten j ein und setzen out$(i, a) := j$. Damit erhalten wir eine Zeigerdarstellung von $T^{\text{fin}}_{U,V}$.

Schließlich bemerken wir, dass der Baumautomat $\mathcal{A}^{\text{fin}}_P$ in Linearzeit auf der Zeigerdarstellung von $T^{\text{fin}}_{U,V}$ ausgewertet werden kann. Dies liefert die gesuchte Darstellung eines Linearzeitalgorithmus für das Wortproblem für $\mathrm{FIM}(\Gamma)/P$.

□

4.2 Der uniforme Fall

Im Gegensatz zu (WP) ist beim uniformen Wortproblem (UWP) die Präsentation P nicht fest, sondern Teil der Eingabe. Dies führt zu einer höheren Komplexität. Genauer definieren wir (UWP) wie folgt

(UWP)	EINGABE:	Eine idempotente Präsentation P und zwei Wörter $u, v \in (\Gamma \cup \Gamma^{-1})^*$.
	AUSGABE:	Ist u = v in $\mathrm{FIM}(\Gamma)/P$?

Wir benötigen für die Betrachtung des uniformen Wortproblems einige Grundkenntnisse des modalen μ-Kalküls, siehe etwa [65], die wir hier kurz zitieren. Der modale μ-Kalkül ist eine Logik über einem (mit Elementen aus einer Menge Σ kantenmarkierten) gerichteten Graph $G = (V, (E_a)_{a\in\Sigma})$; die Grundstruktur des μ-Kalküls.

Sei $G = (V, (E_a)_{a\in\Sigma})$ ein kantenmarkierter gerichteter Graph, $\mathcal{V} : \mathsf{VAR} \to 2^V$ eine Interpretation der MSO-Variablen (Variablen zweiter Stufe) VAR. Die Abbildung $\mathcal{V}[X := U]$ sei die Auswertungsabbildung, genauer $\mathcal{V}[X := U] = U$ und $\mathcal{V}[X := U](Y) = \mathcal{V}(Y)$. Syntax (Formel φ) und Semantik (Menge $\|\varphi\|^G_{\mathcal{V}} \subseteq V$ von Knoten, die φ erfüllen) des modalen μ-Kalküls werden wie folgt definiert:

	Syntax	Semantik
$\varphi ::=$	true	$\|\|\text{true}\|\|^G_{\mathcal{V}} = V$
	$\|$false	$\|\|\text{false}\|\|^G_{\mathcal{V}} = \emptyset$
	$\|\varphi \wedge \psi$	$\|\|\varphi \wedge \psi\|\|^G_{\mathcal{V}} = \|\|\varphi\|\|^G_{\mathcal{V}} \cap \|\|\psi\|\|^G_{\nu}$
	$\|\varphi \vee \psi$	$\|\|\varphi \vee \psi\|\|^G_{\mathcal{V}} = \|\|\varphi\|\|^G_{\mathcal{V}} \cup \|\|\psi\|\|^G_{\nu}$
	$\|\langle a\rangle\varphi$	$\|\|\langle a\rangle\varphi\|\|^G_{\mathcal{V}} = \{u \in V \mid \exists v \in V : (u,v) \in E_a$ und $v \in \|\|\varphi\|\|^G_{\mathcal{V}}\}$
	$\|[a]\varphi$	$\|\|[a]\varphi\|\|^G_{\mathcal{V}} = \{u \in V \mid \forall v \in V : (u,v) \in E_a \Rightarrow v \in \|\|\varphi\|\|^G_{\mathcal{V}}\}$
	$\|\mu X.\varphi$	$\|\|\mu X.\varphi\|\|^G_{\mathcal{V}} = \bigcap\{U \subseteq V \mid U \supseteq \|\|\varphi\|\|^G_{\mathcal{V}[X:=U]}\}$
	$\|\nu X.\varphi$	$\|\|\nu X.\varphi\|\|^G_{\mathcal{V}} = \bigcup\{U \subseteq V \mid U \subseteq \|\|\varphi\|\|^G_{\mathcal{V}[X:=U]}\}$

Mit anderen Worten, $\|\mu X.\varphi\|^G_{\mathcal{V}}$ ist der kleinste Fixpunkt der Abbildung

$$U \to \|\mu X.\varphi\|^G_{\mathcal{V}[X:=U]}$$

und $\|\nu X.\varphi\|^G_{\mathcal{V}}$ der größte Fixpunkt dieser Abbildung. Meist sind G und $\mathcal{V}$ aus dem Kontext klar (oder irrelevant, φ enthält keine freien Variablen), dann schreiben wir statt $\|\varphi\|^G_{\mathcal{V}}$ einfach $\|\varphi\|$. Ferner schreiben wir $s \models \varphi$, falls $s \in \|\varphi\|$.

Wir wollen ein Resultat für das Modelchecking Problem des modalen μ-Kalkül nutzen, um eine untere Schranke für (UWP) zu beweisen. Dieses Ergebnis gilt, falls die Grundstruktur ein (kantenmarkierter gerichteter) kontextfreier Graph ist. Ein kontextfreier Graph ist ein Transitionsgraph eines Kellerautomaten. Insbesondere ist der Cayleygraph $\mathcal{C}(\Gamma)$ der freien Gruppe FG(Γ), mit welchem wir hier arbeiten, kontextfrei (siehe [42]).

Theorem 4.2.1 ([28, 69]) *Das folgende Problem (Model-Checking Problem für den modalen μ-Kalkül) ist in EXPTIME.*

(MCH$_\mu$) *EINGABE:* *Ein Kellerautomat A, der einen kontextfreien Graph $G(A)$ definiert, ein Knoten $v \in G(A)$ und eine Formel φ des modalen μ-Kalküls.*
AUSGABE: *Gilt $v \models \varphi$?*

Mit diesem Theorem können wir folgendes Resultat beweisen.

Theorem 4.2.2 *Das uniforme Wortproblem für inverse Monoide* $\mathrm{FIM}(\Gamma)/P$ *mit endlich idempotenter Präsentation* P *ist EXPTIME-vollständig.*

Beweis: Seien $u, v \in (\Gamma \cup \Gamma^{-1})^*$. Um zu zeigen, dass u = v in $\mathrm{FIM}(\Gamma)/P$ in EXPTIME entscheidbar ist, genügt es (Bemerkung 3.5.1) zu zeigen, dass $\gamma(u) = \gamma(v)$ und $\mathrm{MT}(v) \subseteq \mathrm{cl}_P(\mathrm{MT}(u))$ in EXPTIME entscheidbar ist. Ersteres kann bereits in Linearzeit getestet werden, für Zweiteres übersetzen wir das Problem in eine Formel im μ-Kalkül des um einen Knoten und eine Kante erweiterten Cayleygraphen $\mathcal{C}(\Gamma)$ der freien Gruppe FG(Γ).

Genauer sei G derjenige Graph, der aus $\mathcal{C}(\Gamma)$ durch Hinzufügen eines Knotens und einer Kante von der $1 \in$ FG(Γ) zu diesem Knoten, die mit \$ markiert ist, entsteht. Da $\mathcal{C}(\Gamma)$ kontextfrei, ist auch G ein kontextfreier Graph. Können wir nun $\mathrm{MT}(u) \subseteq \mathrm{cl}_P(\mathrm{MT}(v))$ in eine Formel des modalen μ-Kalküls übersetzen, so folgt mit Theorem 4.2.1, dass (UWP) in EXPTIME ist.

Zur Übersetzung in den modalen μ-Kalkül sei $P = \{(e_i, f_i) \mid i \in I\}$ eine idempotente Präsentation mit $\mathrm{MT}(e_i) \subseteq \mathrm{MT}(f_i)$ und I endlich. Ferner sei für ein Wort $w = a_1 \cdots a_n$ mit $a_i \in \Gamma \cup \Gamma^{-1}$ und zwei Positionen i, j das Teilwort $w[i,j] = a_i \cdots a_j$, falls $i \leq j$ und $w[i,j] = \epsilon$ andernfalls. Wir verwenden $\langle w \rangle \varphi$ als Abkürzung für $\langle a_1 \rangle \langle a_2 \rangle \cdots \langle a_m \rangle \varphi$.

Wir formulieren zunächst eine Formel $\varphi_{u,P}$, die den Abschluss $\mathrm{cl}_P(MT(u))$ beschreibt, also $\|\varphi_{u,P}\| = \mathrm{cl}_P(MT(u))$. Dann ist $x \models \varphi_{u,P}$ genau dann, wenn x in $\mathrm{cl}_P(\mathrm{MT}(u))$ liegt. Es ist

$$\| \bigvee_{i=0}^{|u|} \langle u[1,i]^{-1} \rangle \langle \$ \rangle \mathrm{true} \| = \mathrm{MT}(u).$$

Wir drücken damit aus, dass $\mathrm{MT}(v) \subseteq \mathrm{cl}_P(\mathrm{MT}(u))$.

Um den Abschluss $\mathrm{cl}_P(\mathrm{MT}(u))$ zu formulieren verwenden wir den $\langle - \rangle$-Operator (oder auch den $[-]$-Operator, beides ist im Cayleygraph der freien Gruppe äquivalent). Der vordere Teil der Formel $\varphi_{u,P}$ stellt sicher, dass $\mathrm{MT}(u) \subseteq \mathrm{cl}_P(\mathrm{MT}(u))$.

$$\varphi_{u,P} := \mu X. \left(\bigvee_{i=0}^{|u|} \langle u[1,i]^{-1} \rangle \langle \$ \rangle \mathrm{true} \ \vee \ \bigvee_{i \in I} \bigvee_{j=0}^{|f_i|} \langle f_i[1,j]^{-1} \rangle (\bigwedge_{k=0}^{|e_i|} \langle e_i[1,k] \rangle X) \right).$$

Man beachte, dass μX den kleinsten Fixpunkt bestimmt.

Nun bleibt noch zu formulieren, dass $\mathrm{MT}(v) \subseteq \mathrm{cl}_P(\mathrm{MT}(u))$, genauer sei $\varphi_{v,u,P}$ die folgende Formel:

$$\bigwedge_{i=0}^{|v|} \langle v[1,i] \rangle \varphi_{u,P}.$$

Dann ist $\|\varphi_{v,u,P}\| = \{x : \ x, xv_1, xv_1v_2 \dots xv_1 \dots v_{|v|} \in \mathrm{cl}_P(\mathrm{MT}(u))\}$ und damit offenbar $1 \models \varphi_{v,u,P}$ genau dann wenn $\mathrm{MT}(v) \subseteq \mathrm{cl}_P(\mathrm{MT}(u))$.

Um zu zeigen, dass (UWP) EXPTIME-schwer ist, nutzen wir, dass EXPTIME gleich APSPACE, die Klasse aller Probleme, die mit polynomieller Platz von einer alternierenden Turingmaschine erkannt werden.

Sei $T = (Q, \Sigma, \delta, q_0, q_f)$ eine alternierende Turingmaschine, die eine EXPTIME-vollständige Sprache erkennt, wobei $Q = Q_\forall \cup Q_\exists \cup \{q_f\}$, disjunkte Vereinigung. Wir können ohne Beschränkung folgende Annahmen treffen:

- $q_0 \in Q_\exists$.
- Es gibt keinen Übergang aus q_f heraus.
- T wechselt in jedem Schritt von $Q_\forall$ nach $Q_\exists \cup \{q_f\}$ oder von $Q_\exists$ nach $Q_\forall \cup \{q_f\}$.
- In jedem Schritt hat T, entsprechend δ genau 2 Möglichkeiten (Wahl 1 bzw. Wahl 2).
- Das Zeichen, welches unter dem Kopf von T beim Übergang in den Endzustand q_f auf dem Band steht, sei $\$$.

Im Folgenden konstruieren wir ein inverses Monoid $\mathrm{FIM}(\Gamma)/P$ mit idempotenter Präsentation P, sowie Wörter $u, v \in (\Gamma \cup \Gamma^{-1})^*$ so, dass ein Wort $w \in \Sigma^*$ genau dann von T erkannt wird, wenn $u = v$ in $\mathrm{FIM}(\Gamma)/P$. Dazu codieren wir eine Konfiguration von T zunächst in ein Wort über dem Alphabet $\Gamma \cup \Gamma^{-1}$ und schließlich in einen Munnbaum. Sei dazu

$$\Gamma = \Sigma \cup (Q \times \Sigma) \cup \{a_1, a_2, b_1, b_2, \#\},$$

disjunkte Vereinigung.

Eine Konfiguration c von T ist ein Tupel

$$(w_l, (q, a), w_r),$$

mit $w_l, w_r \in \Sigma^*$, $a \in \Sigma$ und $q \in Q$.

Wir fassen c als ein Wort der Form $\#\Sigma^*(Q \times \Sigma)\Sigma^*\#$ in Γ^* auf. Wobei w_l in das erste Σ^* nach dem $\#$ codiert wird, w_r in das entsprechend letzte. Ist also $w \in \Sigma^*$ ein Eingabewort und m der Platz (polynomiell abhängig von der Länge von w), den T benötigt, um w abzuarbeiten, so ist eine Konfiguration von T während der Abarbeitung von w ein Wort aus der Menge

$$\bigcup_{i=0}^{m-1} \#\Sigma^i(Q \times \Sigma)\Sigma^{m-i-1}\# \subseteq \Gamma^{m+2}.$$

Die Übergänge von T sollen nun als Wortersetzungen in Γ angegeben werden.

Offenbar hängt eine Konfiguration $c = (w_l x, (q, a), y w_r)$, mit $x, y \in \Sigma$, zum Zeitpunkt t lediglich von den Konfigurationen $c_l = (w_l, (q', x'), a y w_r)$ und $c_r = (w_l x a, (q'', y'), w_r)$ zum Zeitpunkt $t-1$ ab. So übersetzen wir einen Übergang wie folgt:

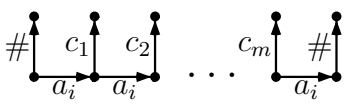
Wir schreiben $c_1c_2c_3 \xrightarrow{j} c$, $j \in \{1, 2\}$, falls drei aufeinander folgende Zeichen einer Konfiguration aus $\bigcup_{i=0}^{m-1} \#\Sigma^i(Q \times \Sigma)\Sigma^{m-i-1}\# \subseteq \Gamma^{m+2}$ die Sequenz $c_1c_2c_3$ an den Positionen $i-1, i, i+1$ beinhalten und nach Übergang von T mit Wahl j an der Position i ein c steht.

Wir schreiben $c_1c_2c_3 \xrightarrow{\exists} (d_1, d_2)$ für $c_1, c_2, c_3, d_1, d_2 \in \Sigma^* \cup (Q \times \Sigma) \cup \{\#\}$ falls einer der folgenden Fälle gilt:

- $c_1c_2c_3 \in \{\varepsilon, \#\}\Sigma^*(Q_\exists \times \Sigma)\Sigma^*\{\varepsilon, \#\}$, und $c_1c_2c_3 \xrightarrow{j} d_j$ für $j \in \{1, 2\}$
- $c_1c_2c_3 \in \{\varepsilon, \#\}\Sigma^*\{\varepsilon, \#\}$ und $d_1 = d_2 = c_2$.

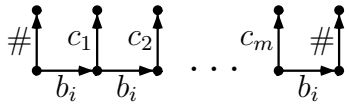
Analog schreiben wir $c_1c_2c_3 \xrightarrow{\forall} (d_1, d_2)$, falls einer der beiden obigen Fälle gilt, wobei im ersten Punkt $Q_\exists$ durch $Q_\forall$ ersetzt wird.

