Algorithmische Gruppentheorie

Volker Diekert[1]

Wintersemester 2018/19

[1] Übungen Armin Weiß

Vorbemerkungen

Typische algorithmische Fragestellungen für Gruppen (oder Monoide), die durch Erzeugende und Relationen endlich präsentiert sind.

1.) Wortproblem: $u = v$?

2.) Konjugation: $\exists x : xux^{-1} = v$?

3.) Mitgliedschaft in Untergruppen: $u \in H \leq G$?

4.) Mitgliedschaft in rationalen Mengen:
$u \in L(A) \subseteq G$ für einen NFA A?

5.) Isomorphieproblem: $G \cong H$?

6.) Entscheidbarkeit der existenziellen Theorie freier Gruppen.

Gliederung

1.) Einführung: $\mathrm{SL}(2,\mathbb{Z})$.
2.) Konfluente und konvergente Ersetzungssysteme.
3.) Darstellungen von Gruppen.
4.) Freie Gruppen $F(\Sigma)$ und freie Produkte.
5.) Rationale Sprachen und M-Automaten.
Entscheidbarkeitsresultate: Der Satz von Benois.
6.) Residuell endliche Gruppen und hopfsche Gruppen.
7.) Stallingsautomaten und Anwendungen.
8.) Die existentielle Theorie freier Gruppen
9.) Einrelatorgruppen.

$\mathrm{SL}(2,\mathbb{Z})$

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z} \;\&\; ad - bc = 1 \right\}$$

Beachte, $\det(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bc$.

$\mathrm{SL}(2,\mathbb{Z})$ und die Modulgruppe $\mathrm{PSL}(2,\mathbb{Z})$

$\mathrm{SL}(2,\mathbb{Z})$ operiert auf der oberen Halbebene $\{\, z \in \mathbb{C} \mid \mathrm{im}(z) > 0 \,\}$ sowie auf $\mathbb{R} \setminus \mathbb{Q}$ vermöge gebrochen linearer Transformationen:

$$A(z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}.$$

Das Bild ist die Modulgruppe $\Gamma = \mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm 1\}$.
Nachrechnen:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}(z) = \frac{a\frac{a'z+b'}{c'z+d'} + b}{c\frac{a'z+b'}{c'z+d'} + d} = \frac{(aa'+bc')z + (ab'+bd')}{(ca'+dc')z + (cb'+dd')}.$$

Ferner, $\mathrm{im}(z) > 0$ dann ist auch $\mathrm{im}(\frac{az+b}{cz+d}) > 0$.
Ist $t = A(z) \in \mathbb{R} \setminus \mathbb{Q}$, so ist $z = A^{-1}(t) \in \mathbb{R} \setminus \mathbb{Q}$.

$\Sigma^* \subseteq \mathrm{SL}(2,\mathbb{Z})$

Sei $\Sigma = \{a, b\}$. Definiere:

$$f(a) = L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad f(b) = U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Bemerkung

1.) *f ist injektiv auf* Σ^*.

2.) $f(\Sigma^*) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{N},\ ad - bc = 1 \right\}$

$\Sigma^* = \mathrm{SL}_2(\mathbb{N})$

Proof:

$$f(\Sigma^*) \subseteq \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \;\middle|\; a_i \in \mathbb{N},\ a_1 a_4 - a_2 a_3 = 1 \right\} =: \mathrm{SL}_2(\mathbb{N})$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_1 + a_3 & a_2 + a_4 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 + a_3 & a_2 + a_4 \\ a_3 & a_4 \end{pmatrix}$$

Angenommen $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{N})$ and $a_1 > a_3$ and $a_2 < a_4$. Dann gilt
$1 = a_1 a_4 - a_2 a_3 \geq (a_3 + 1)(a_2 + 1) - a_2 a_3 = a_2 + a_3 + 1$.
Daher $a_1 = a_4 = 1,\ a_2 = a_3 = 0$.

$\Sigma^* = \mathrm{SL}_2(\mathbb{N})$

Dies definiert ein Dekodierungsschema und zeigt damit

$$\Sigma^* = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \;\middle|\; a_i \in \mathbb{N},\ a_1 a_4 - a_2 a_3 = 1 \right\}$$

L, U erzeugen keine freie Untergruppe in $\mathrm{SL}(2,\mathbb{Z})$

$$f(a^{-1}ba) = f(b^{-1}a^{-1}b) \in \mathrm{SL}(2,\mathbb{Z})$$

Wir identifizieren a mit der Matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ und b mit $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und lesen beide als 2×2 Matrizen über $\mathbb{R}$.

Sei $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$. Dann gilt:

$$\begin{aligned} a^{-1}ba \begin{pmatrix} x \\ y \end{pmatrix} &= a^{-1}b \begin{pmatrix} x \\ x+y \end{pmatrix} &&= a^{-1} \begin{pmatrix} 2x+y \\ x+y \end{pmatrix} = \begin{pmatrix} 2x+y \\ -x \end{pmatrix} \\ b^{-1}a^{-1}b \begin{pmatrix} x \\ y \end{pmatrix} &= b^{-1}a^{-1} \begin{pmatrix} x+y \\ y \end{pmatrix} &&= b^{-1} \begin{pmatrix} x+y \\ -x \end{pmatrix} = \begin{pmatrix} 2x+y \\ -x \end{pmatrix} \end{aligned}$$

Es versteckt sich ein Ping Pong:

$$a \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x+y \end{pmatrix} \qquad b \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \end{pmatrix}$$

Einbettung freier Gruppen in die $\mathrm{SL}(2,\mathbb{Z})$

Betrachte die folgenden beiden Matrizen:

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

Es gilt für alle $n \in \mathbb{Z}$:

$$A^n = \begin{pmatrix} 1-n & n \\ -n & n+1 \end{pmatrix} \quad B^n = \begin{pmatrix} 1-n & -n \\ n & n+1 \end{pmatrix}.$$

Einbettung freier Gruppen in die $\mathrm{SL}(2,\mathbb{Z})$

Sei $z \in \mathbb{R} \setminus \mathbb{Q}$ und $z > 0$. Für $n \neq 0$ gilt

$$\text{Ping} \quad B^n(z) = \begin{pmatrix} 1-n & -n \\ n & n+1 \end{pmatrix}(z) = \frac{(1-n)z - n}{nz + n + 1} < 0$$

Analog, sei $z \in \mathbb{R} \setminus \mathbb{Q}$ und $z < 0$. Dann gilt

$$\text{Pong} \quad A^n(z) = \begin{pmatrix} 1-n & n \\ -n & n+1 \end{pmatrix}(z) = \frac{(1-n)z + n}{-nz + n + 1} > 0$$

Frage: Wann ist $B^n(z) < 0$ für $n \neq 0$?
Antwort: Für $n = 1$ gilt $B^n(z) < 0 \iff z > -2$
Für $n \neq 1$ betrachte die Parabel $y = ((1-n)z - n)(nz + n + 1)$ mit den Nullstellen $-1 - \frac{1}{n}$ und $-1 - \frac{1}{n-1}$. Nur innerhalb dieses Intervalls (innerhalb der negativen Zahlen) ist $B^n(z)$ positiv.

Einbettung freier Gruppen in die $\mathrm{SL}(2,\mathbb{Z})$

Sei $W = B^{m_1}A^{n_1}B^{m_2}\cdots$ ein endliches Produkt aus A, B mit $m_i, n_i \in \mathbb{Z}$ und alle Exponenten (bis auf evtl. m_1) seien von Null verschieden.
Zu zeigen ist $W \neq 1 \in \mathrm{SL}(2,\mathbb{Z})$.
Ohne Einschränkung sei $W = B^{m_1}A^{n_1}\cdots B^{m_k}A^{n_k}B^{m_{k+1}}$, alle $n_i, m_i \neq 0$ und $k \geq 1$.
(Die B-Matrizen am Anfang und Ende können durch Konjugation von W erreicht werden.)
Sei $z \in \mathbb{R} \setminus \mathbb{Q}$ und $z > 0$.
Ping-Pong-Argument: Dann ist $W(z) < 0$, also $W \neq 1$. □

Ersetzungssysteme

Ein Ersetzungssystem besteht aus einer Menge X und einer Relation $\Longrightarrow \subseteq X \times X$.

1.) $\Longleftrightarrow$ bezeichnet den symmetrischen Abschluss von $\Longrightarrow$.

2.) $\overset{+}{\Longrightarrow}$ bezeichnet den transitiven Abschluss.

3.) $\overset{*}{\Longrightarrow}$ bezeichnet den reflexiven und transitiven Abschluss.

4.) $\overset{*}{\Longleftrightarrow}$ bezeichnet den symmetrischen, reflexiven und transitiven Abschluss, also die von $\Longrightarrow$ erzeugte *Äquivalenzrelation*.

Wir schreiben auch $y \Longleftarrow x$, falls $x \Longrightarrow y$ und $x \overset{\leq k}{\Longrightarrow} y$, falls y in höchstens k Schritten von x aus erreicht werden kann.

Definition

Eine Relation $\Longrightarrow \subseteq X \times X$ heißt

i.) *stark konfluent*, falls $y \Longleftarrow x \Longrightarrow z$ impliziert $\exists w : y \overset{\leq 1}{\Longrightarrow} w \overset{\leq 1}{\Longleftarrow} z$

ii.) *konfluent*, falls $y \overset{*}{\Longleftarrow} x \overset{*}{\Longrightarrow} z$ impliziert $\exists w : y \overset{*}{\Longrightarrow} w \overset{*}{\Longleftarrow} z$

iii.) *Church-Rosser*, falls $y \overset{*}{\Longleftrightarrow} z$ impliziert $\exists w : y \overset{*}{\Longrightarrow} w \overset{*}{\Longleftarrow} z$

iv.) *lokal konfluent*, falls $y \Longleftarrow x \Longrightarrow z$ impliziert $\exists w : y \overset{*}{\Longrightarrow} w \overset{*}{\Longleftarrow} z$

v.) *terminierend*, falls jede unendliche Kette

$$x_0 \overset{*}{\Longrightarrow} x_1 \overset{*}{\Longrightarrow} \cdots x_{i-1} \overset{*}{\Longrightarrow} x_i \overset{*}{\Longrightarrow} \cdots$$

stationär wird,

vi.) *konvergent* oder auch *vollständig*, falls sie lokal konfluent und terminierend ist.

Resultate

Es gilt:

i.) Starke Konfluenz impliziert Konfluenz.

ii.) Konfluenz ist äquivalent zur Church-Rosser-Eigenschaft.

iii.) Konfluenz impliziert lokale Konfluenz, aber die Umkehrung ist im Allgemeinen falsch.

iv.) Konvergenz impliziert Konfluenz (d.h. ein lokal konfluentes System, welches terminierend ist, ist konfluent).

Die Beweise sind nicht schwierig. Siehe Tafel

Ersetzungssystem über Monoiden

Sei M ein Monoid. Ein *Ersetzungssystem* über M ist eine Relation $S \subseteq M \times M$. Es definiert die Ersetzungsrelation $\underset{S}{\Longrightarrow} \subseteq M \times M$ durch

$$x \underset{S}{\Longrightarrow} y \text{ genau dann, wenn } x = p\ell q,\ y = prq \text{ und } (\ell, r) \in S.$$

Die Relation $\overset{*}{\underset{S}{\Longleftrightarrow}} \subseteq M \times M$ ist eine *Kongruenz*. Dies bedeutet, wir können Äquivalenzklassen multiplizieren, indem wir Repräsentanten multiplizieren:

$$[x] \cdot [y] = [xy]$$

Die Kongruenzklassen bilden ein Monoid, das wie folgt bezeichnet wird: $M/\overset{*}{\underset{S}{\Longleftrightarrow}}$ oder $M/\{\, \ell = r \mid (\ell, r) \in S \,\}$ oder einfach M/S

Definierende Gleichungen

Sei $G = M/\overset{*}{\underset{S}{\Longleftrightarrow}} = M/S$. Dann nennen wir S auch definierende Gleichungen von M für G.
Ist $G \tilde{=} \Delta^*/\overset{*}{\underset{S}{\Longleftrightarrow}} = \Delta^*/S$, so heißt das Paar (Δ, S) auch eine Darstellung von G.

G ist genau dann eine Gruppe, wenn:

$$\forall a \in \Delta\ \exists w_a \in \Delta^* : aw_a \overset{*}{\underset{S}{\Longleftrightarrow}} 1.$$

1.) G heißt *endlich erzeugt* (Abk. f.g.), falls es eine Darstellung (Δ, S) mit $|\Delta| < \infty$ gibt.
2.) G heißt *endlich präsentiert* (Abk. f.p.), falls es eine Darstellung (Δ, S) mit $|\Delta| < \infty$ und $|S| < \infty$ gibt.
3.) S heißt stark konfluent oder konfluent etc., falls dies für $\overset{}{\underset{S}{\Longrightarrow}}$ gilt.

Für $(\ell, r) \in S$ schreiben wir auch $\ell \longrightarrow r \in S$ und $\ell \longleftrightarrow r \in S$ falls sowohl $(\ell, r) \in S$ als auch $(r, \ell) \in S$.