Im zweiten Schritt codieren wir eine Konfiguration c in einen Munnbaum also in einen endlichen Teilgraphen von FG(Γ). Genauer, sei $c = \#c_1c_2\cdots c_m\# \in \Gamma^*$ und T befindet sich in einem Zustand aus $Q_\exists$, so soll der entsprechende Munnbaum wie folgt aussehen:



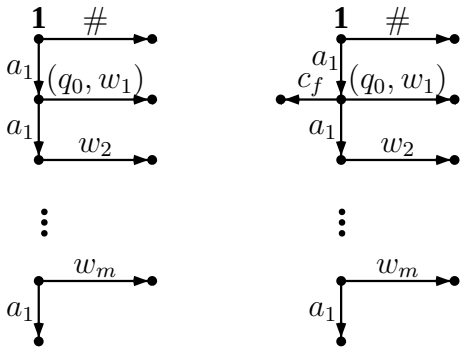
wobei $i \in \{1, 2\}$, je nach Wahl.

Befindet sich T in einem Zustand aus $Q_\forall$, so sieht der der Konfiguration $c = \#c_1c_2 \cdots c_m\# \in \Gamma^*$ zugeordnete Munnbaum genauso aus, lediglich die $a_i's$ werden durch Kantenmarkierungen b_i ersetzt:



Wir wollen erreichen, dass, um Gleichheit zweier Wörter in M zu überprüfen, der kompletter Berechnungsbaum von T aufgebaut werden muss. Sei dazu $w = w_1w_2 \cdots w_n$ mit $w_i \in \Sigma$ ein Eingabewort, welches T mit Platz $m = p(n)$ (für ein Polynom p) berechnet (wir setzen $w = w_1w_2 \cdots w_m$, mit $w_i = \square$, das Blanksymbol von T, für $i \in \{n + 1, \ldots, m\}$).

Zunächst geben wir die beiden Wörter u und v durch ihre Munnbäume an ($\sigma(u)$ und $\sigma(v)$ seien idempotent, also $r(u) = r(v) = \epsilon$):

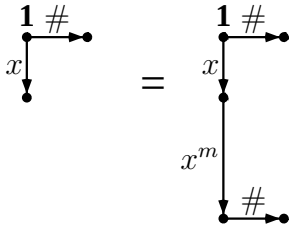


wobei $c_f = (q_f, \$)$. Der linke Baum sei der Munnbaum $\mathrm{MT}(u)$ von u, der rechte der Munnbaum von v.

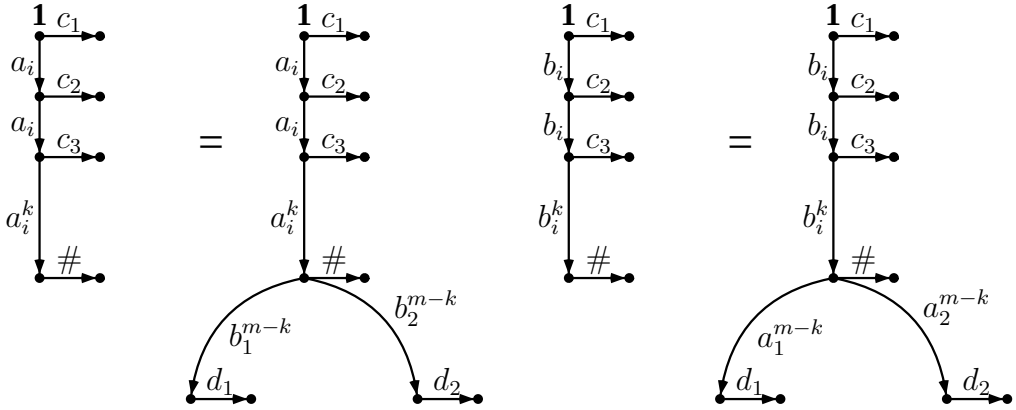
Um die mit $c_f = (q_f, \$)$ markierte Kante (im Abschluss des Munnbaums von u) zu erhalten (die einzige, durch die sich $\mathrm{MT}(u)$ und $\mathrm{MT}(v)$ unterscheiden) werden wir mit den im folgenden angegebenen Gleichungen für P erreichen, dass der komplette Berechnungsbaum von T für den Erhalt dieser Kante aufgebaut werden muss. Die Gleichungen in P spiegeln nun Übergänge der Turingmaschine T wider.

Sei zunächst $x \in \{a_1, a_2, b_1, b_2\}$. Wir geben die rechte und linke Seite von Gleichungen aus P jeweils durch die entsprechenden Munnbäume an (man beachte, dass $\mathrm{MT}(e) \subseteq \mathrm{MT}(f)$, der Munnbaum der linken Seite ein Teilbaum des Munnbaums der rechten Seite ist). Die reduzierten Wörter sind (da idempotent) alle gleich ϵ.

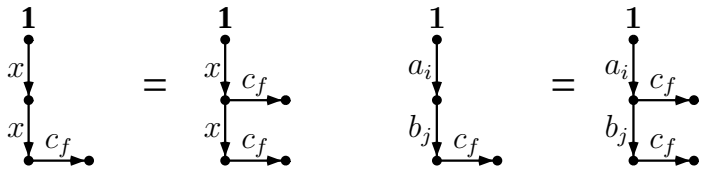
Folgende idempotente Gleichungen gehören zu P:



Für die Übergänge $c_1c_2c_3 \xrightarrow{\exists} (d_1, d_2)$ und $c_1c_2c_3 \xrightarrow{\forall} (d_1, d_2)$ sind für alle $0 \leq k \leq m-1$ folgende Gleichungen in P:

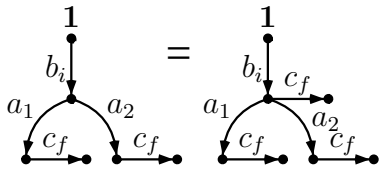


Schließlich benötigen wir noch Gleichungen, die dafür sorgen, dass die c_f-Kante, nachdem w akzeptiert wurde, auch im Abschluss des Munnbaums von u vorkommt. Dazu benötigen wir zunächst folgende Gleichungen:



wobei $i, j \in \{1, 2\}$ und $x \in \{a_1, a_2, b_1, b_2\}$. Wir erinnern, dass die a_i-Kanten zu den $\exists$-Zuständen korrespondieren. Für die b_i-Kanten benötigen wir entsprechend, dass man durch alle (beide) Wahlen ($Q_\forall$-Zustände) in einen Endzustand (symbolisiert durch c_f) gelangt.

Dies wird durch folgende Gleichungen sichergestellt:



Durch die Konstruktion haben wir nun erreicht, dass T ein Wort w akzeptiert genau dann, wenn $\mathrm{MT}(v) \subseteq \mathrm{cl}_P(\mathrm{MT}(u))$, wegen $\mathrm{MT}(u) \subseteq \mathrm{MT}(v)$ gilt schließlich $\mathrm{cl}_P(\mathrm{MT}(v)) = \mathrm{cl}_P(\mathrm{MT}(u))$ und damit folgt mit Bemerkung 3.5.1 die Behauptung.

□

Kapitel 5

Die Komplexität des Wortproblems für $\mathrm{IM}(G)/P$

In diesem Kapitel beweisen wir die Entscheidbarkeit des Wortproblems in Linearzeit für inverse Monoide $\mathrm{IM}(G)/P$ mit endlich idempotenter Präsentation P und virtuell freier Gruppe G. Im Gegensatz zum Beweis im Kapitel 4 erfolgt dieser Beweis direkt und ohne die Hilfe von Rabins Baumtheorem. Dadurch wird der Beweis etwas länger, wir können das Resultat aber auch gleich für eine größere Klasse inverser Monoide beweisen.

5.1 Virtuell freie Gruppen

In diesem Kapitel bezeichnen wir mit G eine unendliche, endlich erzeugte virtuell freie Gruppe. Mit anderen Worten, G besitzt eine endlich erzeugte nicht-triviale freie Untergruppe F von endlichem Index in G. Wir wählen eine endliche Teilmenge von G (wir bezeichnen diese von nun an mit H) so, dass $1 \in H$ und G als disjunkte Vereinigung

$$G = \bigcup_{h \in H} Fh$$

geschrieben werden kann. Sei Γ eine minimale Menge von Erzeugern der freien Gruppe F. Da die Menge der reduzierten Wörter aus $\Gamma \cup \Gamma^{-1}$ in 1–1-Beziehung mit F steht kann offenbar jedes Element von G eindeutig in der Form $\hat{u}h$, mit reduziertem $\hat{u} \in (\Gamma \cup \Gamma^{-1})^*$ und $h \in H$, geschrieben werden.

Es ist leicht zu sehen, dass diese Normalform in Linearzeit berechnet werden kann. Genauer berechnet man diese mit Hilfe eines endlichen vollständigen Termersetzungssystems über dem Alphabet $\Delta = \Gamma \cup \Gamma^{-1} \cup H$:

$$\begin{aligned} aa^{-1} &\rightarrow 1, \quad a \in \Gamma \cup \Gamma^{-1}, \\ ha &\rightarrow u(h,a)g(h,a), \quad h \in H, a \in \Gamma \cup \Gamma^{-1}, \\ hh' &\rightarrow u(h,h')g(h,h'), \quad h, h' \in H. \end{aligned}$$

Hierbei ist $u(h,a), u(h,h') \in (\Gamma \cup \Gamma^{-1})^*$ und $g(h,a), g(h,h') \in H$ ist so gewählt, dass $ha = u(h,a)g(h,a)$ und $hh' = u(h,h')g(h,h')$ in der Gruppe G gelten.

Ferner können wir die $1 \in H$ entweder (durch eine weitere Regel) mit dem leeren Wort identifizieren oder wir fassen die $1 \in H$ als einen ausgezeichneten Buchstaben von Δ auf und arbeiten über nichtleeren Wörtern aus Δ. Letztere Sichtweise ist für dieses Kapitel die geeignetere.

Lesen wir nun einen Eingabestring aus Δ, so beschreibt obiges System im Wesentlichen die Arbeit eines deterministischen Kellerautomaten. Man sieht damit schnell das bekannte Resultat der Lösbarkeit des Wortproblems für virtuell freie Gruppen G in Linearzeit. Dies ist der erste Punkt (siehe Theorem 3.4.1) zum Beweis der Existenz eines Linearzeitalgorithmus für die Entscheidbarkeit des Wortproblems für $\mathrm{IM}(G)/P$.

Im Folgenden ist die Gruppe G nicht Teil der Eingabe, weshalb wir die Größen von Δ und des obigen Ersetzungssystems als Konstanten auffassen können. Ist insbesondere $w \in \Delta^+$ ein Wort der Länge n, dann hat seine Normalform $\hat{u}h \in (\Gamma \cup \Gamma^{-1})^* H$ höchstens die Länge cn wobei c eine feste Konstante ist, die lediglich von G abhängt.

Wir stellen ein Element (U, g) aus $\mathrm{IM}(G)$ wie folgt dar (für den Linearzeit-Algorithmus): Gegeben wird das Paar (U, g) durch eine alternierende Sequenz

$$(a_1, b_1, \ldots, a_n, b_n),$$

mit $n \geq 1$, $a_i \in \Delta$, $b_i \in \{0, 1\}$ für $1 \leq i \leq n$. Wir lesen ein Wort aus Δ^* als ein Element von G und definieren dann $g = a_1 \cdots a_n$ und

$$U = \{a_1 \cdots a_i \mid b_i = 1, 1 \leq i \leq n\}.$$

Wir erinnern daran, dass U nicht notwendig zusammenhängend sein muss. Deswegen nutzen wir die Bits b_i. Damit wird aus dem Paar $(\{1\}, 1)$ aus $\mathrm{IM}(G)$ die Sequenz $(1, 1)$ wobei die linke $1 \in H$ ein Buchstabe aus Δ ist und die rechte $1 \in \{0, 1\}$ gerade das Bit, welches anzeigt, dass $1 \in H$ in der Sequenz liegt.

Die Darstellung einer Regel $(E, E') \in P$ erfolgt wieder durch eine Sequenz $(a_1, b_1, \ldots, a_n, b_n)$ hier mit $n \geq 1$, $a_i \in \Delta$, $b_i \in \{0, 1, 2\}$ für $1 \leq i \leq n$. Dazu definieren wir:

$$\begin{aligned} E &= \{a_1 \cdots a_i \mid b_i = 1, 1 \leq i \leq n\}, \\ E' &= \{a_1 \cdots a_i \mid b_i \geq 1, 1 \leq i \leq n\}. \end{aligned}$$

5.2 Ersetzungen über endlichen Teilmengen

Wegen Theorem 3.4.1, Lemma 3.4.1 und den Ausführungen im Abschnitt 5.1 genügt es zur Lösung des Wortproblems von $\mathrm{IM}(G)$ folgendes Problem zu betrachten: Sei P eine endliche Menge von Paaren (E, E') mit $E \subseteq E' \subseteq G$ und endlichen Mengen E, E'.

EINGABE: Zwei endliche Mengen $U, U' \subseteq G$.
AUSGABE: Gibt es ein $V \subseteq G$ so, dass $U \overset{*}{\underset{P}{\Rightarrow}} V$ und $U' \subseteq V$?

Wir benötigen ein weiteres Konzept, welches ein entscheidendes Hilfsmittel im Rest des Kapitels sein wird: Zu gegebener Teilmenge $W \subseteq G$ definieren wir die Ersetzungsrelation $\underset{P,W}{\Rightarrow}$ mit $U \underset{P,W}{\Rightarrow} U'$ für $U, U' \subseteq G$ falls es ein $g \in W$ und $(E, E') \in P$ gibt so, dass $gE \subseteq U$ und $U' = U \cup gE'$.

Wir verlangen nicht, dass $1 \in E$ oder $1 \in E'$ liegt, weswegen g auch außerhalb von U liegen kann.

Auch die Relation $\underset{P,W}{\Rightarrow}$ ist stark konfluent. Ist jedoch zudem die Menge W endlich, dann ist $\underset{P,W}{\Rightarrow}$ terminierend. Das heißt jede Kette $U \overset{*}{\underset{P,W}{\Rightarrow}} U_1 \overset{*}{\underset{P,W}{\Rightarrow}} U_2 \overset{*}{\underset{P,W}{\Rightarrow}} \cdots$ wird stationär. Dies ist klar, weil $U_1 \subseteq U_i \subseteq U_{i+1}$ für alle i. Das heißt jedes U_i in dieser Kette ist eine Teilmenge der endlichen Menge

$$U \cup \bigcup_{\substack{g \in W, \\ (E, E') \in P}} gE'.$$

Das heißt aber auch, sind U und W endlich dann gibt es eine eindeutige endliche Teilmenge $\widehat{U} \subseteq G$ so, dass

- $U \underset{P,W}{\overset{*}{\Rightarrow}} \widehat{U}$ und
- aus $U \underset{P,W}{\overset{*}{\Rightarrow}} U'$ folgt $U' \underset{P,W}{\overset{*}{\Rightarrow}} \widehat{U}$.

Die Teilmenge $\widehat{U}$ ist eine Normalform für das Ersetzungssystem $\underset{P,W}{\Rightarrow}$. Wir schreiben auch $U \underset{P,W}{\overset{\max}{\Rightarrow}} \widehat{U}$ um zu sagen, dass aus $\widehat{U} \underset{P,W}{\overset{*}{\Rightarrow}} U'$ bereits $\widehat{U} = U'$ folgt (das heißt $\widehat{U}$ ist die größte Menge U' (bezüglich Inklusion) so, dass $U \underset{P,W}{\overset{*}{\Rightarrow}} U'$).

5.3 Vorberechnungen

In diesem Abschnitt transformieren wir das Eingabesystem P in ein größeres System P_∞ welches dann verwendet wird, um das Wortproblem für $\mathrm{IM}(G)/P$ zu lösen. Wie wir später sehen werden, führt dies zu einem optimalen Algorithmus.

Eine Teilmenge $S \subseteq F$ der freien Gruppe F heißt suffixabgeschlossen, falls für alle reduzierten Wörter $uv \in S$ gilt, dass $v \in S$.

Sei P, wie zuvor, eine endliche Liste von Paaren (E, E'). Im ersten Schritt unserer Vorberechnungen ermitteln wir eine suffixabgeschlossene Menge $S \subseteq F$ so, dass

$$\bigcup_{(E,E')\in P} HE' \subseteq SH.$$

Die Berechnung einer geeigneten Menge $S \subseteq F$ ist in Polynomialzeit in der Größe von P möglich ist.

Der wichtigste Punkt ist, dass wenn $x \in gE'$ für ein $g \in G$ und $(E, E') \in P$ ist, dann können wir x wie folgt erreichen: Wir schreiben $g = fh$ mit $f \in F$ und $h \in H$ und erhalten $x \in fSH$. Dadurch können wir schließlich die Relation $\underset{P}{\Rightarrow}$ durch eine Relation $\underset{P_0,F}{\Rightarrow}$ ersetzen. Das heißt, ein Großteil der Berechnungen kann über einer Baumstruktur ausgeführt werden: dem Cayleygraph von F.

Die nächsten Schritte sind aufwändig, genauer kosten sie exponentielle Zeit in der Größe von P. Wegen Abschnitt 4.2 (untere Schranke für das uniforme Wortproblem für $\mathrm{FIM}(\Gamma)/P$) ist dies jedoch nicht zu vermeiden.

Wir definieren zunächst ein System P_0 wie folgt:

$$P_0 = \{(B, B') \mid B \subseteq B' \subseteq SH,\ B \underset{P}{\Rightarrow} B'\}.$$

Lemma 5.3.1 *Seien $U, U' \subseteq G$. Dann gilt $U \underset{P}{\Rightarrow} U'$ genau dann wenn $U \underset{P_0,F}{\Rightarrow} U'$.*

Beweis: Sei $U \underset{P_0,F}{\Rightarrow} U'$. Per Definition gibt es also ein $f \in F$ und $(B, B') \in P_0$ mit $fB \subseteq U$ und $U' = U \cup fB'$. Auf der anderen Seite, da $B \underset{P}{\Rightarrow} B'$ gibt es ein $g \in G$ und $(E, E') \in P$ mit $gE \subseteq B$ und $B' = B \cup gE'$. Wir erhalten insgesamt $fgE \subseteq U$ (da $fB \subseteq U$ und $gE \subseteq B$) und $U' = U \cup fgE'$ (da $U' = U \cup fB'$, $B' = B \cup gE'$ und $fB \subseteq U$). Per Definition ist damit $U \underset{P}{\Rightarrow} U'$.

Um die andere Richtung zu zeigen, sei $U \underset{P}{\Rightarrow} U'$. Für ein $f \in F$, $h \in H$ und (E, E') erhalten wir $fhE \subseteq U$ und $U' = U \cup fhE'$. Es ist

$$hE \subseteq hE' \subseteq SH,$$

per Definition von S, und $hE \underset{P}{\Rightarrow} hE'$. Deshalb ist $(hE, hE') \in P_0$ und damit $U \underset{P_0,F}{\Rightarrow} U'$. □

Sei im folgenden $\Sigma = \Gamma \cup \Gamma^{-1}$ und $\Sigma_1 = \Sigma \cup \{1\}$. Mit anderen Worten, Σ_1 ist der Ball vom Radius 1 im Cayleygraph von F. Da Σ_1 endlich ist (tatsächlich ist die Größe konstant) können wir den Begriff der Normalform wie im vorangegangenem Abschnitt verwenden. Wir erinnern, dass $B \underset{P_i,\Gamma_1}{\overset{\max}{\Rightarrow}} \widehat{B}$ die Menge $\widehat{B}$ in B bezüglich des Systems P_i definiert.

Seien $i \geq 0$ und P_i als ein System von Paaren (B, B') mit $B \subseteq B' \subseteq SH$ bereits definiert. Dann definieren wir P_{i+1} wie folgt:

$$P_{i+1} = \{(B, B') \mid B \subseteq SH,\ B' = \widehat{B} \cap SH,\ B \underset{P_i,\Gamma_1}{\overset{\max}{\Rightarrow}} \widehat{B}\}.$$

Wir bemerken, dass es genau $2^{|SH|}$ Regeln in P_{i+1} gibt. Die Berechnung von P_{i+1} (und der entsprechenden Darstellung) ist aufwändig, kann jedoch noch in exponentieller Zeit in der Größe von P durchgeführt werden. Wir bemerken, dass falls $(B, B') \in P_i$ dann gibt es genau eine Teilmenge $B'' \subseteq SH$ so, dass $B' \subseteq B''$ und $(B, B'') \in P_{i+1}$. Dies gilt da $1 \in \Sigma_1$. Wir benötigen das folgende wichtige Lemma.

Lemma 5.3.2 *Sei $i \geq 0$ und seien U, U' endliche Teilmengen von G. Dann sind folgende Aussagen äquivalent:*

1. $\exists V :\ U \overset{*}{\underset{P}{\Rightarrow}} V$ *und* $U' \subseteq V$.

2. $\exists V' : U \underset{P_i,F}{\overset{*}{\Rightarrow}} V'$ *und* $U' \subseteq V'$.

Beweis: Die Äquivalenz gilt für $i = 0$ da $U \underset{P}{\Rightarrow} U'$ äquivalent ist zu $U \underset{P_0,F}{\Rightarrow} U'$ (siehe Lemma 5.3.1).

Sei also $i \geq 0$ und sei zunächst $U \underset{P_i,F}{\overset{*}{\Rightarrow}} V$. Wir müssen zeigen, dass es ein V' mit $U \underset{P_{i+1},F}{\overset{*}{\Rightarrow}} V'$ und $V \subseteq V'$ gibt. Dies ist jedoch klar, da für alle $(B, B') \in P_i$ ein $(B, B'') \in P_{i+1}$ existiert mit $B' \subseteq B''$.

Es bleibt, die andere Richtung zu zeigen. Wir nehmen an, dass $U \underset{P_{i+1},F}{\overset{*}{\Rightarrow}} V'$. Es genügt zu zeigen, dass wir ein V mit $V' \subseteq V$ und $U \underset{P_i,F}{\overset{*}{\Rightarrow}} V$ finden können. Dazu sei $\widehat{P} = \{(B, B') \mid B \subseteq SH, B \underset{P_i,\Gamma_1}{\overset{\max}{\Rightarrow}} \widehat{B}\}$. Offenbar gibt es für jedes $(B, \widehat{B}) \in P_{i+1}$ nun ein $(B, \widehat{B}) \in \widehat{P}$ mit $B' \subseteq \widehat{B}$. Damit erhalten wir für eine Teilmenge V'' dass $U \underset{\widehat{P},F}{\Rightarrow} V''$ und $V' \subseteq V''$. Es genügt daher, ein V mit $U \underset{P_i,F}{\overset{*}{\Rightarrow}} V$ und $V'' \subseteq V$ zu finden. Dies ist jedoch trivial, da mit $(B, B') \in \widehat{P}$ folgt, dass $B \underset{P_i,F}{\overset{*}{\Rightarrow}} \widehat{B}$. □

Wir erinnern daran, dass $(B, B') \in P_i$ die Existenz einer eindeutigen Regel

$$(B, B'') \in P_{i+1} \text{ mit } B \subseteq B' \subseteq B'' \subseteq SH$$

impliziert. Es gibt höchstens exponentiell viele Regeln und jede Regel kann sich exponentiell oft ändern, wenn der Index i ansteigt. Das heißt, nach einer Berechnung in Exponentialzeit haben wir einen Index $i \geq 0$ gefunden so, dass $P_i = P_{i+1}$. Wir beenden hier die Phase der Vorberechnung und definieren $P_\infty = P_i$. Das heißt für alle $(B, B') \in P_\infty$ haben wir $B' = \widehat{B} \cap SH$ wobei $B \underset{P_\infty,\Gamma_1}{\overset{\max}{\Rightarrow}} \widehat{B}$.

Wir müssen nun das folgende Problem entscheiden.

EINGABE: Zwei endliche Mengen $U, U' \subseteq G$.
AUSGABE: Gibt es ein $V \subseteq G$ so, dass $U \underset{P_\infty,F}{\overset{*}{\Rightarrow}} V$ und $U' \subseteq V$?

5.4 Die Lösung des Wortproblems

Wir halten in diesem Abschnitt die folgende Notation fest: Seien P und P_∞ wie zuvor, wir betrachten die beiden endlichen Teilmengen $U, U' \subseteq G$. Es gibt eine suffixabgeschlossene Menge $S \subseteq F$ so, dass aus $(B, B') \in P_\infty$ folgt, dass $B \subseteq B' \subseteq SH$. Sei $W \subseteq F$ ein Teilbaum des Cayleygraphen von F mit

$$\{1\} \cup U \cup U' \subseteq WSH.$$

Sei $\widehat{U}$ definiert durch $U \underset{P_\infty, W}{\overset{*}{\Rightarrow}} \widehat{U}$.

Wir beweisen das folgende Theorem, welches das Wortproblem von $\mathrm{IM}(G)/P$ im Wesentlichen auf das Problem der Berechnung von $\widehat{U}$ reduziert.

Theorem 5.4.1 *Seien U, U' und $\widehat{U}$ wie oben. Dann sind die beiden folgenden Aussagen äquivalent:*

(1) $\exists V : U \underset{P}{\overset{*}{\Rightarrow}} V$ *und* $U' \subseteq V$,

(2) $U' \subseteq \widehat{U}$.

Die Richtung von (2) nach (1) haben wir bereits in Lemma 5.3.2 gesehen: Sei $U \subseteq \widehat{U}$. Per Definition ist $U \underset{P_\infty, W}{\overset{*}{\Rightarrow}} \widehat{U}$, insbesondere gibt es ein V wie in Lemma 5.3.2. Mit dem Lemma 5.3.2 folgt die Existenz eines V mit $U' \subseteq V$ und $U \underset{P}{\overset{*}{\Rightarrow}} V$.

Der schwierige Teil ist, die Richtung von (1) nach (2) zu zeigen. Dem werden wir uns im Rest des Abschnitts widmen.

Wir benötigen dazu folgende Notation: Für eine Teilmenge $V \subseteq G$ und ein Element $f \in F$ definieren wir die Ableitung

$$V \circ f = V',$$

durch $V' = V \cup fB'$, wobei $(B, B') \in P_\infty$ und $fB = V \cap fSH$.

Wir bemerken, dass $V \circ f$ für alle $V \subseteq G$ und $f \in F$ definiert ist, da alle Teilmengen von SH als linke Seite einer Regel aus P_∞ vorkommen. Offenbar folgt aus $V' = V \circ f$, dass $V \underset{P_\infty, F}{\Rightarrow} V'$ und umgekehrt folgt aus $V \underset{P_\infty, F}{\Rightarrow} V'$ dass $V' \subseteq V \circ f$ für ein $f \in F$.

Aus dem vorangegangenem Abschnitt wissen wir, dass $U' \subseteq V$ und $U \overset{*}{\underset{P}{\Rightarrow}} V$ für ein V genau dann gilt, falls es eine Sequenz $(f_1, \ldots, f_m)$ mit $f_i \in F$ für $1 \leq i \leq m$ gibt so, dass

$$U' \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m.$$

Da $U' \subseteq WSH$ (per Definition von W) genügt es, für den Beweis von Theorem 5.4.1, das folgende Lemma zu beweisen.

Lemma 5.4.1 *Seien $f_1, \ldots, f_m \in F$. Dann ist*

$$WSH \cap \widehat{U} \circ f_1 \circ \cdots \circ f_m \subseteq \widehat{U}.$$

Zunächst beschränken wir uns auf einen Spezialfall von Ableitungen - baumartige Ableitungen:

Definition 5.4.2 *Eine Ableitung $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ heißt baumartig, falls folgende Bedingungen gelten:*

1. $W = \{f_1, \ldots, f_n\}$ *für ein* $n \leq m$.
2. $f_i \notin \{f_1, \ldots, f_{i-1}\}$ *für* $1 \leq i \leq m$.
3. *Für alle* $1 \leq i \leq m$ *gibt es ein* $j \in \{1, \ldots, i-1\}$ *und ein* $a \in \Gamma$ *mit* $f_j a = f_i$ *in* F.

Die obigen Bedingungen besagen, dass $\{f_1, \ldots, f_i\}$ für alle i einen Teilbaum der Größe i des Cayleygraphen von F bildet, welcher W für $n \leq i \leq m$ enthält. Ferner ist $m \geq |W| = n$.

Die nächste Aussage ist das Schlüssellemma dieses Kapitels. Es besagt, dass wenn eine rechte Seite einer Regel in einer Teilmenge vorkommt, diese Teilmenge unverändert bezüglich weiterer Ableitungen bleibt (bei baumartigen Ableitungen). Genauer:

Lemma 5.4.3 *Sei $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ eine baumartige Ableitung. Für $1 \leq i \leq m$ definieren wir $B(i)$ als Teilmenge von SH durch:*

$$f_i B(i) = f_i SH \cap \widehat{U} \circ f_1 \circ \cdots \circ f_i.$$

Dann gilt:

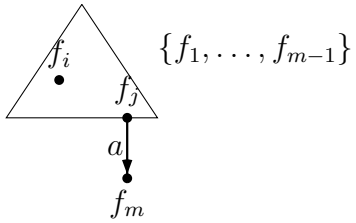
$$f_i B(i) = f_i SH \cap \widehat{U} \circ f_1 \circ \cdots \circ f_m.$$

Beweis: Die Aussage ist trivial für $m = n$ da $\widehat{U} \circ f_1 \circ \cdots \circ f_n = \widehat{U}$, wegen $W = \{f_1, \ldots, f_n\}$ und $\widehat{U} \overset{\max}{\underset{P_\infty, W}{\Rightarrow}} \widehat{U}$.

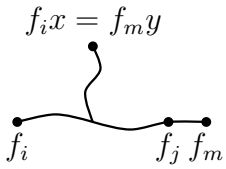
Sei also $m > n$ und $V = \widehat{U} \circ f_1 \circ \cdots \circ f_{m-1}$. Wir bemerken, dass $V \subseteq \bigcup_{f_i SH}$. Wir müssen zeigen, dass

$$f_i B(i) = f_i SH \cap V \circ f_m,$$

für alle $1 \leq i \leq m$. Dies gilt für $i = m$ per Definition von $f_i B(i)$. Wir nehmen per Induktion an, dass $f_i B(i) = f_i SH \cap V$ für alle $1 \leq i < m$. Wir wählen $j \in \{1, \ldots, m-1\}$ und $a \in \Gamma$ so, dass $f_j a = f_m$ in F. Angenommen, dass $f_i SH \cap f_m SH \neq \emptyset$ für ein $1 \leq i < m$. Dann ist $f_i x = f_m y$ für gewisse $x, y \in S$.



Da der Cayleygraph von F ein Baum ist, geht der kürzeste Pfad von f_i nach f_m über f_j. Das heißt $f_i x = f_m y = f_j z$, wobei z entweder ein Suffix von x oder ein Suffix von y ist.