Freie Gruppen

Es sei $\Delta = \Sigma \cup \overline{\Sigma}$, wobei $\overline{\Sigma}$ eine disjunkte Kopie von Σ sei.
Wir nehmen stets $\overline{\overline{a}} = a$ für Buchstaben aus Δ an; und setzen

$$\overline{a_1 \cdots a_n} = \overline{a_n} \cdots \overline{a_1}$$

Betrachte das konvergente System S:

$$S = \{\, a\,\overline{a} \longrightarrow 1 \mid a \in \Delta \,\}$$

Dann ist $F(\Sigma) = \Delta^*/S$ die *freie Gruppe* mit Basis Σ. Ist G eine beliebige Gruppe, so gilt:

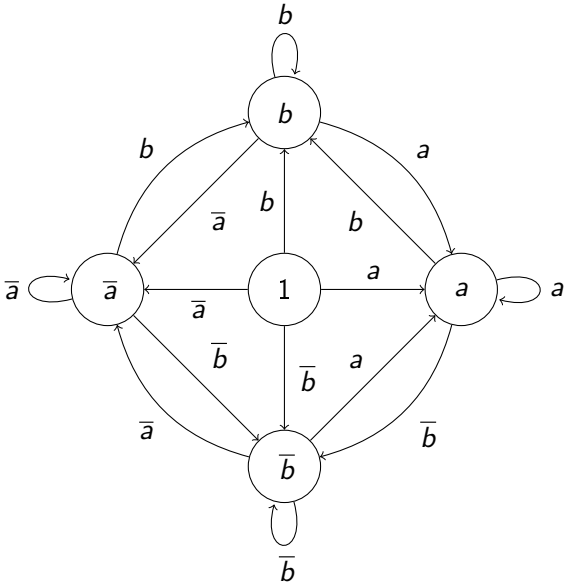
$$\mathrm{Hom}(F(\Sigma), G) = \mathrm{Abb}(\Sigma, G).$$

Gruppenelemente haben *Normalformen*. Dies sind Wöter ohne Faktoren $a\,\overline{a}$ (also auch ohne Faktoren $\overline{a}a$). Die reguläe Menge der Normalformen wird von einem DFA mit $|\Delta| + 1$ Zuständen erkannt.

$$\mathrm{NF} = \Delta^* \setminus \bigcup_{a \in \Delta} \Delta^* a\,\overline{a}\Delta^*$$

Das Wortproblem für $F(\Sigma)$ kann in linearer Zeit entschieden werden.

DFA für Normalformen in $F(a, b)$



Darstellung freier Gruppen durch Walther Ritter von Dyck

(Dyck 1882): Wähle als Erzeugende $\Sigma = \{ a, b, c \}$ mit den definierenden Gleichungen.

$$\begin{aligned} abc &= 1 \\ bca &= 1 \\ cab &= 1 \end{aligned}$$

Dies liefert eine Darstellung der $F(a, b)$ ohne negative Exponenten.
Die Teilmengenbeziehung $\{ a, b \} \subseteq \{ a, b, c \}$ liefert:

$$F(a, b) \tilde{\to} \{ a, b, c \}^* / \{ abc = bca = cab = 1 \}.$$

Randbemerkung zu Dyck-Sprachen

In der Theorie Formaler Sprachen spielen Dyck-Sprachen eine wichtige Rolle, die Namensgebung geht offenbar auf Chomsky/Schützenberger (1963) zurück. Sie schrieben: *We define the Dyck language ...*

$D^* = \{w \in \{a, \overline{a}, b, \overline{b}\}^* \mid w = 1 \in F(a,b)\}$

$=$ symmetrische Dyck-Sprache.

Bsp.: $b\overline{a}a\overline{b}ba\overline{a}\overline{b} \in D^*$

$D_2 =$ Menge der richtig geklammerten Ausdrücke mit zwei Klammerpaaren: $a = [, \quad \overline{a} =], \quad b = (, \quad \overline{b} =)$

Bsp.: `[[(())(())]]` $\in D_2$

`)[[)]` $\notin D_2$

`[(])` $\notin D_2$

Der Bezug zu den freien Gruppen ergibt sich, da die (kontext-freie) Sprache D^* genau die Wörter beschreibt, die in $F(a,b)$ die Eins darstellen.

Darstellung der $\mathrm{SL}(2,\mathbb{Z})$

$\mathrm{SL}(2,\mathbb{Z})$ wird erzeugt von $\rho = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ und $\tau = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Es gilt $\rho^3 = \tau^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ und daher auch $\tau^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$.

Behauptung

$$\mathrm{SL}(2,\mathbb{Z}) = \{\, \rho, \tau \,\} \,/\, \{\, \rho^3 = \tau^2, \tau^4 = 1 \,\}\,.$$

Beweisskizze zum Selbsttest: Ein konvergentes System mit den Regeln:

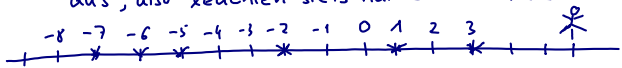
$$\begin{aligned} \tau^4 &\to 1 \\ \rho^3 &\to \tau^2 \\ \rho\tau^2 &\to \tau^2\rho \end{aligned}$$

Ping-Pong zeigt, dass irreduzible Normalformen injektiv nach $\mathrm{SL}(2,\mathbb{Z})$ abgebildet werde.

Lamplighter- und Heisenberg-Gruppe

Lamplighter group

Konfig ① Straße $= \mathbb{R}$ mit Laternen bei $\mathbb{Z}$, fast alle sind aus, also leuchten stets nur endlich viele



Lampen bei $-7, -6, -5, -2, 1, 3$

② Das Laternenmännchen M bei 7.

Operationen M geht einen Schritt nach links/rechts oder modifiziert den Status der Laterne bei seiner Position

Aufgabe: Mathematische Beschreibung einer Konfiguration und der Operationen. Ziel: Def. der Lamplighter-Gruppe $L(\mathbb{Z}/2\mathbb{Z})$.

Lamplighter- und Heisenberg-Gruppe

$\bigoplus_{n\in\mathbb{Z}} \{0,1\} \rtimes \mathbb{Z}$ $\qquad \bigoplus_{n\in\mathbb{Z}} \{0,1\} = \{ f : \mathbb{Z} \to \{0,1\} \mid f(n)=0 \ \forall' n \}$

$f(n) = 1 \iff$ Laterne n leuchtet

$(x_0, 1)$ = M geht nach rechts

$(x_0, -1)$ = M geht nach links

$(x_1, 1)$ = M ändert Status der Laterne

Gruppenelemente (f, p), $f : \mathbb{Z} \to \{0,1\}$, $f(n)=0$ für $n \gg 0$, $p \in \mathbb{Z}$

$$(f,p)\cdot(g,q) = (f \oplus p\cdot g,\ p+q)$$

$n \cdot (f \oplus p\cdot g) := n\cdot f + (n-p)\cdot g$ mod 2 semi-direktes Produkt

Lamplighter- und Heisenberg-Gruppe

$UT(3,\mathbb{Z})$ Heisenberg Gruppe

nach Hermann Weyl
Heisenberg-Bild = Schrödinger-Bild

Betrachte $(x,y,z) \in \mathbb{R}^3$

$$(x,y,z)\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = (x,\ ax+y,\ cx+by+z)$$

Schreibe Matrix als Vektor (a,b,c). Dann

$(a,b,c)\cdot(a',b',c') = (a+a',\ b+b',\ c+c'+ab')$

$(a,b,c)^{-1} = (-a,-b,c')$ mit

$c+c'-ab=0$. Also $c' = ab-c$.

$a_n = \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $b_n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$, $c_n = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

a_1, b_1 erzeugen $UT(3,\mathbb{Z})$. Abstrakt sei $a=a_1$, $b=b_1$, $c=c_1$

Def. gl. $[a,c]=[b,c]=1$ $\quad [x,y]=x^{-1}y^{-1}xy$

$[a,b]=c$

Konvergentes Ersetzungssystem etc

$ba \to abc$
$ca \to ac$
$cb \to bc$

Lamplighter- und Heisenberg-Gruppe

Rubiks Cube

8 Eckenstücke, 12 Kantenstücke

$24 = 8 \times 3$ Eckenfacetten, $24 = 12 \times 2$ Kantenfacetten

Cube-group $\leq S(24) \times S(24)$ etc

Nilpotente Gruppen

(1) Untere Zentralreihe

$G_0 = G \qquad G_{i+1} = [G_i, G]$ sind Normalteiler

$G_0 \trianglerighteq G_1 \trianglerighteq \cdots \qquad G_n = \{1\}$

(2) Obere Zentralreihe

$\{1\} = Z_0 \trianglelefteq Z_1 \trianglelefteq \cdots \trianglelefteq Z_n = G$

where $Z_1 = Z(G)$ = Zentrum von G

und $Z_{i+1}/Z_i = Z(G/Z_i)$

Bsp $Z[UT(3,\mathbb{Z})] = \langle c \rangle = \left\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle$, $UT(3,\mathbb{Z})/\langle c \rangle = \mathbb{Z}a + \mathbb{Z}b = \mathbb{Z} \times \mathbb{Z}$

Baumslag-Solitar Gruppen

Sei $1 \leq p \leq |q|$. Definiere

$$\mathbf{BS}_{p,q} = \left\langle \left\{ a, t \;\middle|\; ta^p t^{-1} = a^q \right\} \right\rangle.$$

Bezeichnungen; $\widetilde{a} \in \{ a, \overline{a} \}$ und $x \in \{ a, \overline{a}, t, \overline{t} \}$ mit $\overline{\overline{x}} = x$.
Spezialfall: $\mathbf{BS}_{1,2} = \mathbb{Z}[1/2] \rtimes \mathbb{Z}$.
Ein unendliches konvergentes Ersetzungssystem für $\mathbf{BS}_{1,q}$: Schiebe t nach rechts und $\overline{t} = t^{-1}$ nach links.

$$\begin{aligned} x\overline{x} &\to 1 \\ t\widetilde{a} &\to \widetilde{a}^q t \\ \widetilde{a}\overline{t} &\to \overline{t}\widetilde{a}^q \\ \overline{t}\widetilde{a}^{qm} t &\to \widetilde{a}^m \text{ für } m \in \mathbb{N} \end{aligned}$$

Baumslag-Solitar Gruppen. Ein endliches konvergentes Ersetzungssystem

$$\mathbf{BS}_{p,q} = \langle \{ a, t \mid ta^p t^{-1} = a^q \} \rangle .$$

Schiebe t und $\overline{t} = t^{-1}$ nach rechts.
Regeln mit den

$$x\overline{x} \to 1$$
$$t\widetilde{a}^p \to \widetilde{a}^q t$$
$$\overline{t}\widetilde{a}^q \to \widetilde{a}^p \overline{t}$$

Britton-Reduktion: Konfluent auf der Eins.

$$x\overline{x} \to 1$$
$$t\widetilde{a}^m \overline{t} \to \widetilde{a}^n \qquad \text{falls } m \in p\mathbb{Z} \text{ und } n = m \cdot \tfrac{q}{p}$$
$$\overline{t}\widetilde{a}^n t \to \widetilde{a}^m \qquad \text{falls } n \in q\mathbb{Z} \text{ und } n = m \cdot \tfrac{q}{p}$$

Gewichtsreduzierende Systeme und Linearzeitalgorithmen

Definiere ein Gewicht (also eine Abbildung):

$$\gamma : \Delta \to \mathbb{N}$$

Ein Wort $w = a_1 \cdots a_n$ erhält das Gewicht $\sum_{i=1}^{n} \gamma(a_i)$.
Angenommen, es gilt stets $\gamma(\ell) > \gamma(r)$ für alle $(\ell, r) \in S$.
Dann ist S terminierend.
Wir können (durch Lösen eines LGS) entscheiden, ob S gewichtsreduzierend ist.
$\{ a, b, c \}^* / \{ ab \longrightarrow c^2 \}$ besitzt keine längenreduzierende endliche konvergente Darstellung (Übungsaufgabe, siehe D. 1987).
R. Book (1982): Irreduzible Nachfolger können in Linearzeit berechnet werden.

Theorem

Das Wortproblem für Monoide mit einer endlichen gewichtsreduzierenden konvergenten Darstellung kann in Linearzeit gelöst werden.

Beweisskizze

Eingabe $w \in \Delta^*$ mit $|w| = n$.

1. $(u, v) := (1, w)$
2. while $v \neq 1$ do
   - write $v = av'$ with $a \in \Delta$
   - if $ua = u'\ell$ for some $(\ell, r) \in S$
     then $(u, v) := (u', rv')$
     else $(u, v) := (ua, v')$ fi

   endwhile

   return u

Invarianten: $uv \overset{*}{\underset{S}{\Longleftrightarrow}} w$ und $u \in \mathrm{IRR}(S)$.

Termination nach $\mathcal{O}(n)$, denn für ein geeignetes $\varepsilon > 0$ verringert jeder Schleifendurchlauf das Gewicht

$$\gamma'(u, v) = (1 - \varepsilon)\gamma(u) + \gamma(v).$$

Semi-Entscheidbarkeiten für f.p. Gruppen

1.) Sei G endlich präsentiert, d.h. $G = \Delta^*/S$ mit $|\Delta \cup S| < \infty$.
Dann ist das Wortproblem für G semi-entscheidbar.

2.) Seien G und H endlich präsentiert. Dann gilt:
- $\mathrm{Hom}(G, H)$ ist aufzählbar.
- Das Isomorphieproblem $G \overset{?}{\cong} H$ semi-entscheidbar.

Isomorphie ist semi-entscheidbar

Betrachte $G \cong \Delta^*/\overset{*}{\underset{S}{\Longleftrightarrow}}$ und $H \cong \Delta'^*/\overset{*}{\underset{S'}{\Longleftrightarrow}}$, wobei G und H Gruppen seien. Dann

$$\mathrm{Hom}(G,H) = \left\{ h \in \mathrm{Abb}(\Sigma, \Delta'^*) \;\middle|\; h(\ell) \overset{*}{\underset{S'}{\Longleftrightarrow}} h(r) \forall (\ell, r) \in S \right\}.$$

$h : G \to H$ ist surjektiv, wenn $h : \Delta^* \to H$ dies ist. Das heißt:

$$\forall a' \in \Sigma' \exists w \in \Sigma^* : h(w) \overset{*}{\underset{S}{\Longleftrightarrow}} a'$$

$h : G \to H$ ist ein Isomorphismus, wenn es zudem eine Abbildung $s : \Sigma' \to \Delta^*$ gibt mit

1.) $s(\ell') \overset{*}{\underset{S}{\Longleftrightarrow}} s(r')$ für alle $(\ell', r') \in S'$,

2.) $sh(a) \overset{*}{\underset{S}{\Longleftrightarrow}} a$ für alle $a \in \Sigma$.