Da S suffixabgeschlossen ist folgt, dass $z \in S$ und damit $f_i SH \cap f_m SH \subseteq f_j SH$ für alle $1 \leq i < m$. Es folgt, dass

$$f_m SH \cap V \subseteq f_m SH \cap \bigcup_{i<m} f_i SH \subseteq f_j SH.$$

Damit ist $f_m SH \cap V \subseteq f_j SH \cap V = f_j B(j)$. Wir haben also

$$V \circ f_m = V \cup (f_j B(j)) \circ f_m.$$

Nun ist, $(f_j B(j)) \circ f_m = f_j(B(j) \circ a)$, weil $f_m = f_j a$ (wir setzen $f_j = f_j^{-1} b(j)$, d.h. wir verschieben $B(j)$ in die 1 zurück und erhalten so eine rechte Seite einer Regel aus P_∞). Deshalb ($B(j)$ ist rechte Seite einer Regel aus P_∞) ist

$$B(j) \circ a \cap SH = B(j)$$

per Definition von P_∞. Es folgt, dass

$$(f_jB(j)) \circ f_m \cap f_jSH = f_j(B_j \circ a \cap SH) = f_jB_j$$

und deshalb

$$\begin{aligned} V \circ f_m \cap f_jSH &= (V \cup (f_jB(j)) \circ f_m) \cap f_jSH \\ &= (V \cap f_jSH) \cup ((f_jB(j)) \circ f_m \cap f_jSH) \\ &= (V \cap f_jSH) \cup f_jB_j \\ &= V \cap f_jSH \\ &= f_jB_j \subseteq V. \end{aligned}$$

Wir erhalten für $1 \leq i < m$:

$$\begin{aligned} V \circ f_m \cap f_iSH &= (V \cap f_iSH) \cup (V \circ f_m \cap f_iSH \cap f_mSH) \\ &\subseteq f_iB(i) \cup (V \circ f_m \cap f_iSH \cap f_jSH) \\ &\subseteq f_iB(i) \cup (f_iSH \cap V) \\ &= f_iB(i). \end{aligned}$$

Da jedoch $f_iB(i) \subseteq V \circ f_m \cap f_iSH$ folgt schließlich $f_iB(i) = V \circ f_m \cap f_iSH$.

□

Das folgende Lemma zeigt, dass wir uns auf baumartige Ableitungen beschränken können.

Lemma 5.4.4 *Sei $g_1, \ldots, g_k \in F$. Dann gibt es eine baumartige Ableitung $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ so, dass:*

$$\widehat{U} \circ g_1 \circ \cdots \circ g_k \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m.$$

Beweis: Offenbar gilt für alle $g \in F$:

$$\widehat{U} \circ g_1 \circ \cdots \circ g_k \subseteq \widehat{U} \circ g \circ g_1 \circ \cdots \circ g_k.$$

Deshalb können wir $\{g_1, \ldots, g_k\}$ durch eine größere Menge ersetzen und dann annehmen, dass für eine baumartige Ableitung $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ gilt, dass

$$\{g_1, \ldots, g_k\} = \{f_1, \ldots, f_m\}$$

und $g_i = f_i$ für $1 \leq i \leq m$.

Um zu zeigen, dass $\widehat{U} \circ g_1 \circ \cdots \circ g_k \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m$, sei per Induktion $\widehat{U} \circ g_1 \circ \cdots \circ g_{k-1} \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m$. Damit genügt es zu zeigen, dass

$$\widehat{U} \circ f_1 \circ \cdots \circ f_m \circ g_k \subseteq \widehat{U} \circ f_1 \circ \cdots \circ f_m.$$

Es ist jedoch $g_k = f_i$ für ein $1 \leq i \leq m$.

Sei $V = \widehat{U} \circ f_1 \circ \cdots \circ f_m$. Wir zeigen dass $V \circ f_i = V$ für alle $1 \leq i \leq m$. Wie in Lemma 5.4.3 sei $f_i B(i) = f_i SH \cap \widehat{U} \circ f_1 \circ \cdots \circ f_i$. Dann besagt Lemma 5.4.3 dass $f_i SH \cap V = f_i B(i)$. Wir erhalten

$$V \circ f_i = V \cup (f_i B(i)) \circ f_i = V \cup f_i B(i) = V.$$

□

Wir können nun Lemma 5.4.1 beweisen:

Beweis: Wegen Lemma 5.4.4 können wir annehmen dass $\widehat{U} \circ f_1 \circ \cdots \circ f_m$ baumartig ist. Jedes Element aus WSH ist in einem $f_i SH$ für $1 \leq i \leq n$ enthalten. Wegen Lemma 5.4.3 erhalten wir

$$f_i SH \cap \widehat{U} \circ f_1 \circ \cdots \circ f_m = f_i SH \cap \widehat{U} \circ f_1 \circ \cdots \circ f_i.$$

Es ist jedoch $i \leq n$ und damit $\widehat{U} \circ f_1 \circ \cdots \circ f_i = \widehat{U}$, deshalb ist

$$WSH \cap \widehat{U} \circ f_1 \circ \cdots \circ f_m \subseteq \widehat{U}.$$

Dies beweist Lemma 5.4.1 und auch Theorem 5.4.1. □

5.5 Berechnung in Linearzeit

Sei von nun an, G eine virtuell freie Gruppe und P ein endliches, fest gegebenes System von Gleichungen. Zunächst haben wir das System P_∞ und eine suffixabgeschlossene Menge $S \subseteq F$ vorberechnet mit $B \subseteq B' \subseteq SH$, für alle $(B, B') \in P_\infty$.

Das Wortproblem erhält als Eingabe die beiden Mengen $U, U' \subseteq G$. Wir nehmen an, dass diese wie in Abschnitt 5.1 als alternierende Sequenzen gegeben sind. Wir arbeiten auf einer RAM, wir können also Zeiger (wie etwa bei der Darstellung der Munnbäume für den Linearzeitalgorithmus für das Wortproblem von $\mathrm{FIM}(\Gamma)/P$ im Kapitel 4) nutzen, um Teilbäume des Cayleygraphen von F darzustellen. Da S

und H als Konstanten aufgefasst werden, kann ein Teilbaum W in Linearzeit in der Eingabegröße von U und U' realisiert werden, so dass für diesen Teilbaum W gilt:

$$\{1\} \cup U \cup U' \subseteq WSH.$$

Wir müssen nun $U \overset{\max}{\underset{P_\infty, W}{\Rightarrow}} \widehat{U}$ in linearer Zeit berechnen. Der abschließende Test, ob $U' \subseteq \widehat{U}$ kann in linearer Zeit durchgeführt werden, indem U' noch einmal gelesen wird.

Um $U \overset{\max}{\underset{P_\infty, W}{\Rightarrow}} \widehat{U}$ zu berechnen bilden wir eine Liste $L = (f_1, \ldots, f_n)$ die zunächst alle Elemente von W enthält.

Solange L nicht leer ist, führen wir folgende Schritte aus: Sei f das erste Element von L.

- Entferne f von der Liste L.
- Berechne eine Menge B so, dass $fB = fSH \cap U$ in konstanter Zeit.
- Finde, durch Table–Lookup in P_∞, eine Menge B' mit $(B, B') \in P_\infty$.
- Falls $B \neq B'$ dann ersetze U durch $U \cup fB'$ in konstanter Zeit und füge die Elemente $g \in W$ zur Liste L hinzu, die $gSH \cap fB' \neq \emptyset$ und $g \neq f$ erfüllen. Dazu müssen wir $W \cap fB'S^{-1}H^{-1}$ berechnen. Dieses Hinzufügen kann in konstanter Zeit erfolgen.
- Ist $B = B'$ so tue nichts.

Ist die Liste L leer, so gilt (für das während obiger Schritte veränderte U) $U = \widehat{U}$. Bevor wir dies beweisen, analysieren wir zunächst die Komplexität.

Die inneren Teile der Schleife können in konstanter Zeit ausgeführt werden. Das heißt, uns bleibt eine obere Schranke für die Anzahl der Schleifenbesuche anzugeben. Nach jeder Schleife ist die Liste L entweder kürzer oder wir haben ihr weniger als c Elemente zugefügt, wobei $c = |S|^2|H|$ eine Konstante ist. Wir geben durch

$$\omega = c|WSH \backslash U| + |L|,$$

ein Gewicht ω für Paare (U, L) an. Hierbei sei $|L|$ die Länge der Liste L. Das Gewicht ist eine natürliche Zahl und zu Beginn gleich $(c+1)|WSH|$. Dies ist linear in der Eingabegröße von U und U'. Wir zeigen nun, dass dieses Gewicht in jeder Runde tatsächlich kleiner wird.

Innerhalb der Schleife gibt es zwei Fälle: entweder $B = B'$ oder $B \neq B'$. Falls $B = B'$, dann wurde U nicht verändert aber $|L|$ verringert sich um 1. Ist $B \neq B'$, dann wird U größer. Wir haben noch immer $U \subseteq WSH$ und die Größe von $|WSH \backslash U|$ verringert sich um mindestens 1. Damit verringert sich das Gewicht mindestens um den Betrag c, aber wir fügen zu L weniger als c Elemente hinzu. Mit anderen Worten, das Gewicht fällt um mindestens 1. Das heißt nach spätestens $(c+1)|WSH \backslash U|$ Runden ist die Liste L leer.

Bleibt zu zeigen, dass wir $\widehat{U}$ berechnet haben. Wir zeigen dazu: Nach jeder Schleifenrunde enthält die Liste L alle Elemente $g \in W$, so dass $U \circ g \neq U$. (Wir sind fertig, wenn U durch Ableiten mit Elementen aus W nicht mehr vergrößert werden kann.) Dies gilt offenbar bereits am Anfang, da L zu diesem Zeitpunkt alle Elemente von W enthält.

Sei nun f das erste Element von L, und f wurde in der Schleife gerade aus L entfernt. Innerhalb der Schleife haben wir U durch $U \circ f$ ersetzt und da $U \circ f \circ f = U \circ f$ benötigen wir f nicht mehr in L (durch weiteres Ableiten (in dieser Runde) mit f würde sich an U nichts ändern). Das heißt, ist $U = U \circ f$, so ändert sich nichts. Wir können also annehmen, dass U durch $U \cup fB'$ mit $B \neq B'$ ersetzt wurde.

Ist nun

$$(U \cup fB') \circ g \neq U \cup fB',$$

für ein $g \in W$ dann ist $g \neq f$ und entweder $U \circ g \neq U$ oder $gSH \cap fB' \neq \emptyset$. Im ersten Fall ist g noch immer in der Liste, im zweiten Fall wird g zur Liste L hinzugefügt. In beiden Fällen ist also g in der Liste L nach Ende des inneren Teils der Schleife. Ist die Liste L leer, dann ist U irreduzibel bezüglich des Ersetzungssystems $\underset{P_\infty, W}{\Rightarrow}$ ist. Wir erhalten $U = \widehat{U}$.

Dies zeigt, dass $\widehat{U}$ in Linearzeit berechnet werden kann. Zusammenfassend haben wir gezeigt:

Korollar 5.5.1 *Das Wortproblem des inversen Monoids $\mathrm{IM}(G)/P$ kann in Linearzeit gelöst werden.*

Kapitel 6

Strukturen mit Prädikat reach_L

Sei M ein Monoid mit endlicher Erzeugermenge Σ und $h : \Sigma^* \to M$ der kanonische surjektive Homomorphismus. Eine Teilmenge $L \subseteq M$ heißt rational, falls es eine reguläre Sprache $K \in \Sigma^*$ gibt, so dass $L = h(K)$. Mit RAT(M) bezeichnen wir die Menge der rationalen Mengen von M, mit $\mathcal{B}(\mathrm{RAT}(M))$ die boolesche Algebra der rationalen Mengen von M.

Wir führen wir für alle rationalen Sprachen $L \subseteq \mathrm{RAT}(M)$ die Relation reach_L ein. Zwei Elemente u und v aus M stehen in der Relation $reach_L$ wenn es ein $x \in L$ gibt, so dass $ux = v$ in M.

Definition 6.0.2 *Sei M ein Monoid mit Erzeugermenge Σ und $1 \in M$ das neutrale Element von M. Wir definieren folgende Struktur*

$$\begin{aligned} \mathcal{C}(M) &= (M, (\mathrm{reach}_L)_{L \in \mathrm{RAT}(\Sigma)}, 1), \text{ mit} \\ \mathrm{reach}_L &= \{(u, v) \in M \times M \mid \exists w \in L : uw = v\}. \end{aligned}$$

Sei G von nun an eine endlich erzeugte, virtuell freie Gruppe mit endlicher Erzeugermenge $\Delta = \Gamma \cup \Gamma^{-1} \cup H$ wie in Kapitel 5. Sei ferner P eine endlich idempotente Präsentation in $\mathrm{IM}(G)$. Wir zeigen in diesem Kapitel:

Theorem 6.0.1 *Die FO-Theorie von $\mathcal{C}(\mathrm{IM}(G)/P)$ ist entscheidbar.*

Bemerkung 6.0.1 *Mit den gleichen Methoden können wir zeigen (siehe [33]), dass die FO-Theorie von $\mathrm{FIM}(\Gamma)/P$ entscheidbar ist.*

Im ersten Abschnitt dieses Kapitels beweisen wir ein Ergebnis, welches zum Beweis des Hauptresultats benötigt wird.

6.1 Hilfsresultate

Es genügt, sich im Folgenden auf endliche Graphen zu beschränken. Wir geben zwei alternative Beweise des folgenden Resultats an:

Satz 6.1.1 *Sei Σ eine endliche Menge und $L \subseteq \mathrm{RAT}(\Sigma)$.*

Dann gibt es eine MSO-Formel $\mathrm{Reach}_L(x, y, X)$ über der Signatur bestehend aus den binären Symbolen E_a, $a \in \Sigma$ so, dass für jeden gerichteten kantenmarkierten Graph $\mathcal{C} = (V, (E_a)_{a\in\Sigma})$, alle Knoten $s, t \in V$, und jede endliche Menge von Knoten $U \subseteq V$ gilt:

$\mathcal{C} \models \mathrm{Reach}_L(s, t, U) \quad \Leftrightarrow$ *Es gibt einen Pfad in $\mathcal{C}$ mit Anfangsknoten $s \in U$ und Endknoten $t \in U$, der genau die Knoten von U besucht und, wenn die Markierungen der Pfade als Wort aus Σ^* gelesen werden, erhalten wir ein Wort aus L.*

Genauer gilt $\mathcal{C} \models \mathrm{Reach}_L(s, t, U)$ genau dann, wenn es

$$p_1, \ldots, p_m \in V \text{ und } a_1, \ldots, a_m \in \Sigma$$

gibt, mit $p_1 = s$, $p_m = t$, $(p_i, p_{i+1}) \in E_{a_i}$ für $i = 1, \ldots, m-1$ und $a_1 \cdots a_m \in L$, $U = \{p_1, \ldots, p_m\}$.

Für den ersten Beweis geben wir zunächst eine Formel an, die die Existenz eines Pfads, der alle Knoten eines Graphen (Lemma 6.1.2) besucht, beschreibt. Dieses einfache Konzept wird in beiden Beweisen benötigt.

Lemma 6.1.2 *Sei $\mathcal{C} = (V, E)$ ein endlicher, gerichteter Graph. Dann gibt es über der Signatur E eine MSO-Formel $\mathrm{reach}(x, y, X)$ so, dass*

$\mathcal{C} \models \mathrm{reach}(s, t, U) \quad \Leftrightarrow$ *Es gibt einen Pfad in $\mathcal{C}$ mit Anfangsknoten s und Endknoten t der genau die Knoten U aus $\mathcal{C}$ besucht.*

Beweis: Wir nutzen hierfür die Formel $\mathrm{reach}(x, y)$ aus Abschnitt 2.3. Wir formulieren für jeden Knoten u in U die Existenz eines Pfads von s nach u sowie eines Pfads von u nach t. Wir erhalten damit die folgende MSO-Formel über $\mathcal{C} = (V, E)$:

$$\begin{aligned}\mathrm{reach}(x, y, X) \;=\; & x \in X \wedge y \in X \wedge \forall u, v \in X : \\ & \wedge \mathrm{reach}|_X(x, u) \wedge \mathrm{reach}|_X(u, y) \\ & \wedge (\mathrm{reach}|_X(u, v) \vee \mathrm{reach}|_X(v, u)).\end{aligned}$$

Gibt es einen Pfad p von x nach y der genau die Knoten aus X besucht, so ist $\mathrm{reach}(x, y, X)$ offenbar erfüllt, denn $x, y \in X$, da p genau die Knoten aus X besucht, also auch Anfangs- und Endknoten. Ferner gibt es für alle $u \in X$ einen Pfad von x nach u bzw. von u nach y, da x und y Anfangs- bzw. Endknoten und P alle Knoten aus X besucht. Aus letzterem Grund gilt dann offenbar auch für alle $u, v \in X$ $\mathrm{reach}|_X(u, v) \vee \mathrm{reach}|_X(v, u)$.

Sei also umgekehrt $\mathrm{reach}(x, y, X)$ erfüllt und sei $p = (z_1, \ldots, z_n)$ ein Pfad in $\mathcal{C}$ mit $z_i \in X$ und $z_1 = x$ sowie $z_n = y$. Angenommen, es existiert ein $w \in X$ mit $w \neq z_i$ für alle $1 \leq i \leq n$. Wegen $w \in X$ gilt $\mathrm{reach}|_X(x, w)$ und $\mathrm{reach}|_X(w, y)$, es gibt also Pfade q und q' von x nach w bzw. w nach y, die nur Knoten aus X besuchen.

Nun gilt für alle $u \in X$ entweder $\mathrm{reach}|_X(u, w)$ oder $\mathrm{reach}|_X(w, u)$, insbesondere gilt dies auch für $u = z_i$ für alle $1 \leq i \leq n$. Wir bezeichnen die entsprechenden Pfade (von z_i nach w bzw. von w nach z_i) mit p_i bzw. p'_i für alle $1 \leq i \leq n$.

Gilt für alle z_i nun $\mathrm{reach}|_X(z_i, w)$ (bzw. $\mathrm{reach}|_X(w, z_i)$), so ist

$$(z_1, \ldots, z_{n-1}) p_{n-1} q' \qquad \text{(bzw. } (z_1) q p'_2 (z_2, \ldots, z_n)\text{)}$$

ein Pfad von x nach y in X, der alle Knoten z_i und w besucht (wobei wir Pfade p und q durch pq aneinander hängen, wenn der letzte Knoten von p gleich dem ersten Knoten von q ist).

Andernfalls gibt es ein i mit Pfaden $p_i p'_{i+1}$ (bzw. $p'_i p_{i+1}$) so, dass

$$(z_1, \ldots, z_i) p_i p'_{i+1} (z_{i+1}, \ldots, z_n) \qquad \text{(bzw. } (z_1, \ldots, z_{i+1}) p_{i+1} p'_i (z_i, \ldots, z_n)\text{)}$$

Pfade von x nach y in X sind, die alle Knoten z_i und w besuchen.

Mit anderen Worten, es gibt einen Pfad von x nach y in $\mathcal{C}$, der alle Knoten von X besucht. □

Zur Erinnerung möchten wir darauf hinweisen, dass für die in Abschnitt 2.3 angegebene Formel $\mathrm{reach}(x, y)$ und die dabei benutzte Einschränkung $\mathrm{reach}|_X(x, y, X)$ gilt: $\mathcal{C} \models \mathrm{reach}|_U(s, t, U)$ genau dann wenn es einen Pfad von s nach t gibt, der lediglich (jedoch nicht notwendig alle, im Unterschied zur Formel $\mathrm{reach}(x, y, X)$) Knoten aus U besucht.

Nun geben wir eine MSO-Formel an, die die Existenz eines Pfads, der alle Knoten eines Graphen besucht und dabei ein Wort aus einer Sprache abläuft. Hierzu benötigen wir den Begriff der MSO-definierbaren Transduktion (kurz auch MSO-Transduktion) [16, 17, 18].

Hierbei wollen wir eine Struktur $\mathcal{S} \in \mathrm{RS}(\mathsf{SIG}_1)$ in eine Struktur $\mathcal{T} \in \mathrm{RS}(\mathsf{SIG}_2)$, durch Definition von $\mathcal{T}$ „innerhalb“ von $\mathcal{S}$ mittels MSO-Formeln definieren. Die grundsätzliche Idee ist, siehe als weiteres Beispiel auch die Umwandlung einer Formel φ über der Signatur von $\mathcal{C}(\Gamma)$ in eine Formel $\hat{\varphi}$ über der Signatur von T_Γ im Abschnitt 2.4, die semantische Interpretation, siehe hierzu etwa [52, 49], hier um gewisse Aspekte erweitert.

Wir werden $\mathcal{T}$ in einer Art Zwischenstruktur definieren. Diese besteht aus m Kopien von $\mathcal{S}$ zusammen mit einer binären Relation, welche besagt, dass zwei Elemente das gleiche Element in $\mathcal{S}$ darstellen.

Genauer seien zunächst M, M' zwei Mengen und $R \subseteq M \times M'$ eine binäre Relation. Die zugeordnete Abbildung zwischen den Potenzmengen 2^M und $2^{M'}$ bezeichnen wir ebenfalls mit R (wobei $R(m) = \{m' \in M' \mid (m, m') \in R\}$). Dieses R wird auch Transduktion von M nach M' genannt. Wir fassen jedes $m' \in M'$ mit $(m, m') \in R$ als Bild von m unter R auf, R ist damit eine mehrwertige Funktion von M nach M'.

Seien SIG_1 und SIG_2 zwei relationale Signaturen. Ein definierendes Schema[1] für $(\mathsf{SIG}_1, \mathsf{SIG}_2)$ ist ein Tupel Δ_{def} von MSO-Formeln über der Signatur SIG_1:

$$\Delta_{\text{def}} = (\theta_{P,\overline{i}}(\overline{x}))_{P \in \mathsf{SIG}_2, \overline{i} \in \{1,\ldots,m\}^n},$$

wobei $\overline{x}$ ein Tupel von n freien FO-Variablen ist, für alle $n = n_P$-stelligen relationalen Symbole $P \in \mathsf{SIG}_2$ und $\overline{i} = (i_1, \ldots, i_n) \in \{1, \ldots, m\}^n$ mit $m > 0$ (m ist die Anzahl der oben erwähnten Kopien). Die Formeln $\theta_{P,\overline{i}}(x_1, \ldots, x_n)$ werden auch definierende Formeln genannt.

Sei nun $\mathcal{S} = (S, (R^{\mathcal{S}})_{R \in \mathsf{SIG}_1})$ eine Struktur aus $\mathrm{RS}(\mathsf{SIG}_1)$. Eine relationale Struktur über der Signatur SIG_2 wird nun in $\mathcal{S}$ wie folgt definiert:

$$\mathcal{T} = (S \times \{1, \ldots, m\}, (P_{\mathcal{T}})_{P \in \mathsf{SIG}_2}),$$

[1] Wir verwenden eine sehr eingeschränkte Version von MSO-definierbaren Transduktionen. Für eine allgemeinere Darstellung siehe etwa [17, 18]

wobei für jedes n-stellige relationale Symbol $P \in \mathsf{SIG}_2$ gilt:

$$P_{\mathcal{T}} = \{((s_1, i_1), \ldots, (s_n, i_n)) \mid \mathcal{S} \models \theta_{P,(i_1,\ldots,i_n)}(s_1, \ldots, s_n)\},$$

wobei $((s_1, i_1), \ldots, (s_n, i_n)) \in (S \times \{1, \ldots, m\})^n$. Da $\mathcal{T}$, für ein fest definiertes Δ_{def}, in eindeutiger Weise mit $\mathcal{S}$ assoziiert werden kann, können wir $f_{\Delta_{\text{def}}}(\mathcal{S}) = \mathcal{T}$ schreiben. Die Transduktion definiert durch Δ_{def} ist damit die folgende Relation:

$$f_{\Delta_{\text{def}}} = \{(\mathcal{S}, \mathcal{T}) \mid f_{\Delta_{\text{def}}}(\mathcal{S}) = \mathcal{T}\}.$$

Eine Transduktion $g \in \mathrm{RS}(\mathsf{SIG}_1) \times \mathrm{RS}(\mathsf{SIG}_1)$ heißt MSO-definierbar, falls $g = f_{\Delta_{\text{def}}}$ für ein definierendes $(\mathsf{SIG}_1, \mathsf{SIG}_2)$-Schema Δ_{def}.

Ist eine Transduktion $f \in \mathrm{RS}(\mathsf{SIG}_1) \times \mathrm{RS}(\mathsf{SIG}_1)$ MSO-definierbar, so ist f MSO-kompatibel [17].

Eine MSO-Transduktion f heißt MSO-kompatibel [16, 17, 18], falls es eine total rekursive Abbildung $f^\sharp$ (backwards translation von f) gibt, wobei $f^\sharp$ eine Abbildung von der Menge der MSO-Sätze über der Signatur SIG_2 in die Menge der MSO-Sätze über der Signatur SIG_1 ist, so dass für alle MSO-Sätze φ über der Signatur SIG_2 und alle $\mathcal{S} \in \mathrm{RS}(\mathsf{SIG}_1)$ gilt:

$$\mathcal{S} \models f^\sharp(\varphi) \quad \Leftrightarrow \quad f(\mathcal{S}) \models \varphi.$$

Damit können wir das folgende Hilfsresultat beweisen:

Lemma 6.1.3 *Sei Σ eine endliche Menge und $L \subseteq \mathrm{RAT}(\Sigma)$. Dann gibt es eine MSO-Formel φ_L über der Signatur der endlichen Struktur $\mathcal{C} = (V, (E_a)_{a\in\Sigma}, s, t)$ (mit binärem Symbol $(E_a)_{a\in\Sigma}$, sowie den Konstanten s und t) so, dass*

$$\begin{aligned} \mathcal{C} \models \varphi_L \quad \Leftrightarrow \quad & \textit{Es gibt einen Pfad } p = p_1, \ldots, p_n \textit{ in } \mathcal{C} \textit{ und} \\ & a_1, \ldots, a_{n-1} \in \Sigma \textit{) so, dass } p_1 = s, \; p_n = \\ & t, \; (p_i, p_{i+1}) \in E_{a_i} \textit{ für alle } 1 \leq i < n, \\ & a_1 a_2 \cdots a_{n-1} \in L \textit{ und } V = \{p_1, \ldots, p_n\}. \end{aligned}$$

Beweis: Sei $L \subseteq \mathrm{RAT}(\Sigma)$ und $\mathcal{C} = (V, (E_a)_{a\in\Sigma}, s, t)$.

Sei weiterhin $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ ein deterministischer endlicher Automat mit $L(\mathcal{A}) = L$. Wir können ohne Beschränkung annehmen, dass $Q = \{1, \ldots, m\}$.

Sei $\mathcal{C}_\mathcal{A}$ die Struktur $\mathcal{C}_\mathcal{A} = (V \times Q, E, \nabla, I_s, F_t)$, mit

$$\begin{aligned} E &= \{((u,i),(v,j)) \mid \exists a \in \Sigma : (u,v) \in E_a \wedge \delta(i,a) = j\}, \\ \nabla &= \{((v,1),\ldots,(v,m)) \mid v \in V\}, \\ I_s &= \{(s,q_0)\} \text{ und} \\ F_t &= \{t\} \times F. \end{aligned}$$

Wir wollen zeigen, dass $f \subseteq \mathrm{RS}((E_a)_{a\in\Sigma}, s, t) \times \mathrm{RS}(E, \nabla, I_s, F_t)$ eine MSO-Transduktion mit $f(\mathcal{C}) = \mathcal{C}_\mathcal{A}$ ist.

Dazu müssen wir die definierenden MSO-Formeln $\theta_{P,(i_1,\ldots,i_k)}(x_1,\ldots,x_k)$ (über der Signatur von $\mathcal{C}$) für alle (k-wertigen) P aus (E, ∇, I_s, F_t) (der Signatur von $\mathcal{C}_\mathcal{A}$) und alle Tupel $(i_1,\ldots,i_k) \in Q^k = \{1,\ldots,m\}^k$ angeben:

$$\begin{aligned} \theta_{E,(i,j)}(x_1,x_2) &= \bigvee_{a\in\Sigma,\delta(i,a)=j} E_a(x_1,x_2) \\ \theta_{\nabla,(i_1,\ldots,i_m)}(x_1,\ldots,x_m) &= \begin{cases} x_1 = x_2 = \cdots = x_m & \text{falls } i_j = j,\ 1 \le j \le m \\ \text{falsch} & \text{sonst} \end{cases} \\ \theta_{I_s,(i)}(x) &= \begin{cases} x = s & \text{falls } i = q_0 \\ \text{falsch} & \text{sonst} \end{cases} \\ \theta_{F_t,(i)}(x) &= \begin{cases} x = t & \text{falls } i \in F \\ \text{falsch} & \text{sonst} \end{cases} \end{aligned}$$

Es ist leicht zu sehen, dass diese Formeln tatsächlich die Struktur $f(\mathcal{C}) = \mathcal{C}_\mathcal{A}$ beschreibt. Damit ist f MSO-kompatibel, mit anderen Worten es gibt ein $f^\sharp$ so, dass für jede MSO-Formel φ gilt $f(\mathcal{C}) \models \varphi$ genau dann wenn $\mathcal{C} \models f^\sharp(\varphi)$.

Wir betrachten nun die MSO-Formel ψ über der Signatur von $\mathcal{C}_\mathcal{A}$:

$$\psi = \exists X \left\{ \begin{array}{l} \forall x_1 \cdots \forall x_m : \left(\nabla(x_1,\ldots,x_m) \Rightarrow \bigvee_{i=1}^{m} x_i \in X \right) \wedge \\ \exists x \in I_s \, \exists y \in F_t : x, y \in X \wedge \mathrm{reach}(x,y,X) \end{array} \right\}$$

Wobei $\mathrm{reach}(x,y,X)$ die Formel aus Lemma 6.1.2 ist.

Damit ist $f^\sharp$ die gesuchte Formel. □

Es folgt sofort die Existenz der Formel $\mathrm{Reach}_L(x,y,X)$ über der Signatur eines endlichen, gerichteten Graphen $\mathcal{C}$: Wir können über der Signatur aus Lemma 6.1.3 mit der Formel $\varphi_L|_X(X)$ (φ_L ist die Formel aus Lemma 6.1.3) ausdrücken, dass

genau die Knoten aus X besucht werden. Damit erhalten wir $\mathrm{Reach}_L(x, y, X)$ über der Signatur von $\mathcal{C}$.

Der zweite Beweis erfolgt direkt und kommt ohne den Begriff der MSO-definierbaren Transduktion aus. Hier werden induktiv entsprechende MSO-Formeln definiert, dabei wird auch die Idee aus Lemma 6.1.2 genutzt.

Beweis (von Lemma 6.1.1): Der Beweis nutzt Ideen des Beweises von Kleenes Theorem, siehe etwa [23], welches zeigt, dass erkennbare Sprachen rational sind.

Sei $L \in \Sigma^*$ eine reguläre Sprache die durch den nichtdeterministischen Automat $\mathcal{A} = (Q, \Sigma, \delta, I, F)$ gegeben ist. Wir nehmen an, dass $Q = \{1, \ldots, n\}$.