Residuell-$\mathcal{C}$ Gruppen

Sei $\mathcal{C}$ eine Klasse von Gruppen.

Definition

G heißt residuell-$\mathcal{C}$, falls es für alle $1 \neq x \in G$ einen Homomorphismus $h : G \to H \in \mathcal{C}$ gibt mit $h(x) \neq 1$.

Proposition

Sei $\mathcal{C}$ eine Klasse von endlich erzeugter (f.g.) Gruppen mit entscheidbarem Wortproblem. Die Klasse $\mathcal{C}$ zusammen mit den Algorithmen sei aufzählbar.
Sei G endlich präsentiert und residuell-$\mathcal{C}$. Dann hat G ein entscheidbares Wortproblem.

Freie Gruppen sind residuell endlich

Automatentheoretische Sicht.

Proposition

Sei $1 \neq x \in F(\Sigma)$ *mit* $|x| < n$. *Dann gibt es einen Homomorphismus* $h : F(\Sigma) \to G$ *mit* $h(x) \neq 1$, *wobei* $|G| \leq n!$ *gilt.*

Beweis. Sei $Q = \{ a_1 \cdots a_i \mid x = a_1 \cdots a_m, 0 \leq i \leq m \}$ die Menge der Präfixe von x in Normalform. Also $|Q| = m + 1 \leq n$ und:

$$x \in Q \subseteq \Delta^* \setminus \cup_{a \in \Delta} \Delta^* a \bar{a} \Delta^* = F(\Sigma).$$

Für $a \in \Sigma$ definiere eine partielle Injektion $s_a : g \mapsto ga$, falls $g, ga \in Q$.
Da Q endlich ist, können wir s_a zu einer Permutation σ_a von von Q fortsetzen. Dies definiert einen Homomorphismus

$$\sigma : F(\Sigma) \to \mathrm{Perm}(Q)$$

mit $\sigma(x) \neq \mathrm{id}_Q$, da $\sigma(x)(1) = x \neq 1$. □

Freie Gruppen sind residuell endlich

"Modulare" Sicht.

Proposition

Sei $1 \neq x \in F(\Sigma)$ *mit* $|x| < n$. *Dann gibt es einen Homomorphismus* $h : F(\Sigma) \to G$ *mit* $h(x) \neq 1$, *wobei* $|G|$ *polynomiell in* n.

Beweis. Bette $F(\Sigma)$ in die $\mathrm{SL}(2, \mathbb{Z})$ ein. Sei X die Matrix, die zu x gehört. Dann ist $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = X - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ nicht die Nullmatrix. Ohne Einschränkung sei $a \neq 0$. Wähle $p \in \mathbb{N}$ mit $a \not\equiv 0 \bmod p$. Dann ist $X \bmod p$ nicht die 1 in $\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})$. □

Man kann zeigen (Wachstum der Koeffizienten ist durch $3^{|x|}$ begrenzt, Wachstum des $\mathrm{kgV}(n)$ is schneller als 2^n), dass p linear in n gewählt werden kann und damit $|\mathrm{SL}(2, \mathbb{Z}/p\mathbb{Z})| \in \mathcal{O}(n^3)$.

Hopfsche Gruppen

Definition

Eine Gruppe G heißt *hopfsch*, wenn jeder surjektive Homomorphismus $\alpha : G \to G$ bereits ein Automorphismus ist.

Bei Hopf ist jeder Endo, der ein Epi ist, schon ein Iso.

Beispiel

Seien V und W endlich dimensionale Vektorräume über einem einem Primkörper k (also $k = \mathbb{Q}$ oder $k = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) und sei $h : V \to W$ eine surjektiver Homomorphismus der abelschen Gruppen. Dann ist h eine lineare Abbildung und es gilt

$$\dim(V) = \dim(\ker(h)) + \dim(W).$$

Insbesondere ist V hopfsch.
Ist k endlich, so ist V endlich erzeugt. Für $V \neq \{0\}$ gilt:
Die Charakteristik von k ist genau dann positiv, wenn V residuell endlich ist.

Residuell endlich impliziert Hopf

Proposition

Sei G f.g. und residuell endlich, dann ist G hopfsch.

Beweis. Sei $\alpha : G \to G$ surjektiv. Angenommen es gäbe $\alpha(x) = 1$ mit $x \neq 1$. Wähle einen Normalteiler N so, dass G/N endlich ist mit $x \notin N$.
α induziert einen Isomorphismus $G/\alpha^{-1}(N) \to G/N$. Da G endlich erzeugt ist, gibt es nur endlich viele Homomorphismen in die endliche Gruppe G/N, also nur endlich viele $\beta^{-1}(N)$, wenn β ein Homomorphismus bezeichnet.
Alle α^n sind surjektiv für $n \in \mathbb{N}$. Daher gibt es $0 < i < j$ mit

$$\alpha^{-i}(N) = \alpha^{-j}(N).$$

Damit ist $N = \alpha^{i-j}(N)$, aber $x \in \alpha^{-1}(1) \subseteq \alpha^{i-j}(N)$ und gleichzeitig $x \notin N$.
Widerspruch. □

Residuell endlich überträgt sich die Automorphismengruppen

Proposition

Sei G f.g. und residuell endlich, dann ist $\mathrm{Aut}(G)$ residuell endlich.

Beweis:

Sei $\alpha : G \to G \in \mathrm{Aut}(G)$ nicht die Identität. Wähle x mit $\alpha(x) \neq x$ und einen Normalteiler N so, dass G/N endlich ist mit $\alpha(x)x^{-1} \notin N$.

Da G endlich erzeugt ist, gibt es nur endlich viele Homomorphismen γ in die Gruppe G/N, also gibt es nur endlich viele $\gamma^{-1}(N)$. Jedes $\beta^{-1} \in \mathrm{Aut}(G)$ induziert einen Isomorphismus

$$G/\beta(N) \to G/N.$$

Daher gibt es nur endlich viele $\beta(N)$. Damit ist

$$H = \bigcap_{\beta \in \mathrm{Aut}(G)} \beta(N)$$

ein Normalteiler vom endlichen Index.

Beweisfortführung

Jedes $\beta \in \mathrm{Aut}(G)$ induziert einen Isomorphismus $G/H \to G/H$, also haben wir einen kanonischen Homomorphismus

$$\mathrm{Aut}(G) \to \mathrm{Aut}(G/H),\ \alpha \mapsto \overline{\alpha}.$$

Offensichtlich gilt $\alpha(x)x^{-1} \notin H$ und damit $\overline{\alpha}(x) \neq x \in G/H$. □

Rationale Mengen und endliche M-Automaten

Sei M ein Monoid. Ein (endlicher) M-Automat wird durch ein Tupel $A = (Q, \delta, I, F)$ spezifiziert:

- Q ist Menge von Zuständen
- $I \subseteq Q$ initiale Zustände
- $F \subseteq Q$ finale Zustände oder Endzustände
- $\delta \subseteq Q \times M \times Q$ (endliche) Übergangsrelation

Gibt es in A einen mit $w \in M$ beschrifteten Pfad von p nach q, so schreiben wir auch $q \in p \cdot w$. Formal, $q \in p \cdot w$ gilt genau dann, wenn $\exists m \geq 0$, $u_1, \ldots, u_m \in M$, $p_0, \ldots, p_m \in Q$:

1. $w = u_1 \ldots u_m$,
2. $p = p_0$, $q = p_m$, $(p_{i-1}, u_i, p_i) \in \delta \ \forall 1 \leq i \leq m$

Wir setzen $L(A) = \{w \in M | \exists p \in I, q \in F : q \in p \cdot w\}$. Ist $|I| = 1$ und $|p \cdot w| \leq 1$ für alle $p \in Q$, $w \in M$, so heißt A deterministisch.

Rationale Mengen und endliche M-Automaten

Die Menge der *rationalen Teilmengen* $Rat(M)$ von M wird induktiv definiert:

1. $L \subseteq M$ und $|L| < \infty \Rightarrow L \in Rat(M)$,
2. $L, K \in Rat(M) \Rightarrow L \cup K, L \cdot K, L^* \in Rat(M)$.

Hierbei sei L^* das von L erzeugte Untermonoid in M, also:

$$L^* = \bigcup \{ L^i \mid i \in \mathbb{N} \}, L^{i+1} = L \cdot L^i, L^0 = \{1\}.$$

Proposition

Eine Menge $L \subseteq M$ ist genau dann rational, wenn es einen endlichen M-Automaten A gibt mit:

$$L = L(A)$$

Beweis

1. $L \in Rat(M)$: definiere A mit den Standardkonstruktionen aus der Automatentheorie.
2. (Analog zum Kleeneschen Satz)
   Sei $L = L(A)$ und $Q = \{1, \ldots, n\}$ mit $(p, 1, p) \in \delta \ \forall p$.
   Für jedes $i, j \in Q$, $k \geq 0$ setze

$$L_{i,j}^k = \{\, w \in M \mid j \in i \cdot w, \text{ Zwischenzustände in } \{1, \ldots, k\} \,\}.$$

$$L_{i,j}^0 = \{\, w \in M \mid (i, w, j) \in \delta \,\}.$$

   Dann ist $L_{i,j}^0$ endlich und $1 \in L_{i,j}^0 \forall i \in Q$. Für $k \geq 0$ gilt:

$$L_{i,j}^k = L_{i,j}^{(k-1)} \cup L_{i,k}^{(k-1)} (L_{k,k}^{(k-1)})^* L_{k,j}^{(k-1)}$$

$$L(A) = \bigcup_{i \in I, j \in F} L_{i,j}^n$$

□

Satz von Benois

Theorem

Sei Σ ein endliches Alphabet und $Rat(F(\Sigma)$ die freie Gruppe über Σ. Dann ist $Rat(F(\Sigma))$ eine effektive Boolesche Algebra.

Beweis: Satz von Benois

Zu $L = L(A) \subseteq F(\Sigma)$ konstruieren wir einen Automaten A' mit $L(A') = F(\Sigma) \setminus L$. Setze $\Delta = \Sigma \cup \overline{\Sigma}$ und $\pi : \Delta^* \to F(\Sigma)$ die natürliche Projektion. Wir interpretieren $L(A) \subseteq \Delta^*$. Damit gilt dann $L = \pi(L(A))$. Es sei Q die Zustandsmenge von A. Ohne Einschränkung gilt $\delta \subseteq Q \times \Delta \times Q$. Wir erweitern zunächst δ ohne Q oder $\pi(L(A))$ zu verändern nach der folgenden Regel, die solange wie möglich angewendet wird.

Sind $(p, a, q), (q, \overline{a}, r) \in \delta$, so nehme (den ϵ-Übergang) $(p, 1, r)$ hinzu. Entferne die ϵ-Übergänge wir üblich.

Da Q, G_i, I, Σ endlich sind, terminiert dieses Verfahren. Weiterhin gilt $\delta \subseteq Q \times \Delta \times Q$.

Beweis: Satz von Benois

Betrachte das konvergente System S:

$$a\overline{a} \rightarrow 1$$

Betrachte jetzt $w = a_1 \dots a_m \in \Delta^*$ mit $a_i \in \Delta$ und $q \in p \cdot w$ sowie $w \Rightarrow_S v$. Dann gilt auch $q \in p \cdot v$. Für $w \in \Delta^*$ sei $\hat{w} \in \mathrm{NF}$ mit $\pi(w) = \pi(\hat{w}) \in G$. Dann gilt die Implikation (aber nicht Äquivalenz)

$$w \in L(A) \Rightarrow \hat{w} \in L(A).$$

Definiere jetzt einen Δ^*-Automaten mit

$$L(A') = (\Delta^* \setminus L(A)) \cap \mathrm{NF}.$$

Dann gilt $\pi(L(A')) = G \setminus L(A)$.

Beweis: Satz von Benois

Denn sei $w' \in L(A')$. Angenommen es wäre $\pi(w') = \pi(w)$ für ein $w \in L(A)$. Dann gilt $\hat{w} \in L(A)$. Wegen $w' \in \mathrm{NF}$ ist also $\hat{w} = w'$, aber $L(A') \cap L(A) = \emptyset$ in Δ^*. Es folgt $\pi(L(A')) \subseteq G \setminus L(A)$.
Umgekehrt sei $g \in F(\Sigma) \setminus L(A)$. Wähle $\hat{w} \in \mathrm{NF}$ mit $\pi(\hat{w}) = g$. Dann gilt auch $\hat{w} \notin L(A)$, also $\hat{w} \in L(A')$. □

Monadische und reguläre Systeme

Im Folgenden sei Δ endlich. Der Beweis vom Satz von Benois lässt sich verallgemeinern:

Definition

1. Ein Ersetzungssystem $S \subseteq \Delta^* \times \Delta^*$ heißt *monadisch*, falls $|r| \leq 1$ für alle $(\ell, r) \in S$ gilt.
2. Es heißt *regulär*, falls die Menge der linken Seiten $L(S) = \{\ell \in \Delta^* | (\ell, r) \in S\}$ eine reguläre Menge bildet und zu jedem $\ell \in L(S)$ ein $r \in \Delta^*$ mit $(\ell, r) \in S$ berechenbar ist.