Unser Ziel ist die Definition einer Formel

$$\mathrm{Reach}[i, j](x, y, X)$$

so, dass für jeden gerichteten kantenmarkierten Graph $\mathcal{C} = (V, (E_a)_{a\in\Sigma})$, alle Knoten $s, t \in V$ und jede endlich Knotenmenge $U \subseteq V$ gilt:

$\mathcal{C} \models \mathrm{Reach}[i, j](s, t, U)$ genau dann, wenn es einen Pfad $p = p_0, \ldots, p_m$ in $\mathcal{C}$ und einen Pfad $q_0, \ldots, q_m$ in $\mathcal{A}$ gibt mit

- $p_0 = s$, $\{p_0, \ldots, p_m\} = U$, und $p_m = t$,
- $(p_{\ell-1}, p_\ell) \in E_a$, $(q_{\ell-1}, a, q_\ell) \in \delta$ für $a \in \Sigma$ für alle $\ell = 1, \ldots, m$,
- $q_0 = i$ und $q_m = j$.

Die gesuchte Formel des Lemmas ist dann:

$$\mathrm{Reach}_L(x, y, X) := \bigvee_{i\in I, f\in F} \mathrm{Reach}[i, f](x, y, X).$$

Zunächst definieren wir via Induktion nach k eine Formel

$$\mathrm{reach}[i, j, k](x, y, X),$$

für welche wir die Bedingung an X abschwächen und den Automat auf die Zustände $\{1, \ldots, k\}$, $1 \leq k \leq n$, einschränken.

Genauer werden wir eine Formel $\mathrm{reach}[i, j, k](x, y, X)$ für jeden gerichteten Graphen $\mathcal{C} = (V, (E_a)_{a\in\Sigma})$, alle Knoten $s, t \in V$ und alle Knotenmengen $U \subseteq V$ mit den folgenden Eigenschaften angeben:

$\mathcal{C} \models \mathrm{reach}[i, j, k](s, t, U)$ genau dann, wenn es einen Pfad $p = p_0, \ldots, p_m$ in G und einen Pfad $q_0, \ldots, q_m$ im Automat $\mathcal{A}$ gibt, mit

- $p_0 = s$, $\{p_0, \ldots, p_m\} \subseteq U$, und $p_m = t$,
- $(p_{\ell-1}, p_\ell) \in E_a$, $(q_{\ell-1}, a, q_\ell) \in \delta$ für $a \in \Sigma$ für alle $\ell = 1, \ldots, m$,
- $q_0 = i$, $\{q_1, \ldots, q_{m-1}\} \subseteq \{1, \ldots k\}$, und $q_m = j$.

Für $k = 0$ definieren wir:

$$\mathrm{reach}[i,j,0](x,y,X) \;=\; x,y \in X \wedge \left((x = y \wedge i = j) \vee \bigvee_{\substack{a \in \Sigma, \\ (i,a,j) \in \delta}} (x,y) \in E_a \right).$$

Sei nun $k \geq 1$. Sei $\mathrm{reach}[k,k,k-1](x,y,X)$ per Induktion bekannt. Damit können wir die MSO-Formel $\mathrm{reach}[k,k,k](x,y,X)$ als transitiven Abschluss der Formel $\mathrm{reach}[k,k,k-1](x,y,X)$ (bezüglich der Relation zwischen x und y für festes X) definieren.

Wir haben ebenfalls $\mathrm{reach}[k,k,k-1](u,u,X)$ per Induktion und deshalb haben wir ebenso $\mathrm{reach}[k,k,k](u,u,X)$ für alle $u \in X$ (beachte: Wir bilden oben lediglich den transitiven und nicht den reflexiv transitiven Abschluss).

Analog zum Beweis von Kleenes Theorem können wir nun für alle weiteren Paare (i,j) die Formel $\mathrm{reach}[i,j,k](x,y,X)$ definieren:

$$\begin{aligned} \mathrm{reach}[i,j,k](x,y,X) \;=\; & \mathrm{reach}[i,j,k-1](x,y,X) \vee \\ & \exists x' \exists y' \left\{ \begin{array}{l} \mathrm{reach}[i,k,k-1](x,x',X) \wedge \\ \mathrm{reach}[k,k,k](x',y',X) \wedge \\ \mathrm{reach}[k,j,k-1](y',y,X) \end{array} \right\}. \end{aligned}$$

Wir setzen $\mathrm{reach}[i,j](x,y,X) = \mathrm{reach}[i,j,n](x,y,X)$, und erhalten damit:

$$\mathrm{reach}[i,j](x,y,X) \wedge \mathrm{reach}[j,k](y,z,X)$$

impliziert $\mathrm{reach}[i,k](x,z,X)$.

Mit $\mathrm{reach}[i,j](x,y,X)$ können wir nun $\mathrm{Reach}[i,j](x,y,X)$ wie folgt definieren:

$$\exists X_1 \cdots \exists X_n \left\{ \begin{array}{l} x \in X_i \;\wedge\; \bigwedge_{k \neq \ell} X_k \cap X_\ell = \emptyset \;\wedge\; X = X_1 \cup \cdots \cup X_n \wedge \\ \\ \bigwedge_{k,\ell} \forall u \in X_k \forall v \in X_\ell \left\{ \begin{array}{c} \mathrm{reach}[i,k](x,u,X) \wedge \\ \mathrm{reach}[k,j](u,y,X) \wedge \\ (\mathrm{reach}[k,\ell](u,v,X) \vee \\ \mathrm{reach}[\ell,k](v,u,X)) \end{array} \right\} \end{array} \right\}.$$

Um die Korrektheit der Formel zu beweisen, sei zunächst $p_0, \ldots, p_m$ ein Pfad in $\mathcal{C}$ mit $p_0 = x$ und $p_m = y$, welcher genau die Knoten von X besucht und sei $q_0, \ldots, q_m$ der entsprechende Pfad im Automat $\mathcal{A}$ mit $q_0 = i$ and $q_m = j$. Wir können nun leicht die Erfüllbarkeit der Formel zeigen: Dazu setzen wir

$$X_k = \{p_\ell \mid p_\ell \neq p_r \forall r < \ell,\, k = q_\ell,\, 1 \leq \ell \leq m\}.$$

Mit anderen Worten, X_k ist diejenige Menge von Knoten aus $\mathcal{C}$, in welchen wir uns, beim Ablauf des Pfades von x nach y, im Zustand k des Automats befinden (beim ersten Besuch des jeweiligen Knotens).

Dies definiert eine Partition $X = X_1 \cup \cdots \cup X_n$, wobei einige der X_k leer sein dürfen. Offenbar gilt $x \in X_i$, aber es kann passieren, dass $y \in X_\ell$ wobei $\ell \neq j$, da wir nur das erste Erscheinen von y auf dem Pfad berücksichtigen. Jedenfalls ist $\mathrm{reach}[k, j](u, y, X)$ für alle u und k mit $u \in X_k$.

Seien nun $u \in X_k$ und $v \in X_\ell$ auf dem Pfad von x nach y. Damit erhalten wir $\mathrm{reach}[i, k](x, u, X)$ und wir haben $\mathrm{reach}[k, \ell](u, v, X)$ oder $\mathrm{reach}[\ell, k](v, u, X)$, je nachdem, ob das erste Auftreten von u auf dem Pfad vor dem ersten Auftreten von v liegt oder umgekehrt. Damit ist die Formel erfüllt.

Um die andere Richtung zu zeigen sei die Formel $\mathrm{Reach}[i, j](x, y, X)$ erfüllt.

Wir betrachten Folgen $(x_1, \ldots, x_m)$, $x_k \in X$ und $(q(1), \ldots q(m))$, $q(k) \in Q$, $1 \leq k \leq m$, mit maximaler Länge m so, dass:

- $x = x_1$,
- $x_k \neq x_\ell$ für alle $1 \leq k < \ell \leq m$,
- $\mathrm{reach}[q(k-1), q(k)](x_{k-1}, x_k, X)$ für alle $2 \leq k \leq m$,
- $x_k \in X_{q(k)}$ für $k = 2, \ldots, m$.

Weil $\mathrm{Reach}[i, j](x, y, X)$ erfüllt ist, erhalten wir $x \in X_i$ und damit $q(1) = i$.

Angenommen, es gäbe einen Knoten v in X mit $v \notin \{x_1, \ldots, x_m\}$. Wegen $X = X_1 \cup \cdots \cup X_n$, gibt es ein ℓ, so dass $v \in X_\ell$. Und weil $\mathrm{reach}[i, \ell](x, v, X)$ gilt, gibt es ein maximales $k \leq m$ mit $\mathrm{reach}[q(k), \ell](x_k, v, X)$.

Ist $k+1 \leq m$, dann gilt $\mathrm{reach}[q(k+1), \ell](x_{k+1}, v, X)$ nicht (da k maximal gewählt war), damit haben wir $\mathrm{reach}[\ell, q(k+1)](v, x_{k+1}, X)$, weil $\mathrm{reach}[k, \ell](u, v, X) \vee \mathrm{reach}[\ell, k](v, u, X)$ für alle $u \in X_k$ und $v \in X_\ell$.

In jedem Fall ist die Folge $(x_1, \ldots, x_k, v, x_{k+1}, \ldots, x_m)$ länger als $(x_1, \ldots, x_m)$ und erfüllt alle Bedingungen an $(x_1, \ldots, x_m)$. Ein Widerspruch zur maximalen Länge von $(x_1, \ldots, x_m)$. Wir erhalten damit $X = \{x_1, \ldots, x_m\}$.

Schließlich gilt $\mathrm{reach}[q(m), j](x_m, y, X)$, weswegen der gewünschte Pfad existiert.

□

6.2 Die Entscheidbarkeit der FO-Theorie der Struktur $\mathcal{C}(\mathrm{IM}(G)/P)$

Wir sind nun in der Lage, das Hauptresultat dieses Kapitels zu beweisen. Dazu benötigen wir folgendes Pendant zu Theorem 2.4.4:

Theorem 6.2.1 ([42]) *Die MSO-Theorie des Cayleygraphen einer (unendlichen) endlich erzeugten virtuell freien Gruppe ist entscheidbar.*

Beweis (von Theorem 6.0.1): Wir transformieren jede FO-Formel φ über der Signatur der Struktur $\mathcal{C}(\mathrm{IM}(G)/P)$ in eine MSO-Formel $\hat{\varphi}$ über der Signatur des Cayleygraphen $\mathcal{C}(G, \Delta)$ der virtuell freien Gruppe G so, dass

$$\mathcal{C}(\mathrm{IM}(G)/P)) \models \varphi \text{ genau dann wenn } \mathcal{C}(G, \Delta) \models \hat{\varphi}$$

Dazu assoziieren wir nun zu jeder Variable erster Stufe $x = (U, g)$ in $\mathrm{IM}(G)/P$ zwei Variablen:

- eine FO-Variable x' die g repräsentiert und
- eine MSO-Variable X', die U repräsentiert.

Wegen Theorem 3.4.1 ist $x = y$ genau dann, wenn $x' = y'$ und $\mathrm{cl}_P(X') = \mathrm{cl}_P(Y')$. Dies beschreibt die folgende Formel über der Signatur von $\mathcal{C}(G, \Delta)$:

$$\text{istGleich}(x', X', y', Y') = (x' = y' \ \wedge \ \exists Z : \mathrm{cl}_P(X', Z) \wedge \mathrm{CL}_P(Y', Z).$$

Die Formel $\mathrm{CL}_P(X, X')$ ist bereits bekannt.

Wir müssen nun noch ausdrücken, dass (X', x') tatsächlich ein Element aus $\mathrm{IM}(G)/P$ repräsentiert. Dies geschieht durch folgende Formel:

$$\text{istElement}(x', X') = (1, x' \in X' \ \wedge \ \text{endlich}(X').$$

Bleibt noch, eine MSO-Formel (über der Signatur von $\mathcal{C}(G, \Delta)$) für die Endlichkeit einer Menge X' in der virtuell freien Gruppe anzugeben. Dazu nutzen wir, dass wir in Bemerkung 2.3.1 bereits eine Formel endlich(X) über der Signatur eines endlichen Baums T von endlichem Grad angegeben haben, mit $T \models$ endlich(X) genau dann, wenn X eine endliche Menge von Knoten aus T ist. Mit anderen Worten, für eine endlich erzeugte Gruppe $F = \mathrm{FG}(\Gamma)$ können wir Endlichkeit einer Teilmenge über der Signatur von $\mathcal{C}(\Gamma)$ ausdrücken.

Wir erinnern daran, dass $G = \bigcup_{h \in H} Fh$, mit endlichem H und F endlich erzeugt, weil G dies ist. Damit ist eine Menge $X' \subseteq G$ offenbar genau dann unendlich, wenn sie mit einer Nebenklasse Fh von F in G unendlichen Schnitt $Bh = X' \cap Fh$ für ein $h \in H$ hat (da die Anzahl der Nebenklassen endlich ist).

Wir erhalten die folgende MSO-Formel über der Signatur von $\mathcal{C}(G, \Delta)$:

$$\begin{aligned} \text{unendlich}(X') \ := \ & \exists B \subseteq F \wedge \neg\text{endlich}(B) \wedge \\ & \bigvee_{h \in H} Bh_i \subseteq X'. \end{aligned}$$

Mit anderen Worten, $\mathcal{C}(G, \Delta) \models \text{unendlich}(X')$ genau dann, wenn X' eine endliche Menge von Knoten in $\mathcal{C}(G, \Delta)$ ist.

Sei nun φ eine FO-Formel über der Signatur von $\mathcal{C}(\mathrm{IM}(G)/P)$. Wie definieren $\hat{\varphi}$ induktiv:

- für $\varphi = (x = y)$ definiere $\widehat{\varphi} = \text{istGleich}(x', X', y', Y')$.
- für $\varphi = \mathrm{reach}_L(x, y)$ definiere

  $$\widehat{\varphi} = \exists X'' \exists Y'' \exists Z : \left\{ \begin{array}{l} \text{istElement}(x', X'') \ \wedge \ \text{istElement}(y', Y'') \wedge \\ \text{istGleich}(x', X', x', X'') \ \wedge \ \text{istGleich}(y', Y', y', Y'') \wedge \\ Y'' = X'' \cup Z \ \wedge \ \mathrm{Reach}_L(x', y', Z) \end{array} \right\},$$

  wobei Reach_L die Formel aus Lemma 6.1.1 ist.
- für $\varphi = \neg\psi$ definiere $\widehat{\varphi} = \neg\widehat{\psi}$.

- für $\varphi = \psi_1 \wedge \psi_2$ definiere $\widehat{\varphi} = \widehat{\psi_1} \wedge \widehat{\psi_2}$.
- und für $\varphi = \exists x : \psi$ definiere $\widehat{\varphi} = \exists x' \, \exists X' : \text{istElement}(x', X') \ \wedge \ \widehat{\psi}$.

Wir betrachten die Formel

$$\exists X'' \, \exists Y'' \, \exists Z : \left\{ \begin{array}{l} \text{istElement}(x', X'') \ \wedge \ \text{istElement}(y', Y'') \wedge \\ \text{istGleich}(x', X', x', X'') \ \wedge \ \text{istGleich}(y', Y', y', Y'') \wedge \\ Y'' = X'' \cup Z \ \wedge \ \mathrm{Reach}_L(x', y', Z) \end{array} \right\} \tag{6.1}$$

genauer. Es ist $\mathrm{Reach}_L(x', y', Z)$, das heißt, es gibt einen Pfad von x' nach y' in $\mathcal{C}(G, \Delta)$ der genau die Knoten in Z besucht und ein Wort aus der rationalen Menge L durchläuft. Es gibt also $a_1, \ldots, a_n \in \Delta$ mit

$$x' a_1 \cdots a_n = y'$$

in $\mathrm{IM}(G)/P$.

Da alle Knoten in der Menge Z besucht werden gilt:

$$Z = \bigcup_{i=0}^{n} x' a_1 \cdots a_i,$$

mit anderen Worten

$$(x'^{-1} Z, x'^{-1} y') = (\bigcup_{i=0}^{n} a_1 \cdots a_i, a_1 \cdots a_n) \in L.$$

Ferner ist $Y'' = X'' \cup Z$, das heißt

$$\begin{aligned} (X'', x')(x'^{-1} Z, x'^{-1} y') &= (X'' \cup x' x'^{-1} Z, x' x'^{-1} y') && (6.2) \\ &= (X'' \cup Z, y') && (6.3) \\ &= (Y'', y') && (6.4) \end{aligned}$$

wobei die erste Gleichheit schon in $\mathrm{IM}(G)$ gilt.

Wegen $\text{istGleich}(x', X', x', X'')$ und $\text{istGleich}(y', Y', y', Y'')$ gilt $(X', x') = (X'', x')$ und $(Y', y') = (Y'', y')$ in $\mathrm{IM}(G)/P$ und wir erhalten insgesamt $(X'', x')(x'^{-1} Z, x'^{-1} y') = (Y', y')$ in $\mathrm{IM}(G)/P$.

Es ist nun leicht einzusehen, dass $\mathcal{C}(\mathrm{IM}(G)/P) \models \varphi$ genau dann, wenn gilt $\mathcal{C}(G, \Delta) \models \widehat{\varphi}$. Mit Theorem 6.2.1 folgt die Behauptung. $\square$

6.3 MSO-Logik auf dem Cayleygraph des Monoids $\mathrm{FIM}(\Gamma)$

Im Kontrast zu den Ergebnissen des vorherigen Abschnitts ist die MSO-Theorie des Cayleygraphen des frei inversen Monoids $\mathrm{FIM}(\Gamma)$ unentscheidbar. In [33] wurde ein Beweis hierfür vorgestellt, der im Cayleygraph des von zwei Elementen erzeugten frei inversen Monoids ein Gitter sucht. Calbrix hat jedoch schon in [11] gezeigt, dass es einen recht einfachen Beweis schon für frei inverse Monoide mit einem Erzeuger gibt. Der Vollständigkeit halber, geben wir diesen Beweis hier an.

Satz 6.3.1 *Sei Γ, mit $|\Gamma| \geq 1$, ein endliches Alphabet, dann ist die MSO-Theorie des Cayleygraphen von $\mathrm{FIM}(\Gamma)$ unentscheidbar.*

Beweis: Es genügt, die Behauptung für $\Gamma = \{a\}$ zu zeigen. Dazu werden wir ein unendliches Gitter als Minor des Cayleygraphen $\mathcal{C}(\mathrm{FIM}(\{a\}), \{a, a^{-1}\})$ angeben und verwenden, dass die MSO-Theorie eines ungerichteten Graphen G unentscheidbar ist, wenn es einen Minor von G gibt, der isomorph zum unendlichen Gitter ist [58]:

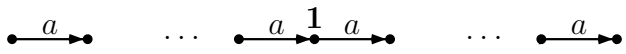
Sei $G = (V, E)$ ein ungerichteter Graph und $R \subseteq V \times V$ eine Relation auf der Knotenmenge V von G. Sei ferner G/R derjenige Graph, den man aus G erhält, wenn man alle Knoten $u, v \in V$ aus $(u, v) \in R$ identifiziert und daraus resultierende Schleifen und Mehrfachkanten entfernt. Ein Minor von G ist nun ein Graph der Form H/R, mit H Teilgraph von G.

Das unendliche Gitter ist der Graph mit Knotenmenge $\mathbb{N} \times \mathbb{N}$, wobei es zwischen den Knoten (a, b) und (c, d) genau dann eine Kante gibt, wenn entweder $a = c$ und $|b - d| = 1$ oder $|a - c| = 1$ und $b = d$.

Sei nun G derjenige ungerichtete Graph, den man durch Vergessen aller Kantenmarkierungen und -richtungen aus dem Cayleygraph $\mathcal{C}(\mathrm{FIM}(\{a\}), \{a, a^{-1}\})$ erhält. Ist $\mathrm{MSOTh}(G)$ unentscheidbar, so ist offenbar auch die MSO-Theorie der Struktur $\mathcal{C}(\mathrm{FIM}(\{a\}), \{a, a^{-1}\})$ unentscheidbar.

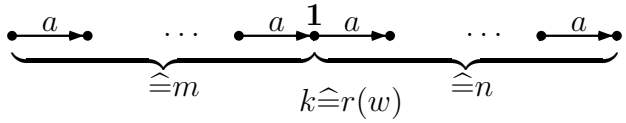
Um die Unentscheidbarkeit von $\mathrm{MSOTh}(G)$ zu zeigen, zeigen wir, dass das unendliche Gitter ein Minor von G ist.

Der Cayleygraph $\mathcal{C}(\{a\})$ der freien Gruppe $\mathrm{FG}(\{a\}) = \mathbb{Z}$ sieht folgendermaßen aus:



Entsprechend können wir den Munnbaum eines Wortes $w \in \{a, a^{-1}\}^*$ mit dem Tripel (m, k, n), identifizieren, wobei

$$\begin{aligned} m &= \min\{|v|_a - |v|_{a^{-1}} \mid v \text{ ist ein Präfix von } w\}, \\ n &= \max\{|v|_a - |v|_{a^{-1}} \mid v \text{ ist ein Präfix von } w\} \text{ und} \\ k &= |w|_a - |w|_{a^{-1}} : \end{aligned}$$



Mit dieser Darstellung von Elemente aus $\mathrm{FIM}(\{a\})$, können wir die Kante des Cayleygraphen $\mathcal{C}(\mathrm{FIM}(\{a\}), \{a, a^{-1}\})$ wie folgt definieren:

$$(m,k,n) \xrightarrow{a} \begin{cases} (m, k+1, n) & \text{falls } k+1 \leq n \\ (m, k+1, n+1) & \text{falls } k = n \end{cases}$$

$$(m,k,n) \xrightarrow{a^{-1}} \begin{cases} (m, k-1, n) & \text{falls } m \leq k-1 \\ (m-1, k-1, n) & \text{falls } k = m \end{cases}$$

Sei nun R die folgende Relation auf $\mathrm{FIM}(\{a\})$:

$$R = \{((m,k,n),(m,\ell,n)) \mid m \leq 0, n \geq 0, m \leq k, \ell \leq n\}.$$

Damit ist G/R das gesuchte unendliche Gitter. □

Kapitel 7

Rationale Mengen und das verallgemeinerte Wortproblem

7.1 Das verallgemeinerte Wortproblem

Mit den Ergebnissen des vorangehenden Kapitels lässt sich leicht die Entscheidbarkeit des verallgemeinerten Wortproblems für inverse Monoide $\mathrm{IM}(G)/P$ zeigen:

Korollar 7.1.1 *Sei P eine endlich idempotente Präsentation und G eine unendliche virtuell freie Gruppe. Dann ist das verallgemeinerte Wortproblem für inverse Monoide $\mathrm{IM}(G)/P$ entscheidbar.*

Beweis: Seien $u, u_1, \ldots, u_n \in (\Gamma \cup \Gamma^{-1})^*$ gegeben. Die Frage des verallgemeinerten Wortproblems, (liegt u in dem von $u_1, \ldots, u_n$ erzeugten Untermonoid von $\mathrm{IM}(G)/P$), lässt sich als FO-Formel über der Struktur $\mathcal{C}(\mathrm{IM}(G)/P)$ formulieren (gibt es einem mit einem Elements aus $\{u_1, \ldots, u_n\}^*$ markierten Pfad, von 1 bis zum Ende eines mit u markierten Pfads im Cayleygraph von $\mathrm{IM}(G)/P$).

Genauer gilt: u liegt genau dann in von $u_1, \ldots, u_n$ erzeugten Untermonoid, wenn gilt:

$$\exists x \exists y : x = 1 \wedge \mathrm{reach}_K(x, y) \wedge \mathrm{reach}_L(x, y)$$

wobei $K = \{u_1, \ldots, u_n\}^*$ und $L = \{u\}$.

Mit Theorem 6.0.1 folgt damit die Behauptung. □

7.2 Rationale Mengen

Es können noch etwas allgemeinere Resultate als in Abschnitt 7.1.1 gezeigt werden.

Korollar 7.2.1 *Sei P eine endlich idempotente Präsentation und G eine virtuell freie Gruppe mit Erzeugermenge Γ. Dann ist das folgende Problem entscheidbar:*

EINGABE:	*Eine boolesche Kombination $B \subseteq \mathcal{B}(\mathrm{RAT}(\mathrm{IM}(G)/P))$ von rationalen Mengen aus $\mathrm{IM}(G)/P$ (jede dieser rationalen Mengen ist etwa gegeben durch einen endlichen Automat über dem Alphabet $(\Gamma \cup \Gamma^{-1})^*$)*
AUSGABE:	*Ist $L_1 \cap L_2 \neq \emptyset$?*

Beweis: Man zeigt leicht, dass das für alle Arten von booleschen Ausdrücken das obige Leerheitsproblem in FO über $\mathcal{C}(\mathrm{IM}(G)/P)$ geschrieben werden kann.

Seien zum Beispiel $K_1, K_2 \subseteq (\Gamma \cup \Gamma^{-1})^*$ reguläre Sprachen mit $L_i = \tau(K_i)$, $i = 1, 2$. Dann ist $L_1 \cap L_2 \neq \emptyset$ genau dann, wenn

$$\mathcal{C}(\mathrm{IM}(G)/P) \models \exists x : \mathrm{reach}_{K_1}(1, x) \wedge \mathrm{reach}_{K_2}(1, x).$$

Mit Theorem 6.0.1 folgt damit die Behauptung. □

Das folgende Resultat wurde in Zusammenarbeit mit Volker Diekert und Klaus-Jörn Lange (Universität Tübingen) erzielt:

Theorem 7.2.1 *Sei $M = \mathrm{FIM}(\Gamma)$, dann ist $\mathrm{RAT}(\mathrm{FIM}(\Gamma))$ nicht unter endlichem Durchschnitt, also auch nicht unter Komplementbildung abgeschlossen, insbesondere gilt:*

$$\mathcal{B}(\mathrm{RAT}(M)) \neq \mathrm{RAT}(M).$$

Der Beweis folgt als Korollar aus den folgenden Ergebnissen. Wir erinnern daran, dass $\sigma : (\Gamma \cup \Gamma^{-1})^* \to \mathrm{FIM}(\Gamma)$ den kanonischen Homomorphismus bezeichnet.

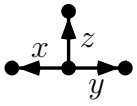
Zunächst sei $T \subseteq \mathrm{FIM}(\Gamma)$ die Menge aller Elemente von $\mathrm{FIM}(\Gamma)$ deren Munnbaum einen Knoten mindestens von Grad drei enthält:

$$T = \{(B, u) \mid B \text{ hat einen Knoten vom Grad } \geq 3\}.$$

Lemma 7.2.2 *$T \subseteq \mathrm{FIM}(\Gamma)$ ist rational.*

Beweis: Wir geben (via regulärem Ausdruck) eine Sprache $L \subseteq (\Gamma \cup \Gamma^{-1})^*$ an, mit $\sigma(L) = T$.

Dazu beschreiben wir die Existenz eines Knotens vom Grad 3. Ist $\sigma(U) \in T$, dann gibt es $x, y, z \in \Gamma \cup \Gamma^{-1}$, so dass der Munnbaum $\mathrm{MT}(u)$ den folgenden Teilgraph enthält:



Wir erhalten deshalb für

$$L = \bigcup_{\substack{x,y,z \in \Gamma \cup \Gamma^{-1} \\ x \neq y \neq z \neq x}} (\Gamma \cup \Gamma^{-1})^* x x^{-1} y y^{-1} z z^{-1} (\Gamma \cup \Gamma^{-1})^*$$

das gewünschte $\sigma(L) = T$. □

Sei nun $L \in \mathrm{FIM}(\Gamma)$ eine weitere rationale Sprache die durch den folgenden regulären Ausdruck gegeben

$$L = \{a^n a^{-m} b \mid m, n \geq 1\}$$

ist. Wir zeigen, dass der Schnitt der beiden rationalen Sprachen T und L nicht rational ist, damit folgt Theorem 7.2.1.

Lemma 7.2.3 *Seien T und L wie oben definiert. Dann ist $T \cap L$ nicht rational.*

Beweis: Es ist offenbar $T \cap L = \{a^n a^{-m} b \mid n > m\}$. Angenommen $T \cap L$ ist rational, dann existiert ein $R \subseteq (\Gamma \cup \Gamma^{-1})^*$ regulär mit $\sigma(R) = T \cap L$. Sei $\mathcal{A}$ ein endlicher Automat mit s Zuständen, der R erkennt. Sei zudem $n > s$. Dann ist

$$\sigma(a^{n+1} a^{-n} b) \in T \cap L.$$

Mit anderen Worten, es gibt $u, v_i, w \in (\Gamma \cup \Gamma^{-1})^*$ mit $u v_1 \cdots v_n w \in R$ und

$$\begin{aligned} \sigma(u v_1 \cdots v_n w) &= \sigma(a^{n+1} a^{-n} b) \\ \gamma(u) &= \gamma(a^{n+1}) \\ \gamma(v_i) &= \gamma(a^{-1}),\ 1 \leq i \leq n \\ \gamma(w) &= \gamma(b). \end{aligned}$$

Sei q_i der Zustand von $\mathcal{A}$ nach Lesen von $uv_1 \cdots v_i$. Dann existiert ein $j > i$ so dass für den Zustand q_i (Zustand von $\mathcal{A}$ nach Lesen von $uv_1 \cdots v_j$) gilt $q_i = q_j$ (wir erinnern, dass $n > s$). Daraus folgt aber

$$uv_1 \cdots v_i (v_{i+1} \cdots v_j)^k v_{j+1} \cdots v_m w \in R,$$

für alle $k \geq 0$.

Da aber $\gamma(v_i) = \gamma(a^{-1})$ erhalten wir für genügend großes k:

$$\gamma(uv_1 \cdots v_i (v_{i+1} \cdots v_j)^k v_{j+1} \cdots v_m w) = \gamma(a^{-\ell} b),$$

für ein $\ell \geq 0$.

Das zeigt jedoch, dass $\sigma(uv_1 \cdots v_i (v_{i+1} \cdots v_j)^k v_{j+1} \cdots v_m w) \notin T \cap L$, ein Widerspruch. □

Bemerkung 7.2.1 *Die obige Menge $T \subseteq \mathrm{FIM}(\Gamma)$ ist ein Beispiel einer rationalen Menge für die gilt:*

$$\mathrm{FIM}(\Gamma) \backslash T \qquad \textit{nicht rational.}$$

Betrachte dazu Elemente der Form $\sigma(a^n a^{-n} b) \in \mathrm{FIM}(\Gamma) \backslash T$ für n groß genug.

Bemerkung 7.2.2 *Da endliche Teilmengen und endlich erzeugte Untermonoide eines Monoids rational sind folgt die Entscheidbarkeit des verallgemeinerten Wortproblems für $\mathrm{IM}(G)/P$ (Korollar 7.1.1) auch schon aus Korollar 7.2.1.*

Kapitel 8

Zusammenfassung und Ausblick

Wir haben eine Konstruktion inverser Monoide $\mathrm{FIM}(\Gamma)/P$ und $\mathrm{IM}(G)/P$, beruhend auf Arbeiten von Birget und Rhodes [3, 4] sowie Margolis und Meakin [36, 37] betrachtet und konnten für dies speziellen Klassen inverser Monoide mit idempotenter Präsentation die Entscheidbarkeit des Wortproblems in linearer Zeit (auf einer RAM) zeigen. Ferner ist das uniforme Wortproblem für diese inversen Monoide EXPTIME-vollständig.