In einem monadischen System haben alle Regeln die Form $\ell \to 1$ oder $\ell \to a$ für ein $a \in \Delta$.
In einem regulären System S ist $\mathrm{IRR}(S)$ ebenfalls regulär, denn $\mathrm{IRR}(S) = \Delta^* L(S) \Delta^*$.

Ein allgemeinerer Satz von Benois

Theorem

Es sei Δ endlich und S ein reguläres, monadisches und konvergentes Ersetzungssystem. Dann ist $\mathrm{Rat}(M)$ eine effektive Boolesche Algebra für das Monoid $M = \Delta^*/S$.

Stallings-Automaten

Die folgenden Folien sind mir nach seinem Vortrag in Bratislava von Enric Ventura zur Verfügung gestellt worden und dann von mir bearbeitet worden. Ich bedanke mich herzlich.

Enric Ventura
Departament de Matemàtica Aplicada III
Universitat Politècnica de Catalunya

AutoMatha ABCD Workshop, Bratislava, November 25, 2008

Bezeichnungen

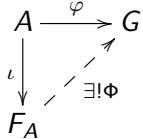
Die Bezeichnungen weichen etwas von der sonst gewählten Form ab. In diesem Abschnitt verwenden wir:

- $A = \{a_1, \ldots, a_n\}$ ist ein (endliches) Alphabet (n Buchstaben).
- $A^{\pm 1} = A \cup A^{-1} = \{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$.
- In den Beispielen gilt stets $A \subseteq \{a, b, c\}$.
- $(A^{\pm 1})^*$ bezeichnet das freie Monoid über $A^{\pm 1}$.
- 1 ist das *leere Wort*
- $F_A = F(A) = (A^{\pm 1})^* / \sim$ ist die freie Gruppe über A.
- Jedes $w \in A^*$ hat eine (frei) reduzierte Normalform $\widehat{w}$ und $|\widehat{w}|$ definiert eine Länge.
- $$|1| = 0, \quad |aba^{-1}| = |abbb^{-1}a^{-1}| = 3, \quad |uv| \leqslant |u| + |v|.$$

Die universelle Eigenschaft

Zurück zu den Grundlagen:

- Die universelle Eigenschaft: Gegeben eine Gruppe G und eine Abbildung $\varphi\colon A \to G$, dann gibt es genau einen Homomorphismus $\Phi\colon F_A \to G$ so, dass das Diagramm



  kommutiert (wobei ι die Inklusionsabbildung ist).

- Jede Gruppe ist Quotient einer freien Gruppe:

$$G = \langle a_1, \ldots, a_n \,|\, r_1, \ldots, r_m \rangle = F_A / \triangleleft r_1, \ldots, r_m \triangleright .$$

- Dies führt zum Studium des Verbandes der (normalen) Untergruppen von F_A.

Vergleich mit der linearen Algebra

Vektorräume	Freie Gruppen
• K^n endlichdim. K-VR	• F_n endlich erzeugte freie Gruppe
• Jeder K-VR hat die Gestalt K^B,	• Jede Gruppe G ist Quotient einer freien Gruppe,
• $K^n \simeq K^m \Leftrightarrow n = m$,	• $F_n \simeq F_m \Leftrightarrow n = m$,
• –	• (Nielsen-Schreier) Jede Untergruppe einer freien ist frei,
• Steinitz-Lemma (= Basisergänzungssatz)	• Nicht wahr, aber ähnliches Resultat nach M. Hall.
• $F \leqslant E \Rightarrow \dim F \leqslant \dim E$,	• **ff**: föllig falsch $F_{\aleph_0} \leqslant F_2$.

Stallings-Automaten als Spezialfall von Benois' Konstruktion

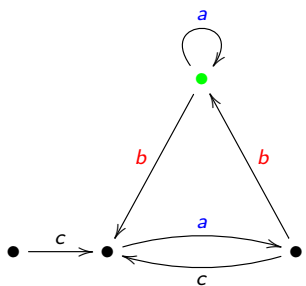
Ein Stallings-Automat ist ein endlicher A-beschrifteter orientierter Graph mit einem ausgezeichneten Basisknoten, (X, v) so, dass:

1- X ist zusammenhängend,

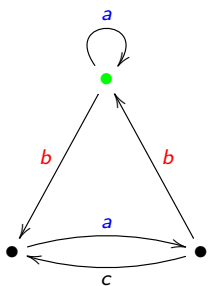
2- Kein Knoten vom Grad 1 existiert außer möglicherweise v (X ist ein Kerngraph),

3- Keine zwei verschiedenen Kanten mit gleicher Beschriftung starten im selben Knoten oder enden dort. Jede Kante e ist orientiert. Ist e mit a beschriftet, so ist $\overline{e}$ mit $\overline{a}$ beschriftet.

: −(



: −)



Stallings-Automaten

In der einflussreichen Arbeit

J. R. Stallings, Topology of finite graphs, Inventiones Math. 71 (1983), 551-565,

hat Stallings (basierend auf früheren Arbeiten) eine Bijektion zwischen endlich erzeugten Untergruppen von F_A und Stallings-Automata angegeben:

$$\{\text{end.erz. Untergruppen von } F_A\} \quad \longleftrightarrow \quad \{\text{Stallings-Automaten}\},$$

welche entscheidend für das heutige Verständnis des Untergruppenverbandes von F_A ist. Es ist davon auszugehen, dass Stallings die Arbeit von Benois nicht kannte.

Ablesen der Untergruppe aus dem Automaten

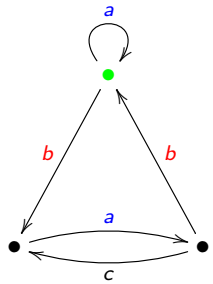
Definition

Jedem Stallings-Automaten (X, v) ordnen wir seine Fundamentalgruppe zu:

$$\pi(X, v) = \{ \text{ Beschriftungen geschlossener Pfade von } v \text{ nach } v \} \leqslant F_A,$$

Dies ist eine Untergruppe von F_A und die von (X, v) erkannte rationale Teilmenge.

$X =$



$$\pi(X, \bullet) = \{1, a, a^{-1}, bab, bc^{-1}b, bababc^{-1}cb^{-1}, \ldots\}$$

$$\pi(X, \bullet) \not\ni bc^{-1}bcaa$$

$w \overset{?}{\in} \pi(X, \bullet)$ ist entscheidbar.

Eine Basis von $\pi(X, v)$

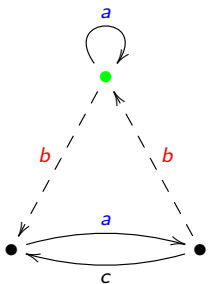
Proposition

Für jeden Stallings-Automaten (X, v) ist die Gruppe $\pi(X, v)$ frei vom Rang $rk(\pi(X, v)) = |EX| - (|VX| - 1)$ = Anzahl der Nichtspannbaumkanten

Beweis:

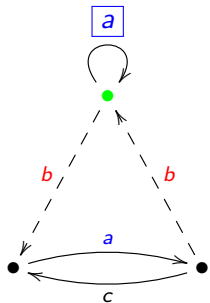
- Wähle einen maximalen Baum T in X.
- Schreibe $T[p, q]$ für die Geodätische (d.h. den eindeutig bestimmten kürzesten Pfad) in T von p nach q.
- Für jedes $e \in EX - ET$ ist $x_e = label(T[v, \iota e] \cdot e \cdot T[\tau e, v])$ Element von $\pi(X, v)$.
- Einfach zu sehen: $\{x_e \mid e \in EX - ET\}$ ist Basis von $\pi(X, v)$.
- Außerdem: $|EX - ET| = |EX| - |ET| = |EX| - (|VT| - 1)$. $\square$

Beispiel 1



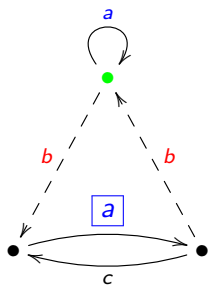
$H = \langle \quad \rangle$

Beispiel 1



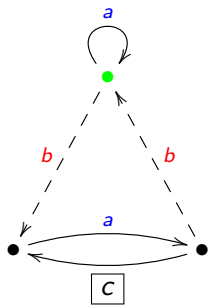
$H = \langle a, \quad \rangle$

Beispiel 1



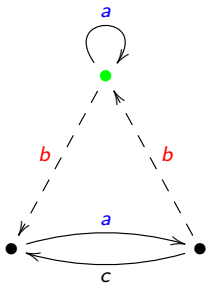
$H = \langle a,\ bab,\quad \rangle$

Beispiel 1



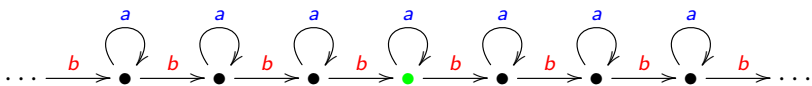
$H = \langle a,\ bab,\ b^{-1}cb^{-1} \rangle$

Beispiel 1



$H = \langle a,\ bab,\ b^{-1}cb^{-1} \rangle$
$rk(H) = 1 - 3 + 5 = 3.$

Beispiel 2

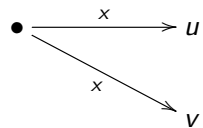


$F_{\aleph_0} \simeq H = \langle \ldots, b^{-2}ab^2, b^{-1}ab, a, bab^{-1}, b^2ab^{-2}, \ldots \rangle \leqslant F_2.$

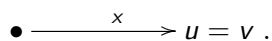
Folgerung:
Jede abzählbar erzeugte freie Gruppe ist Untergruppe der F_2.

Konstruktion des Automaten aus der Untergruppe

In jedem Automaten, welcher die folgende Konstellation enthält (mit $x \in A^{\pm 1}$),



können wir falten, d.h. die Knoten u und v identifizieren, und erhalten



Die Operation $(X, v) \rightsquigarrow (X', v)$ heißt Stallings-Faltung.
Benois würde ε-Kanten von u nach v und umgekehrt ziehen. Dann kann man in jedem NFA u und v identifizieren.
Benois würde 1-Kanten (= ε-Kanten) von u nach v und von v nach u einfügen wegen der Pfade $\overline{x}x$. Dann können u und v wie in jedem NFA identifiziert werden.

Konstruktion des Automaten aus der Untergruppe

Lemma (Stallings, Benois)

Ist $(X, v) \rightsquigarrow (X', v')$ *eine Stallings-Faltung, dann gilt* $\pi(X, v) = \pi(X', v')$ *(in* $F(A)$*).*

Dies ist klar, denn $\pi(X, v)$ ist die erkannte rationale Sprache.

Problem

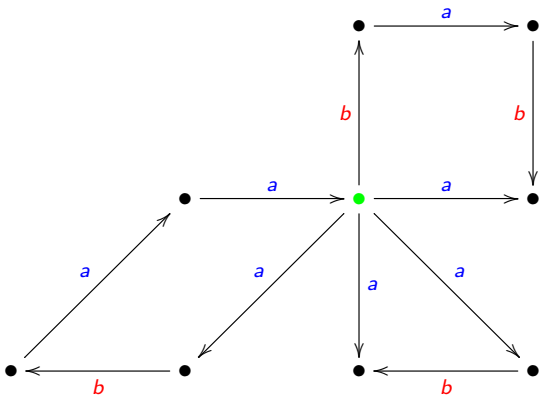
Gegeben eine endl. erz. Untergruppe $H = \langle w_1, \ldots, w_m \rangle \leqslant F_A$ *(wir nehmen an, dass die* w_i *reduzierte Wörter sind), tun wir das Folgende:*

1- *Zeichne den Blumenautomaten,*

2- *Führe sukzessive Faltungen durch, bis ein Stallings-Automat entsteht, diesen bezeichnen wir mit* $\Gamma(H)$*.*

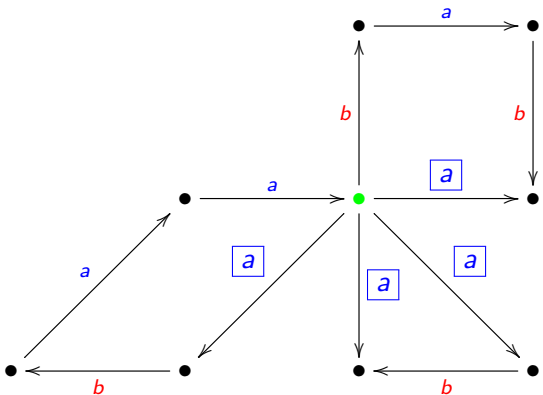
Wohldefiniertheit? Wir müssen zeigen, dass die Ausgabe nicht von der Art und Reihenfolge der durchgeführten Schritte abhängt ...
Dies ist klar nach Benois, denn $\Gamma(H)$ ist der eindeutig bestimmte minimale deterministische Automat, der die reguläre Sprache der reduzierten Normalformen erkennt.

Beispiel: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



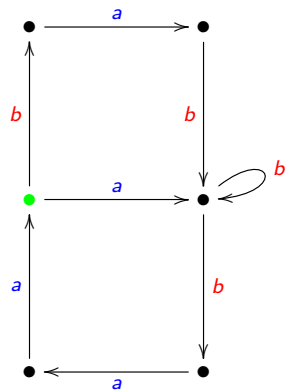
Flower(H)

Beispiel: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



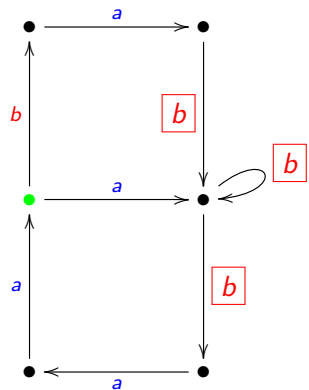
Flower(H)

Beispiel: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



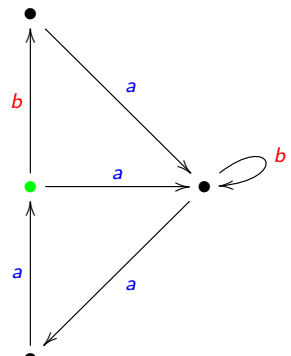
1. Faltung

Beispiel: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



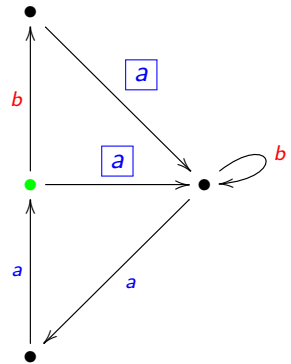
1. Faltung

Beispiel: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



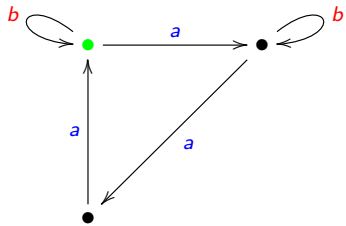
2. Faltung

Beispiel: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



2. Faltung

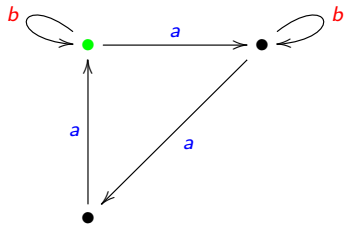
Beispiel: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



3. Faltung $\Gamma(H)$

Nach Stallings Lemma: $\pi(\Gamma(H), \bullet) = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$

Beispiel: $H = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$



3. Faltung $\Gamma(H)$

Nach Stallings Lemma: $\pi(\Gamma(H), \bullet) = \langle baba^{-1}, aba^{-1}, aba^2 \rangle$
$= \langle b, aba^{-1}, a^3 \rangle$

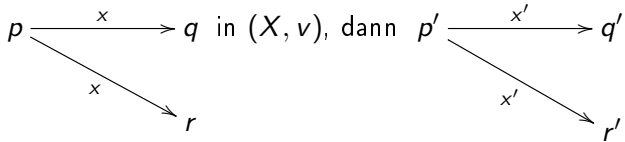
Starke Konfluenz

Proposition (Benois)

Der Automat $\Gamma(H)$ hängt nicht von der Reihenfolge der Faltungen ab.

Beweis (nach Stallings):

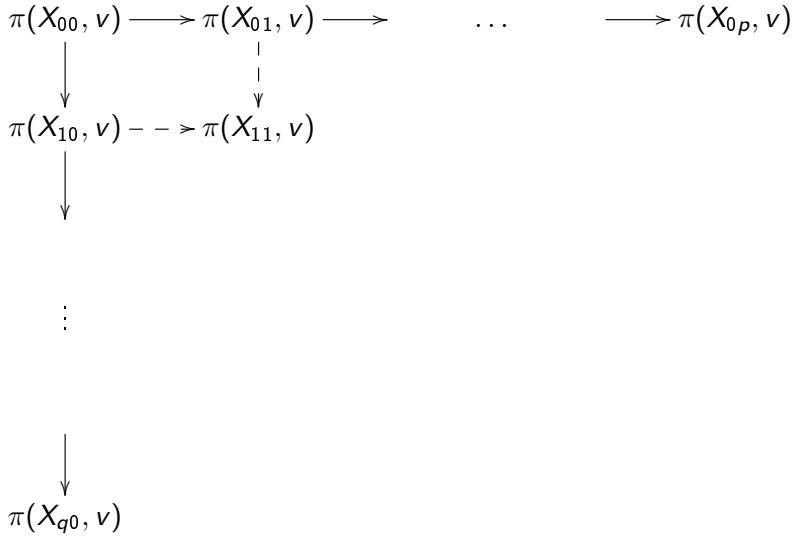
- Angenommen, $(X, v) \rightsquigarrow (X', v')$ ist eine einzelne Faltung zweier Kanten.
- Falls $p \xrightarrow{x} q$ in (X, v), dann $p' \xrightarrow{x'} q'$ in (X', v')



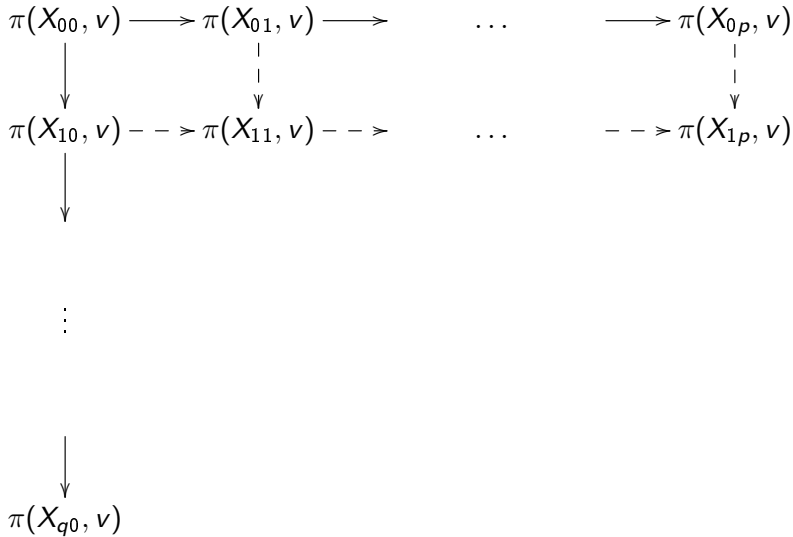
  (möglicherweise $q' = r'$).
- Also haben wir starke Konfluenz:

$$\begin{array}{ccc} (X, v) & \xrightarrow{\forall} & \pi(X', v') \\ \Big\downarrow{\scriptstyle \forall} & & \Big\downarrow{\scriptstyle \exists !} \\ \pi(X'', v'') & \xrightarrow{\exists} & \pi(X''', v''') \end{array}$$

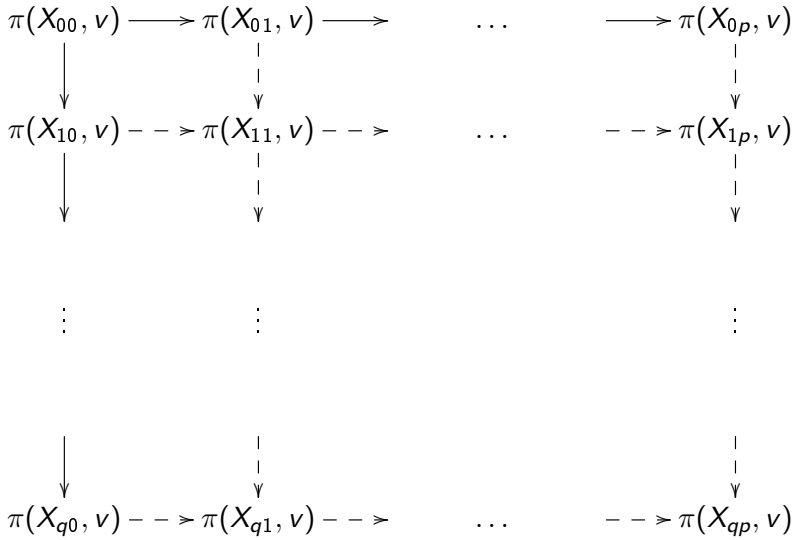
Das Konfluenzgitter



Das Konfluenzgitter

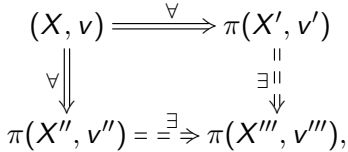


Das Konfluenzgitter



Konfluenz

- Damit haben wir Konfluenz:



  wobei $\Rightarrow$ für eine beliebige Folge von Faltungen steht.

- Wegen der Konfluenz und der Tatsache, dass Falten die Kantenzahl reduziert ist die Ausgabe eindeutig. $\square$

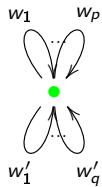
Unabhängigkeit von den Erzeugern

Proposition

Der Automat $\Gamma(H)$ hängt nicht von den Erzeugern von H ab.

Beweis:

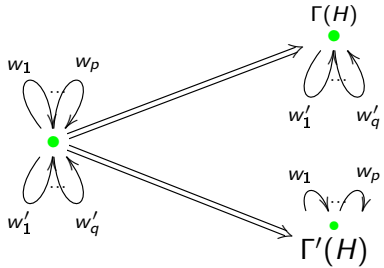
- Angenommen, $H = \langle w_1, \ldots, w_p \rangle = \langle w'_1, \ldots, w'_q \rangle$ und $\Gamma(H)$ sowie $\Gamma'(H)$ sind die daraus gewonnenen Stallings-Automaten.
- Betrachte den doppelten Blumenautomat



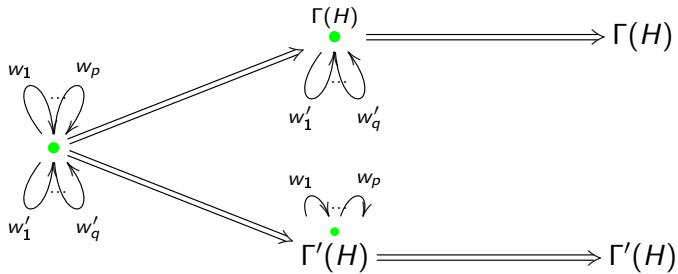
dessen Fundamentalgruppe $\langle w_1, \ldots, w_p, w'_1, \ldots, w'_q \rangle = H$ ist.

- Nun falten wir auf zwei Arten:

Unabhängigkeit von den Erzeugern



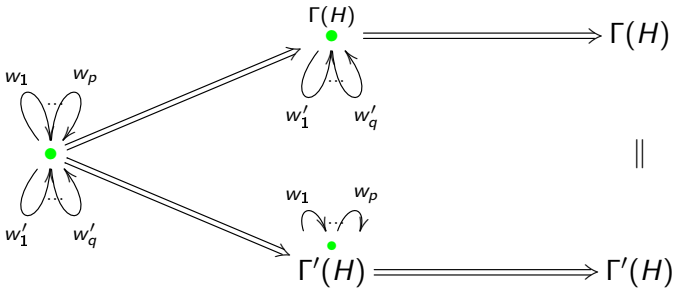
Unabhängigkeit von den Erzeugern



Lemma (Useless-w)

Falls $H \leqslant_{fg} F_A$ und $w \in H$, dann erhalten wir, wenn wir ein mit w beschriftetes Blütenblatt an den Basispunkt von $\Gamma(H)$ ankleben und falten, wieder $\Gamma(H)$.

Unabhängigkeit von den Erzeugern



Lemma (Useless-w)

Falls $H \leqslant_{fg} F_A$ und $w \in H$, dann erhalten wir, wenn wir ein mit w beschriftetes Blütenblatt an den Basispunkt von $\Gamma(H)$ ankleben und falten, wieder $\Gamma(H)$.

□

Stallings Bijektion

Theorem

Es gibt eine kanonische Bijektion:

$$\begin{array}{rcl} \{\textit{f.g. Untergruppen von } F_A\} & \longleftrightarrow & \{\textit{Stallings Automaten}\} \\ H & \mapsto & \Gamma(H) \\ \pi(X, v) & \hookleftarrow & (X, v) \end{array}$$

Beweis:

- Stallings Lemma sagt $\pi(\Gamma(H)) = H$.
- Sei (X, v) ein Stallings Automat.
  Dann ist $\pi(X, v)$ eine endlich erzeugte freie Untergruppe von (Schreier Formel) $\langle w_1, \ldots, w_p \rangle$ von F_A.
- Da (X, v) keine weiteren Stallings Faltungen erlaubt, gilt nach der Eindeutigkeit des Automaten $(X, v) = \Gamma(\pi((X, v))$.

Nielsen-Schreier-Theorem: Untergruppen freier Gruppen sind frei.

- Wir haben den Fall endlich erzeugter Untergruppen bewiesen, aber auch den allgemeinen Fall kann man daraus ableiten. (Etwas technisch.)
- Der ursprüngliche Beweis (aus den 1920ern) ist weniger durchsichtig.

Korollar (Schreiers Indexformel)

Falls $H \leqslant_{f.i.} F$ von endlichem Index $[F : H]$ ist, dann gilt
$r(H) - 1 = [F : H] \cdot (r(F_A) - 1)$.

Beweis: Der Schreiergraph mit der Eckenmenge der Rechtsnebenklassen $\{ Hg \mid g \in G \}$ und den Kanten $Hg \to Hga$ für $a \in A$ ist der Stallingsautomat. Daher: Kantenzahl - Eckenzahl + 1 = $r(F_A)[F : H] - [F : H] + 1 = r(H)$.

Korollar

Eine echte Untergruppe in F_2 vom endlichen Index hat mindestens den Rang 3.
Der Rang ist 3 genau denn wenn die Untergruppe ein Normalteiler vom Index 2 ist.

Enthaltensein und Inklusion (folgt auch aus Benois)

Problem (Enthaltensein)

Liegt w in $H = \langle w_1, \ldots, w_m \rangle$?

- Konstruiere $\Gamma(H)$,
- Prüfe, ob w als geschlossener Pfad in $\Gamma(H)$ lesbar ist (beginnend am Basispunkt).

Problem (Inklusion)

Gegeben $H = \langle w_1, \ldots, w_m \rangle$ und $K = \langle v_1, \ldots, v_n \rangle$, ist $H \leqslant K$?

- Konstruiere $\Gamma(K)$,
- Prüfe, ob alle w_i als geschlossene Pfade in $\Gamma(H)$ lesbar sind (beginnend am Basispunkt).