Margolis und Meakin verwenden einen Spezialfall einer von Stephen [63] vorgestellten allgemeineren Darstellung. Stephen betrachtet ferner das inverse Monoid $\mathrm{FIM}(\Sigma)/_{\cong_R}$, wobei $\cong_R$ die kleinste von $R = \{(u, v) \mid |u| = |v|, u, v \in \Sigma^*\}$ erzeugte Kongruenz in $\mathrm{FIM}(\Sigma)$ ist. Für dieses Monoid ist das Wortproblem [63] entscheidbar. Diekert, Lohrey und Miller [67] können für das frei partiell kommutative Monoid $\mathrm{FIM}(\Sigma, I) = \mathrm{FIM}(\Sigma)/_{\cong_{\widehat{I}}}$ mit Unabhängigkeitsrelation I und $\cong_{\widehat{I}}$ die kleinste von $\widehat{I} = \{(ab, ba) \mid (a, b) \in I\} \cup \{(a^{-1}b, ba^{-1} \mid (a, b) \in I\}$ erzeugte Kongruenz in $\mathrm{FIM}(\Sigma)$ zeigen, dass das Wortproblem in Zeit $O(n \log(n))$ (auf einer RAM) entscheidbar ist. Schon das verallgemeinerte Wortproblem für das frei inverse Monoid $\mathrm{FIM}(\{a, b\})$ ist NP-vollständig. Ferner zeigen Diekert, Lohrey und Miller für inverse Monoide $\mathrm{FIM}(\Sigma, I)$ mit idempotenter Präsentation, dass das Wortproblem genau dann entscheidbar ist, wenn die zu (Σ, I) entsprechende Abhängigkeitsrelation transitiv ist. Diese inversen Monoide sind als Quotientenmonoide der Form M/R definiert, können jedoch umgekehrt auch über Ersetzungen von Teilmengen definiert werden. Möglicherweise kann durch eine Modifikation letzterer Ersetzungen eine neue Beschreibung der Quotientenmonoide $\mathrm{FIM}(\Gamma)/R$ für weitere Kongruenzen R gefunden werden. Dies könnte zu Erkenntnissen über diese Monoide $\mathrm{FIM}(\Gamma)/R$ führen.

Wir haben ferner die relationale Struktur $\mathcal{C}(\mathrm{IM}(G)/P)$ mit Prädikat reach_L betrachtet. Hierfür konnten wir die FO-Theorie auf die MSO-Theorie des Cayeyleygraphen von G reduzieren und haben damit die Entscheidbarkeit der FO-Theorie von $\mathcal{C}(\mathrm{IM}(G)/P)$ erhalten. Diese impliziert, wie wir in Kapitel 7 gesehen haben, eine Reihe weiterer Resultate, insbesondere die Entscheidbarkeit des verallgemeinerten Wortproblems für $\mathrm{IM}(G)/P$ sowie die Entscheidbarkeit des Leerheitsproblems für boolesche Kombinationen rationaler Mengen in $\mathrm{IM}(G)/P$. Es stellt sich die Frage, für welche Monoide M die Struktur $\mathcal{C}(M)$ noch entscheidbar ist, bzw. für welche Monoide Unentscheidbarkeit gezeigt werden kann.

Deis, Meakin und Sénizergues [19] haben, motiviert durch die Frage nach der Lösbarkeit von Gleichungen in $\mathrm{FIM}(\Sigma)$, das Erweiterbarkeitsproblem dieses Monoids betrachtet. Dies ist die Frage, ob sich eine Lösung eines Gleichungssystems in der freien Gruppe $\mathrm{FG}(\Sigma)$ auf natürliche Weise zu einer Lösung in $\mathrm{FIM}(\Sigma)$ fortsetzen lässt. Dies bedeutet, ist $\nu(x)$ für $x \in X$, X die Menge der Unbekannten im Gleichungssystem, eine Lösung eines Gleichungssystems über der freien Gruppe $\mathrm{FG}(\Sigma)$, so ist die Frage, ob es ein Idempotent e_x gibt, so dass $e_x\nu(x)$ Lösung des Gleichungssystems über dem frei inversen Monoid $\mathrm{FIM}(\Sigma)$ ist. Für dieses Erweiterbarkeitsproblem konnten sie Entscheidbarkeit zeigen und es stellt sich die Frage, ob sich dieses Resultat auch auf $\mathrm{FIM}(\Sigma)/P$ übertragen lässt.

Literaturverzeichnis

[1] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[2] J.-C. Birget, S. W. Margolis, and J. C. Meakin. The word problem for inverse monoids presented by one idempotent relator. *Theoretical Computer Science,* 123(2):273–289, 1994.

[3] J.-C. Birget and J. Rhodes. Almost finite expansions of arbitrary semigroups. *Journal of Pure and Applied Algebra,* 32(3):239–287, 1984.

[4] J.-C. Birget and J. Rhodes. Group theory via global semigroup theory. *Journal of Algebra*, 120:284–300, 1989.

[5] J.-C. Birget, S. W. Margolis, J. C. Meakin, and M. Sapir, editors. *Algorithmic Problems in Groups and Semigroups*. Trends in Mathematics. Birkhäuser, 2000.

[6] R. Book. Confluent and other types of thue systems. *Journal of the Association for Computing Machinery*, 29(1):171–182, 1982.

[7] R. V. Book and F. Otto. *String–Rewriting Systems*. Springer, 1993.

[8] W. Boone. The word problem. *Annals of Mathematics*, 70:171–182, 1959.

[9] J. R. Büchi. Weak second-order arithmetic and finite automata. *Z. Math. Logik Grundl. Math*, 6:66–92, 1960.

[10] J. R. Büchi. On a decision method in restricted second-order arithmetic. In *Proc. 1960 Int. Congr. for Logic, Methodology and Phylosophy of Science*, pages 1–11. Standford Univ. Press, 1962.

[11] H. Calbrix. La théorie monadique du second ordre du monoïde inversif libre est indécidable (The second-order monadic theory of the free inverse monoid is undecidable). *Bulletin of the Belgian Mathematical Society*, 4:53–65, 1997.

[12] A. K. Chandra, D. C. Kozen, and L. J. Stockmeyer. Alternation. *Journal of the Association for Computing Machinery*, 28(1):114–133, 1981.

[13] C. Choffrut. Conjugacy in free inverse monoids. In H. Abdulrab and J.-P. Pécuchet, editors, *IWWERT*, volume 677 of *Lecture Notes in Computer Science*, pages 6–22. Springer, 1991.

[14] C. Choffrut and F. D'Alessandro. Commutativity in free inverse monoids. *Theoretical Computer Science*, 204(1-2):35–54, 1998.

[15] K. J. Compton and C. W. Henson. A uniform method for proving lower bounds on the computational complexity of logical theories. *Annals of Pure and Applied Logic*, 48:1–79, 1990.

[16] B. Courcelle. The monadic second-order logic of graphs vi: On several representations of graphs by logical structures. *Discrete Applied Mathematics*, 54:117–149, 1994.

[17] B. Courcelle. The expression of graph properties and graph transforamtions in monadic second-order logic. In G. Rozenberg, editor, *Handbook of Graph Grammars and Computing by Graph Transformation*, volume 1, pages 313–400. World Scientific, 1997.

[18] B. Courcelle and I.Walukiewicz. Monadic second-order logic, graph coverings and unfoldings of transition systems. *Annals of Pure and Applied Logic*, 92:35–62, 1998.

[19] T. Deis, J. Meakin, and G. Sénizergues. Equations in free inverse monoids. 2005. to appear.

[20] C. C. Elgot. Decision problems of finite automata design and related arithmetics. *Transactions of the American Mathematical Society*, 98:21–52, 1961.

[21] M. Gromov. Hyperbolic groups. In S. M. Gersten, editor, *Essays in Group Theory*, number 8 in MSRI Publ., pages 75–263. Springer-Verlag, 1987.

[22] W. Hodges. *Model Theory*. Cambridge University Press, 1993.

[23] J. E. Hopcroft and J. D. Ullman. *Introduction to automata theory, languages and computation*. Addison–Wesley, Reading, MA, 1970.

[24] A. Karrass, W. Magnus, and D. Solitar. *Combinatorial Group Theory*. Wiley, 1966.

[25] A. V. Kelarev. On undirected Cayley graphs. *Australasian Journal of Combinatorics*, 25:73–78, 2002.

[26] A. V. Kelarev and C. E. Praeger. On transitive Cayley graphs of groups and semigroups. *European Journal of Combinatorics*, 24(1):59–72, 2003.

[27] A. V. Kelarev and S. J. Quinn. A combinatorial property and Cayley graphs of semigroups. *Semigroup Forum*, 66(1):89–96, 2003.

[28] O. Kupferman and M. Vardi. An automata-theoretic approach to reasoning about infinite state systems. In E. A. Emerson and A. P. Sistla, editors, *Proceedings of the 12th International Conference on Computer Aided Verification (CAV 2000)*, number 1855 in Lecture Notes in Computer Science, pages 36–52. Springer-Verlag New York, Inc., 2000.

[29] D. Kuske and M. Lohrey. Logical aspects of cayley-graphs: the group case. *Annals of Pure and Applied Logic*, 131(1–3):263–286, 2005.

[30] D. Kuske and M. Lohrey. Logical aspects of cayley-graphs: the monoid case. *International Journal of Algebra and Computation*, 2005. to appear.

[31] M. V. Lawson. *Inverse Semigroups: The Theory of Partial Symmetries*. World Scientific, Singapore, 1998.

[32] R. Lipton and Y. Zalcstein. Word problems solvable in logspace. *Journal of the Association for Computing Machinery*, 24(3):522–526, 1977.

[33] M. Lohrey and N. Ondrusch. Inverse monoids: decidability and complexity of algorithmic questions. In J. Jedrzejowicz and A. Szepietowski, editors, *Proceedings of the MFCS 2005*, number 3618 in Lecture Notes in Computer Science, Berlin-Heidelberg-New York, 2005. Springer-Verlag.

[34] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory*. Springer-Verlag, 1977.

[35] S. Margolis and J. Meakin and J. B. Stephen. Some decision problems for inverse monoid presentations. In D. Reidel, editor, *Semigroups and their applications*, pages 99–110. Dordrecht, 1987.

[36] S. Margolis and J. Meakin. E-unitary inverse monoids and the cayley graph of a group presentation. *Journal of Pure and Applied Algebra*, 58:45–76, 1989.

[37] S. Margolis and J. Meakin. Inverse monoids, trees, and context-free languages. *Transactions of the American Mathematical Society*, 335(1):259–276, 1993.

[38] S. Margolis, J. Meakin, and M. Sapir. Algorithmic problems in groups, semigroups and inverse monoids. In J. Fountain, editor, *Semigroups, Formal Languages and Groups*, pages 147–214. Kluwer Academic Press, 1995.

[39] A. Markov. On the impossibility of certain algorithms in the theory if associative systems. *Doklady Akademii Nauk SSSR*, 55:58:587–590, 1947.

[40] A. Meyer. Weak monadic second order theory of one successor is not elementary recursive. In R. Parikh, editor, *Logic Colloquium (Proc. Symposium on Logic, Boston, 1972), Lecture Notes in Mathematics vol. 453*, pages 132–154. Springer-Verlag, 1975.

[41] D. E. Muller and P. E. Schupp. Groups, the theory of ends, and context-free languages. *J. Comput. Syst. Sci.*, 26:295–310, 1983.

[42] D. E. Muller and P. E. Schupp. The theory of ends, pushdown automata, and second order logic. *Theoretical Computer Science*, 37:51–75, 1985.

[43] W. Munn. Free inverse semigroups. *Proceedings of the London Mathematical Society*, 30:385–404, 1974.

[44] P. S. Novikov. *On the algorithmic unsolvability of the word problem in group theory*. Providence, R.I.: American Mathematical Society, 1958.

[45] C. H. Papadimitriou. *Computational Complexity*. Addison Wesley, 1994.

[46] M. Petrich. *Inverse semigroups*. Wiley, Stuttgart, 1984.

[47] O. Poliakova and B. M. Schein. A new construction for free inverse semigroups. *Journal of Algebra*, 288:20–58, 2005.

[48] E. Post. Recursive unsolvability of a problem of thue. *Journal of Symbol Logic*, 12(1):1–11, 1947.

[49] M. O. Rabin. A simple method for undecidability proofs and some applications. In Y. Bar-Hillel, editor, *Logic, Methodology and Philosophy of Science II*, pages 58–68. North Holland, 1965.

[50] M. O. Rabin. Decidability of second-order theories and automata on infinite trees. *Transactions of the American Mathematical Society*, 141:1–35, 1969.

[51] M. O. Rabin. *Automata on Infinite Objects and Church's Problem*. American Mathematical Society, Boston, MA, USA, 1972.

[52] M. O. Rabin. Decidable theories. In J. Barwise, editor, *Handbook of mathematical logic*, pages 595–629. North-Holland, 1977.

[53] R. Reischuk. *Komplexitaetstheorie, Bd. 1: Grundlagen*. Teubner Verlag Stuttgart, 1999.

[54] E. Rips. Subgroups of small cancellation groups. *Bulletin of the London Mathematical Society*, 14:45–47, 1982.

[55] H. Scheiblich. Free inverse semigoups. *Proceedings of the American Mathematical Society*, 38:1–7, 1973.

[56] B. Schein. On the theory of generalized groups. *Doklady Akademii Nauk SSSR*, 153:296–299, 1933. english translation in Soviet Math. Dokl. 4 (1963), 1680-1683.

[57] P. E. Schupp. Groups and graphs: Groups acting on trees, ends, and cancellation diagrams. *Mathematical Intelligencer*, 1:205–222, 1979.

[58] D. Seese. The structure of the models of decidable monadic theories of graphs. *Annals of Pure and Applied Logic*, 53:169–195, 1991.

[59] P. V. Silva. Rational languages and inverse monoid presentations. *International Journal of Algebra and Computation*, 2:187–207, 1992.

[60] P. V. Silva. On free inverse monoid languages. *R.A.I.R.O. — Informatique Théorique et Applications*, 30:349–378, 1996.

[61] P. V. Silva and B. Steinberg. Extensions and submonoids of automatic monoids. *Theoretical Comput. Sci.*, 289:727–754, 2002.

[62] P. V. Silva and B. Steinberg. A geometric characterization of automatic monoids. *The Quarterly Journal of Mathematics*, 55:333–356, 2004.

[63] J. Stephen. Presentations of inverse monoids. *Journal of Pure and Applied Algebra*, 63:81–112, 1990.

[64] J. Stillwell. The word problem and the isomorphism problem for groups. *Bulletin of the American Mathematical Society*, 6:33–56, 1982.

[65] C. Stirling. *Modal and Temporal Properties of Processes*. Springer-Verlag, 2001.

[66] W. Thomas. Languages, automata, and logic. In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Languages*, volume 3, pages 389–455, New York, 1997. Springer-Verlag.

[67] A. M. Volker Diekert, Markus Lohrey. Partially commutative inverse monoids. 2006. submitted.

[68] N. R. Wagner and M. R. Magyarik. A public key cryptosystem based on the word problem. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 19–36, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[69] I. Walukiewicz. Pushdown processes: Games and model-checking. *Information and Computation*, 164(2):234–263, 2001.

[70] C. Wrathall. The word problem for free partially commutative groups. *Journal of Symbolic Computation*, 6(1):99–104, 1988.

[71] B. Zelinka. Graphs of semigroups. *Casopis. Pest. Mat.*, 106:407–408, 1981.

Index