Basen

Problem (Berechnen einer Basis)

Gegeben $H = \langle w_1, \ldots, w_m \rangle$, finde eine Basis von H.

- Konstruiere $\Gamma(H)$,
- Wähle einen maximalen Baum,
- Lies die zugehörige Basis ab.

Konjugiertheit

Problem (Konjugiertheit)

Gegeben $H = \langle w_1, \ldots, w_m \rangle$ und $K = \langle v_1, \ldots, v_n \rangle$, sind diese konjugiert (d.h. $\exists w : wHw^{-1} = K$ für ein $w \in F_A$)?

- Konstruiere $\Gamma(H)$ und $\Gamma(K)$.
- Lösche die Basispunkte: Genauer verlege Basispunkte in Punkte v_H und v_K vom Grad 2.
- *Konsequenz: Haare schneiden.*
- Prüfe, ob die Graphen (ohne die Basispunkte) *isomorph* sind.
- Ein Pfad von v_K nach v_H hat als Beschriftung ein derartiges x und kann von v_K in $\Gamma(K)$ gelesen werden.

Korollar

Sind H und K konjugiert, so gibt es ein Wort w mit $|w| \leq |\Gamma(H)| + |\Gamma(K)|$ so, dass $K = wHw^{-1}$.

Repräsentation gewisser Nebenklassen

Seien p ein Knoten in $\Gamma(H)$ und T ein Spannbaum von $\Gamma(H)$ und $g = T[1,p] \in F_A$. Dann gilt:

1.) $1 \cdot h = 1 \cdot g = p \implies 1 \cdot gh^{-1} = 1 \implies gh^{-1} \in H$
$\implies Hg = Hh \implies 1 \cdot h = 1 \cdot g = p$

2.) $\{\, T[1,p] \in F_A \mid p \in V\Gamma(H) \,\}$ repräsentiert also $|V\Gamma(H)|$ (Rechts-)Nebenklassen in $H \backslash F_A$.

3.) Wann werden alle Nebenklassen dargestellt?

Vollständige Stallings-Automaten

Definition

Ein A-Automat heißt *vollständig*, falls für jeden Knoten p und jedes $a \in A$ mit a und mit a^{-1} beschriftete Kanten bei p ausgehen. (D.h. für jedes $a \in A^{\pm}$ geht eine mit a beschriftete Kante bei p aus.)

Lemma

Sei $\Gamma(H)$ vollständig. Dann gilt:

$$\{\, T[1,p] \in F_A \mid p \in V\Gamma(H) \,\} = H \backslash F_A.$$

Insbesondere ist H vom endlichen Index in F_A, also $H \leq_{f.i.} F_A$.

Beweis. Wir wissen schon: $\{\, T[1,p] \in F_A \mid p \in V\Gamma(H) \,\} \subseteq H \backslash F_A$. Sie jetzt $g \in F_A$, dann können wir das Wort g lesen, das zu einem Punkt im Stallingsgraphen führt. Es ist $1 \cdot g = p \in V\Gamma(H)$ definiert und damit $Hg = H\,T[1,p]$. □

Theorem

Sie $N \neq \{1\}$ ein endlich erzeugter Normalteiler von F_A und $H \leq F_A$ eine endlich erzeugte Untergruppe mit $N \leq H$. Sei $\Gamma(H)$ der Stallings Automat von H. Dann ist $\Gamma(H)$ vollständig.

Beweis. Wir zeigen zunächst, dass für jedes $a \in A^{\pm}$ ein reduziertes Wort der Form $v_a = av \in N$ gefunden werden kann: Sei w ein Erzeuger von N, schreibe w als reduziertes Wort und $w = uv\overline{u}$ mit v zyklisch reduziert. Nehme v in die erzeugende Menge auf. Betrachte jetzt ein $a \in A^{\pm}$. Kommt a in v vor, so gilt $v = v'av''$. Das Wort $av''v'$ ist reduziert und $av''v' \in N$. Kommt $\overline{a}$ in v vor, so nehme $\overline{v}$ hinzu und betrachte $\overline{v}_a$. Kommen weder a noch $\overline{a}$ in v vor, so ist $av\overline{a} \in N$ reduziert.
For jedes Wort $uw \in H$ ist jetzt auch $uv_aw \in H$ da N ein Normalteiler in H ist:

$$uv_aw = uw\ \overline{w}v_aw \in H \cdot N \subseteq H.$$

Hefte jetzt alle Wörter v_a an jeden Knoten als Einzelblume an.
Dies erzeugt keine Knoten vom Grad 1. Jetzt können alle neuen Blumen eingefaltet werden. Damit war der Stallings Automat schon vorher vollständig. □

Korollar

Sei $N \neq \{1\}$ ein endlich erzeugter Normalteiler von F_A, dann hat N endlichen Index.

Beweis. Wähle $N = H$ im obigen Theorem. $\Gamma(N)$ ist vollständig und dies impliziert endlichen Index. □

Korollar

Eine endlich erzeugte Untergruppe H von F_A ist genau dann vom endlichen Index, wenn $\Gamma(H)$ vollständig ist.

Beweis. Sei H vom endlichen Index. Zu zeigen ist noch, dass $\Gamma(H)$ vollständig ist. Betrachte hierzu einen Normalteiler $N \leq H$ mit $N \leq_{f.i.} F_A$. Wir können N wie folgt wählen:

$$N = \bigcap \left\{ gHg^{-1} \mid g \in F_A \right\}.$$

Dann gilt $N \neq \{1\}$ sind N und H endlich erzeugt und wir können das Theorem mit $\{1\} \neq N \leq H \leq F_A$ anwenden. □

Untergruppen vom endlichen Index

Bemerkung

Sei $N \neq \{1\}$ ein endlich erzeugter Normalteiler von F_A, dann ist der Stallings Automat $\Gamma(N)$ der Cayley-Graph $\mathcal{C}(F_A/N, A)$.

Bemerkung

Seien $H \leq_{f.i.} K \leq_{f.i.} F_A$. Dann induziert $1 \cdot g \in \Gamma(H) \mapsto 1 \cdot g \in \Gamma(K)$ eine Überlagerung $\varphi : \Gamma(H) \to \Gamma(K)$.
Dies bedeutet, φ ist surjektiv auf den Knoten und ist $q \cdot u$ ein Pfad der bei $q = \varphi(p)$ beginnt, so liftet sich dieser eindeutig zu einem Pfad $p \cdot u$ in $\Gamma(H)$.

Dies ist klar, denn der Beweis von eben zeigt, dass $\varphi : \Gamma(H) \to \Gamma(K)$ als Morphismus von Graphen definiert ist. Ferner ist $\Gamma(H)$ ist vollständig, also können alle Pfade eindeutig geliftet werden.

Berechnung einer Basis und der Nebenklassen

Problem (Endlicher Index)

Gegeben sei $H = \langle w_1, \ldots, w_m \rangle$
Frage: Ist $H \leqslant_{f.i.} F_A$?
Falls ja, finde Repräsentanten der Nebenklassen.

- Für $u \in V\Gamma(H)$ sei p die Beschriftung eines Pfades von $\bullet$ nach u;, dann ist

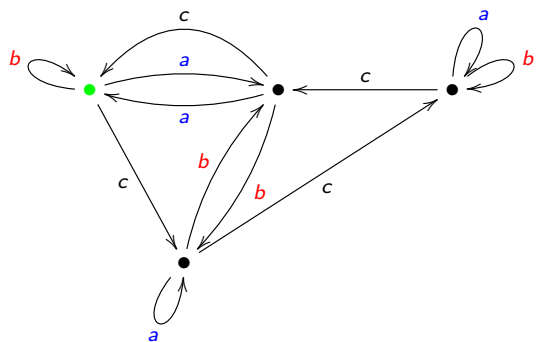
$$\{\text{Beschriftungen von Pfaden von } \bullet \text{ nach } u\} = \pi(\Gamma(H), \bullet) \cdot p = H \cdot p$$

  eine Nebenklasse aus $H \backslash F_A$.
- Konstruiere $\Gamma(H)$,
- Prüfe, ob $\Gamma(H)$ vollständig ist (d.h. zu jedem Buchstaben gibt es eine Kante in jeden und aus jedem Knoten),
- Wähle einen maximalen Baum T in $\Gamma(H)$,
- $\{T[\bullet, v] \mid v \in V\Gamma(H)\}$ ist eine Menge von Vertretern der Nebenklassen $H \leqslant_{f.i.} F_A$.

Beispiel 1

$$H = \langle b, ac, c^{-1}a, cac^{-1}, c^{-1}bc^{-1}, cbc, c^4, c^2ac^{-2}, c^2bc^{-2} \rangle$$

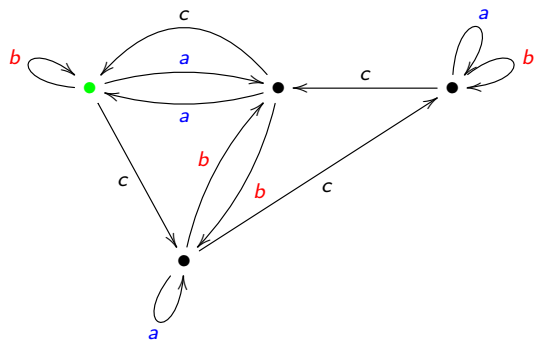
$\Gamma(H) =$



Beispiel 1

$H = \langle b, ac, c^{-1}a, cac^{-1}, c^{-1}bc^{-1}, cbc, c^4, c^2ac^{-2}, c^2bc^{-2} \rangle$

$\Gamma(H) =$



$F_3 = H \sqcup Hc \sqcup Ha \sqcup Hac^{-1}$.

Achtung: anderer Spannbaum als bei der Basisberechnung!

Mehr über Untergruppen von endlichem Index

Ein Analogon zum Basisergänzungssatz:

Theorem (M. Hall)

Jede endlich erzeugte Untergruppe $H \leqslant_{fg} F_A$ ist freier Faktor einer Untergruppe von endlichem Index: $H \leqslant_{ff} H * L \leqslant_{f.i.} F_A$

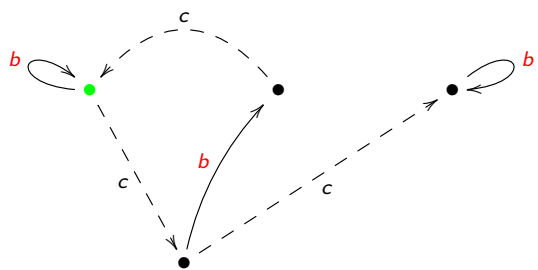
Beweis:

- Berechne $\Gamma(H)$ aus einer Menge von Erzeugenden,
- finde Knoten mit "fehlenden" ein- und ausgehenden Kanten (für jeden Erzeuger gibt es aus Gradgründen jeweils gleich viele),
- Füge neue Kanten hinzu, bis der erhaltene Automat (Y, v) vollständig ist.
- Offensichtlich ist $H = \pi(\Gamma(H)) \leqslant_{ff} \pi(Y, v) \leqslant_{f.i.} F_A$. $\square$

Beispiel

$H = \langle b, cbc, c^2bc^{-2} \rangle$

$\Gamma(H) =$

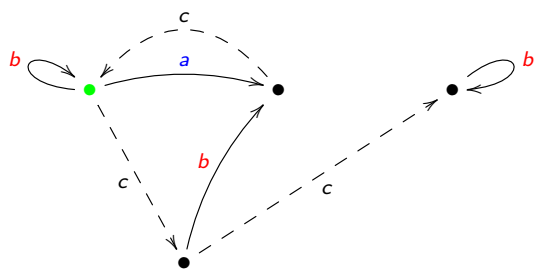


$H \leqslant_{ff} H * \langle \quad \rangle$

Beispiel

$H = \langle b, cbc, c^2bc^{-2} \rangle$

$\Gamma(H) =$

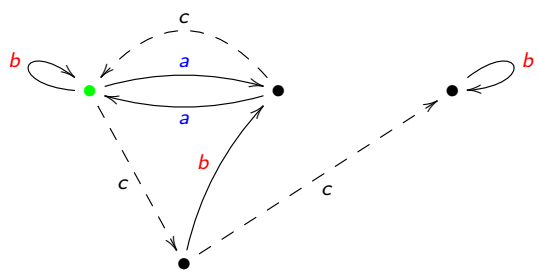


$H \leqslant_{ff} H * \langle ac \rangle$

Beispiel

$H = \langle b, cbc, c^2bc^{-2} \rangle$

$\Gamma(H) =$

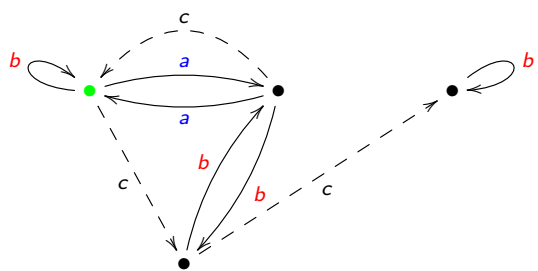


$H \leqslant_{ff} H * \langle ac, c^{-1}a \rangle$

Beispiel

$H = \langle b, cbc, c^2bc^{-2} \rangle$

$\Gamma(H) =$

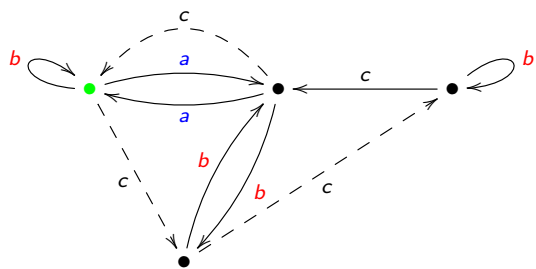


$H \leqslant_{ff} H * \langle ac, c^{-1}a, c^{-1}bc^{-1} \rangle$

Beispiel

$H = \langle b, cbc, c^2bc^{-2} \rangle$

$\Gamma(H) =$

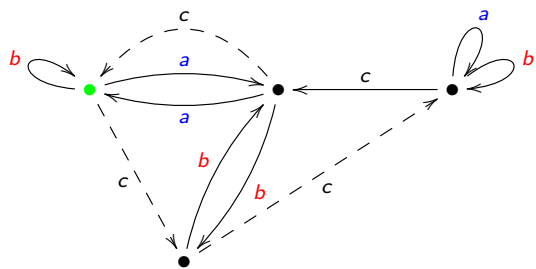


$H \leqslant_{ff} H * \langle ac, c^{-1}a, c^{-1}bc^{-1}, c^4 \rangle$

Beispiel

$H = \langle b, cbc, c^2bc^{-2} \rangle$

$\Gamma(H) =$

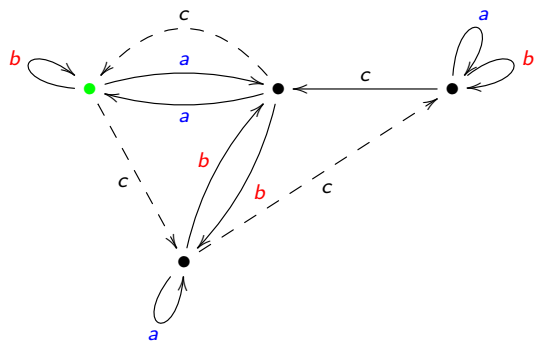


$H \leqslant_{ff} H * \langle ac, c^{-1}a, c^{-1}bc^{-1}, c^4, c^2ac^{-2} \rangle$

Beispiel

$H = \langle b, cbc, c^2bc^{-2} \rangle$

$\Gamma(H) =$



$H \leqslant_{ff} H * \langle ac, c^{-1}a, c^{-1}bc^{-1}, c^4, c^2ac^{-2}, cac^{-1} \rangle \leqslant_4 F_3.$

Das Pullback von Automaten

Definition

Das Produkt (oder Pullback) zweier Stallings-Automaten (X, v) und (Y, w) ist das kartesische Produkt $(X \times Y, (v, w))$ (verträglich mit Beschriftungen). Es ist i.A. nicht zusammenhängend und kann Knoten vom Grad 1 enthalten, aber es ist bereits zusammengefaltet (d.h. deterministisch).

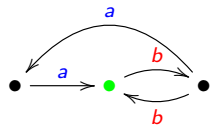
Theorem (H. , Stallings)

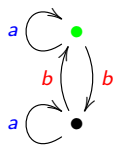
Für jedes Paar endlich erzeugter Untergruppe $H, K \leqslant_{fg} F_A$, stimmt nach dem Haareschneiden die Zusammenhangskomponente von $\Gamma(H) \times \Gamma(K)$, die den Basispunkte enthält, mit $\Gamma(H \cap K)$ überein.

Dies liefert einen schnellen Algorithmus zur Bestimmung des Schnittes von Untergruppen:

Erstes Beispiel zur Schnittberechnung

Seien $H = \langle a, b^2, bab \rangle$ und $K = \langle b^2, ba^2 \rangle$ Untergruppen von F_2.
Berechnen einer Basis von $H \cap K$:

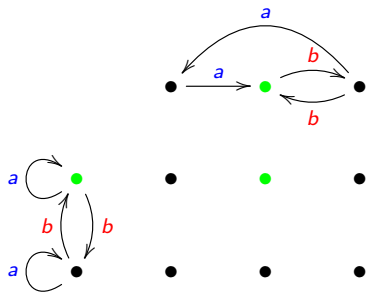




$H \cap K = ?$ Klar, dass $b^2 \in H$, aber... ist das alles?

Erstes Beispiel zur Schnittberechnung

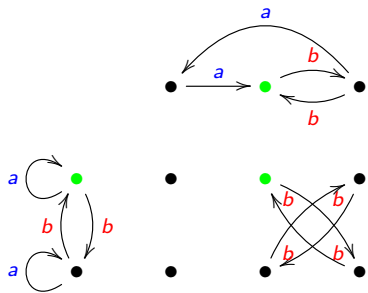
Seien $H = \langle a, b^2, bab \rangle$ und $K = \langle b^2, ba^2 \rangle$ Untergruppen von F_2.
Berechnen einer Basis von $H \cap K$:



$H \cap K = \langle b^2, \ldots (?) \ldots \rangle$

Erstes Beispiel zur Schnittberechnung

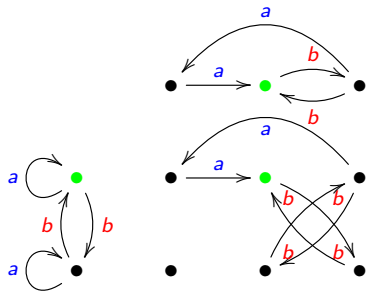
Seien $H = \langle a, b^2, bab \rangle$ und $K = \langle b^2, ba^2 \rangle$ Untergruppen von F_2.
Berechnen einer Basis von $H \cap K$:



$H \cap K = \langle b^2, \quad \rangle$

Erstes Beispiel zur Schnittberechnung

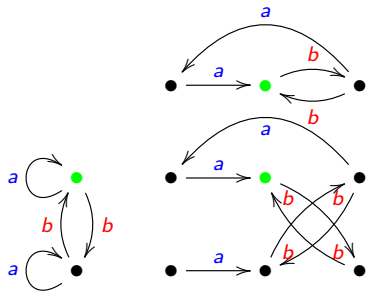
Seien $H = \langle a, b^2, bab \rangle$ und $K = \langle b^2, ba^2 \rangle$ Untergruppen von F_2.
Berechnen einer Basis von $H \cap K$:



$H \cap K = \langle b^2, a^{-2}b^2a^2, \quad \rangle$

Erstes Beispiel zur Schnittberechnung

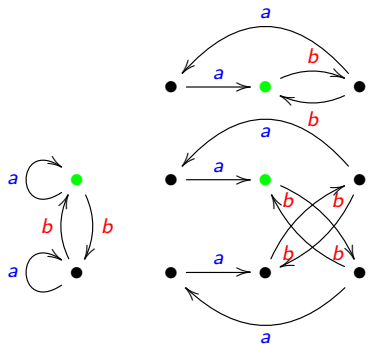
Seien $H = \langle a, b^2, bab \rangle$ und $K = \langle b^2, ba^2 \rangle$ Untergruppen von F_2.
Berechnen einer Basis von $H \cap K$:



$H \cap K = \langle b^2, a^{-2}b^2a^2, \quad \rangle$

Erstes Beispiel zur Schnittberechnung

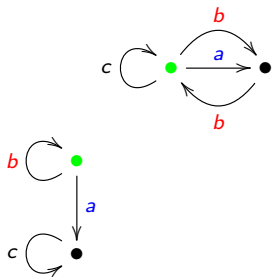
Seien $H = \langle a, b^2, bab \rangle$ und $K = \langle b^2, ba^2 \rangle$ Untergruppen von F_2.
Berechnen einer Basis von $H \cap K$:



$H \cap K = \langle b^2, a^{-2}b^2a^2, ba^2ba^2 \rangle$ ... und sonst nichts.

Zweites Beispiel zur Schnittberechnung

Der Pullback-Automat muss nicht zusammenhängend sein und kann Knoten vom Grad 1 haben.

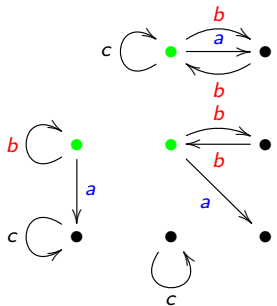


$H = \langle ba^{-1}, ab, c \rangle$

$K = \langle b, aca^{-1} \rangle$

Zweites Beispiel zur Schnittberechnung

Der Pullback-Automat muss nicht zusammenhängend sein und kann Knoten vom Grad 1 haben.



$$H = \langle ba^{-1}, ab, c \rangle$$

$$K = \langle b, aca^{-1} \rangle$$

$$H \cap K = \langle b^2 \rangle$$

Rang des Schnittes zweier Untergruppen

Korollar (Howson, J. London Math. Soc. 29 (1954) 428–434)

Der Schnitt zweier endlich erzeugter Untergruppen von F_A ist wiederum endlich erzeugt.

Aber er kann höheren Rang haben: "$3 = 3 \cap 2 \geq 2$"

Theorem (Hanna Neumann (1957))

Seien H und K nicht triviale Untergruppen in F_A. Dann gilt:

$$r(H \cap K) - 1 \leq 2(r(H) - 1)(r(K) - 1).$$

Vermutung (H. Neumann)

$$r(H \cap K) - 1 \leq (r(H) - 1)(r(K) - 1).$$

Beweise für obere Schranken von $r(H \cap K) - 1$

Betrachte die Stallings-Automaten $\Gamma(H)$, $\Gamma(K)$, $\Gamma(H \cap K)$, mit den Kantenzahlen e_H, e_K, $e_{HK} = e_{H \cap K}$ und Knotenzahlen n_H, n_K, $n_{HK} = n_{H \cap K}$.
Wir wissen

$$r(H \cap K) - 1 = e_{HK} - n_{HK}, \quad r(H) - 1 = e_H - n_H, \quad r(K) - 1 = e_K - n_K.$$

Zu zeigen ist also: $e_{HK} - n_{HK} \leq 2 \cdot (e_H - n_H) \cdot (e_K - n_K)$ und die Hanna-Neumann-Vermutung (HNC) lautet:

$$e_{HK} - n_{HK} \leq (e_H - n_H) \cdot (e_K - n_K)$$

Wir zeigen in den Übungen, dass die Vermutung in wichtigen Spezialfällen richtig ist.

Haare schneiden ist erlaubt

Probleme machen insbesondere die Knoten mit Grad 1, dies ist nur bei den Basispunkten möglich. Nehmen wir daher an, am Basispunkt 1_H gehe nur eine Kante aus, die mit $a \in A^{\pm}$ beschriftet sei. Dann geht auch beim Basispunkt 1_K eine Kante aus, die mit $a \in A^{\pm}$ beschriftet, denn ansonsten gilt $H \cap K = \{1\}$.
Setze $H' = aH\overline{a}$ und $K' = aK\overline{a}$.
Dann ist $\Gamma(H')$ echt kleiner als $\Gamma(H)$;
und $\Gamma(K')$ ist in $\Gamma(K)$ enthalten.
Wegen $H \cap K = \overline{a}(H' \cap K')a$ können wir also H durch H' und K durch K' ersetzen.
Dies entspricht dem Haare schneiden.
Im Folgenden können wir also annehmen, dass weder $\Gamma(H)$ noch $\Gamma(K)$ einen Knoten vom Grad 1 haben.

Beweis der schwachen Schranke für $r(H \cap K)$

Wir lesen $\Gamma(H)$ und $\Gamma(K)$ als ungerichtete Graphen und definieren den Grad $d(u)$ wie üblich, d.h., es werden die inzidenten Kanten gezählt, wobei Schlingen doppelt gezählt werden. In der Summe $\sum_{u \in U} d(u)$ werden also alle Kanten doppelt gezählt und damit gilt bei n Knoten und e Kanten und Knotenmenge U die Formel:

$$2(e - n) = \sum_{u \in U} (d(u) - 2).$$

Da keine Knoten vomGrad 1 existieren, gilt stets $d(u) \geq 2$ und es treten keine negativen Terme auf. Ferner gilt für alle (u, v) im Produktautomaten:

$$d(u, v) - 2 \leq \min\{d(u), d(v)\} - 2 \leq (d(u) - 2)(d(v) - 2).$$

$r(H \cap K) - 1 \leq 2(r(H) - 1)(r(K) - 1)$

Zu zeigen ist $2(r(H \cap K) - 1) \leq 4(r(H) - 1)(r(K) - 1)$. Mit den Bezeichnungen von eben und wegen $\min\{d(u), d(v)\} \geq 2$ gilt:

$$
\begin{aligned}
2(r(H \cap K) - 1) &= \sum_{(u,v) \in W} d(u,v) - 2 \\
&\leq \sum_{(u,v) \in W} \min\{d(u), d(v)\} - 2 \\
&\leq \sum_{(u,v) \in W} (d(u) - 2)(d(v) - 2) \\
&\leq \sum_{(u,v) \in U \times V} (d(u) - 2)(d(v) - 2) \\
&= (\sum_{u \in U} d(u) - 2)(\sum_{v \in V} d(v) - 2) \\
&= 4(e_H - n_H)(e_K - n_K).
\end{aligned}
$$

Historie der Hanna-Neumann-Vermutung

- HNC gilt, falls H den Rang 1 hat. (Trivial.)
- HNC gilt, falls H den Rang 2 hat. (Tardös, 1992: schwierig.)
- HNC gilt, falls H den Rang 3 hat. (Dicks-Formanek, 2001: sehr schwierig.)
- HNC gilt, falls H und K endlichen Index haben. (Siehe oben.)
- HNC gilt, falls H und K positiv erzeugt werden ($\Longleftrightarrow$ $\Gamma(H)$ ist stark zusammenhängend). (Meakin-Weil und Khan, 2002, siehe oben für eine etwas allgemeinere Aussage).
- HNC war lange ein offenes Problem (...und galt als sehr schwierig).
- HNC wurde 2011 gelöst
  (Joel Friedman, Igor Mineyev) Kurzfassung des Beweises von Mineyev durch Warren Dicks

Freie Produkte

Sei M_i, $i \in I$ eine Familie von Monoiden. Ohne Einschränkung gilt $M_i \cap M_j = \{1\}$ $\forall i \neq j$. Wir fassen die disjunkte Vereinigung

$$\Sigma = \bigcup_{i \in I} M_i \setminus \{1\}$$

als ein Alphabet auf und bezeichnen mit $1 \in \Sigma^*$ das leere Wort und mit 1_M das neutrale Element der M_i. Definiere das konvergente Ersetzungssystem $S \subseteq \Sigma^* \times \Sigma^*$ wie folgt.

$$fg \quad \to h \quad \text{falls } f \cdot g = h \text{ in einem } M_i \text{ und } h = 1 \text{ falls } f \cdot g = 1_M \text{ das leere}$$

Termination und starke Konfluenz sind trivial. Das *freie Produkt* $*_{i \in I} M_i$ ist definiert durch Σ^*/S. Offensichtlich gilt $M_i \subseteq *_{i \in I} M_i \neq \emptyset$, wenn wir 1_i mit dem leeren Wort identifizieren. Es gilt die universelle Eigenschaft:

$$\mathrm{Hom}(*_{i \in I} M_i, M) = \prod_{i \in I} \mathrm{Hom}(M_i, M)$$

Freie Produkte

Das freie Produkt ist genau dann eine Gruppe, wenn alle M_i Gruppen sind.
Angenommen, es gilt: $M_i = \Sigma_i^*/S_i$ für alle $i \in I$. Ohne Einschränkung $\Sigma_i \cap \Sigma_j = \emptyset$ $\forall i \neq j$. Dann:

$$*_{i \in I} M_i = (\bigcup_{i \in I} \Sigma_i)^* / \bigcup_{i \in I} S_i$$

Sind alle S_i konvergent, so gibt es keine Überlappungen zwischen linken Seiten von S_i und S_j für $i \neq j$. Daher ist dann auch $S = \bigcup_{i \in I} S_i$ konvergent.

Beispiel

Sind G_i, $i \in I$ endliche Gruppen und ist Σ ein Alphabet und $\overline{\Sigma}$ eine disjunkte Kopie. Setze $\Sigma_i = G_i \setminus \{1_i\}$ und $\overline{g} = g^{-1}$ für $g \in \Sigma_i$. Bilde $\Delta = \Sigma \cup \overline{\Sigma} \cup \bigcup_{i \in I} \Sigma_i$. Dann ist $\overline{a}$ mit $\overline{\overline{a}} = a$ auf Δ definiert. Das freie Produkt $F(\Sigma) * *_{i \in I} G_i$ kann durch die folgende reguläre Menge dargestellt werden

$$NF = \Delta^* \setminus (\bigcup_{a \in \Delta} \Delta^* a \overline{a} \Delta^* \cup \bigcup_{i \in I} \Delta^* \Sigma_i \Sigma_i \Delta^*)$$

HNN-Erweiterungen

Graham Higman, Bernhard Hermann Neumann, Hanna Neumannn (1949)
Sei H eine Gruppe mit Untergruppen $A, B \leq H$ und $\Phi : A \to B$ ein Isomorphismus. Sei t ein Zeichen, das nicht in H vorkommt. Mit $\langle H, t \rangle$ bezeichnen wir das freie Produkt von H mit der von t erzeugten freien Gruppe $F(t)$. Die HNN-Erweiterung von H mit (A, B, Φ) ist die Quotientengruppe

$$\mathrm{HNN}(H, t; A, B, \Phi) = \langle H, t \rangle \,/\, \left\{ \, t^{-1} a t = \Phi(a) \;\middle|\; a \in A \, \right\}.$$

Alternative Schreibweise:

$$\left\langle H, t;\ t^{-1} A t \overset{\Phi}{=} B \right\rangle$$

Normalformen für HNN-Erweiterungen

Wir geben Normalformen für Elemente von $\mathrm{HNN}(H; A, B, \Phi)$ an und folgern, dass sich H in $\mathrm{HNN}(H; A, B, \Phi)$ einbettet. Ferner geben wir ein hinreichende Bedingung für Φ, dass sich die Entscheidbarkeit des Wortproblems für H auf die HNN-Erweiterung überträgt.

Wir beweisen dies mit Hilfe eines konvergenten Ersetzungssystems. Wir definieren $\Delta = \{ t, t^{-1} \} \cup H \setminus \{1\}$ und fassen dies als ein (möglicherweise unendliches) Alphabet auf. Die $1 \in H$ identifizieren wir mit dem leeren Wort $1 \in \Delta^*$. Weiter wählen wir Vertretersysteme für die Nebenklassen von A und B in H, d.h. Mengen $C, D \subseteq H$ so, dass die Zerlegungen

$$H = A \cdot C = B \cdot D$$

eindeutig sind. Ohne Einschränkung sei $1 \in C \cap D$.

Das gesuchte System $S \subseteq \Delta^* \times \Delta^*$ ist durch die folgenden Regeln gegeben:

$$
\begin{array}{rcll}
gh & \longrightarrow & [gh] & \text{mit } g, h \in H \setminus \{1\} \text{ und } gh = [gh] \in H \\
t^{-1}t & \longrightarrow & 1 & \\
tt^{-1} & \longrightarrow & 1 & \\
gh & \longrightarrow & f & \text{falls } gh = f \text{ in } H \\
tg & \longrightarrow & atd & \text{falls } g \notin D,\ a \in A,\ d \in D,\ \Phi(a)d = g \text{ in } H \\
t^{-1}g & \longrightarrow & bt^{-1}c & \text{falls } g \notin C,\ b \in B,\ c \in C,\ \Phi^{-1}(b)c = g \text{ in } H
\end{array}
$$

Offenbar definiert Δ^*/S genau die HNN-Erweiterung von H durch (A, B, Φ).

Obwohl das System nicht längenreduzierend ist, ist der Beweis der Terminierung nicht besonders schwierig. Lokale Konfluenz ist einfach zu zeigen, also ist S tatsächlich konvergent.
Da alle Elemente von H irreduzibel sind, bettet H in die HNN-Erweiterung ein. Zudem erhalten wir: Jedes Element hat eine eindeutige Zerlegung

$$g = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$$

mit n minimal so, dass $n \geq 0$, $g_0 \in H$, $\varepsilon_i = -1 \wedge g_i \in C \vee \varepsilon_i = 1 \wedge g_i \in D$ für alle $1 \leq i \leq n$.

Britton-Reduktionen

Betrachte das folgende Ersetzungssystem:

$$\begin{array}{rcll} gh & \longrightarrow & [gh] & \text{mit } g, h \in H \setminus \{1\} \text{ und } gh = [gh] \in H \\ t^{-1}at & \longrightarrow & \Phi(a) & \text{für } a \in A \\ tbt^{-1} & \longrightarrow & \Phi^{-1}(b) & \text{für } b \in B \end{array}$$

Starten wir mit Wörtern der Form $g = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$, so liefern die Regeln eine Britton-reduzierte Form $h_0 t^{\varepsilon_1} h_1 \cdots t^{\varepsilon_m} h_m$ mit $m \leq n$.

Ziel: $m = 0 \iff g \in H$ (obwohl das System nicht konfluent ist!)

Brittons Lemma für Britton-reduzierte Elemente

Es sei $G = \left\langle H, t;\ t^{-1}At \overset{\Phi}{=} B \right\rangle$.

Definition

Ein Wort $g = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$ heißt Britton-erduziert, falls $g_i \in H$ und kein Faktor $t^{-1}at$ mit $a \in A$ und kein Faktor tbt^{-1} mit $b \in B$ vorkommt.

Lemma (Britton)

Sei $g = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$ ein Britton-reduziertes Wort gelesen als Element in G und $n \geq 1$. Dann gilt $g \neq 1$.

Beweis. Die Ersetzungsregeln erhalten die Eigenschaft Britton-reduziert zu sein. Insbesondere ist die irreduzible Normalform von g von der Gestalt:

$$h_0 t^{\delta_1} h_1 \cdots t^{\delta_n} h_n.$$

□

Amalgamierte Produkte vom Typ $A \star_H B$

Seien A, B und H Gruppen, sowie $\varphi : H \to A$ und $\psi : H \to B$ Homomorphismen.
Dann kann man eine neue Gruppe definieren, die $\varphi(h) \in A$ jeweils mit $\psi(h) \in B$ identifiziert.
Formal:

$$A * B / \{ \varphi(h) = \psi(h) \mid h \in H \}.$$

Wir können nicht erwarten, dass diese Gruppe A oder B als Untergruppe enthält.
Dies ändert sich, wenn φ und ψ injektiv sind.
Wir schreiben dann:

$$A \star_H B = A * B / \{ \varphi(h) = \psi(h) \mid h \in H \}.$$

Beispiele

Die folgenden Beispiele sind aus dem Buch von Serre:

1.) $D_\infty = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$.

2.) $\langle a, b; aba = bab \rangle =$
zwei Kopien von $\mathbb{Z}$ amalgamiert über $2\mathbb{Z}$ und $3\mathbb{Z}$ = *Kleeblattknoten* = *engl.: trefoil knot*.

3.) $\mathrm{SL}(2, \mathbb{Z}) = \mathbb{Z}/4\mathbb{Z} \star_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/6\mathbb{Z}$.

4.) $\mathrm{PSL}(2, \mathbb{Z}) = \mathrm{SL}(2, \mathbb{Z})/\{\pm 1\} = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$.

Amalgamierte Produkte

Es gibt ein natürliches konvergentes Ersetzungssystem, welches amalgamierte Produkte definiert: Seien A und B Gruppen, deren Schnitt eine gemeinsame Untergruppe H ist. Wieder wählen wir Vertretersysteme C und D für die Nebenklassen von H in A und B so, dass die Zerlegungen $A = HC$ und $B = HD$ eindeutig sind.
Wir definieren Δ als $(A \cup B) \setminus \{1\}$ und identifizieren $1 \in A \cap B$ mit dem leeren Wort in Δ^*.
Ferner setzen wir

$$[ab] = c, \text{ falls } \; a \cdot b = c \text{ in } A \text{ oder } B.$$

Amalgamierte Produkte

Das System $S \subseteq \Delta^* \times \Delta^*$ definieren wir durch die Regeln

$$\begin{array}{lcll} ab & \longrightarrow & [ab] & \\ ab & \longrightarrow & [ah]d & \text{falls } 1 \neq a \in A,\ h \in H,\ b \neq d \in D,\ b = hd, \\ ba & \longrightarrow & [bh]c & \text{falls } 1 \neq b \in B,\ h \in H,\ a \neq c \in C,\ a = hc. \end{array}$$

Dieses System ist längenlexikographisch terminierend. Eine kurze Untersuchung zeigt lokale Konfluenz, also haben wir Konvergenz. Das System S definiert das amalgamierte Produkt $A \star_H B$.
Die Normalformen sind alternierende Produkte. Exemplarisch etwa:

$$a_0 d_1 c_1 \cdots d_m c_m.$$

Analogon zu Britton-Reduktionen

Selbsttest: Was ist das Analogon. Nur längenverkürzende Regeln, keine Konfluenz, aber die alternierenden Produkte sind eindeutig definiert.

Wortproblem

Betrachte das amalgamierte Produkt $A \star_H B$ mit A und B endlich erzeugt. Dann ist auch $A \star_H B$ endlich erzeugt.
Angenommen, in A und B ist das Wortproblem lösbar und wir können jeweils die Mitgliedschaft in H testen.
Dann ist das Wortproblem in $A \star_H B$ lösbar:
Berechne ein alternierendes Produkt etwa mittels Britton-Reduktionen.

$$a_0 a_1 \cdots a_m$$

so, dass für alle $0 \leq i < m$ gilt:

1.) $a_i \in A \iff a_{i+1} \in B \setminus H$,

2.) $a_i \in B \iff a_{i+1} \in A \setminus H$.

Ein solches alternierendes Produkt kann durch Regeln aus S nicht mehr verkürzt werden.
Es ist nur dann trivial, wenn $a_0 = 1$ und $m = 0$ gilt.

Einbettungen amalgamierte Produkte

Proposition

Seien A', B', H' und A, B, H Gruppen mit:

1.) $A' \leq A$,

2.) $B' \leq B$,

3.) $A \cap B = H$,

4.) $A' \cap H = B' \cap H = H'$,

Dann ist der natürliche Homomorphismus injektiv:

$$A' \star_{H'} B' \to A \star_H B.$$

Beweis. Nichttriviale alternierende Produkte bleiben nichttriviale alternierende Produkte. □

Konjugation in amalgamierten Produkten

Sei $G = A \star_H B$.
Eingabe: f, g als zyklisch reduzierte alternierende Produkte $f = f_1 \cdots f_m$, $g = g_1 \cdots g_n$.
Frage: $f \sim_G g$? Also:

$$\exists z : zfz^{-1} = g?$$

Für $X \subseteq G$ schreibe $f \sim_X g$, falls $\exists x \in X : xfx^{-1} = g$.

Satz (Collins' Lemma für amalgamierte Produkte)

Liegen f, g als zyklisch reduzierte alternierende Produkte mit $1 \leq m \leq n$ vor, so gilt $f \sim_G g$ genau dann wenn eine der folgenden Bedingungen erfüllt ist.

1. $f, g \in A \cup B$ *(d.h. $m = n = 1$) und* $f \sim_{A \cup B} g$.
   Die Bezeichnung bedeutet: $\exists C \in \{ A, B \} : f, g \in C \wedge f \sim_C g$.
2. $f, g \in A \cup B$ *(d.h. $m = n = 1$) und es gibt eine Folge* $h_1, \ldots, h_k \in H$ *mit* $h_i \sim_{A \cup B} h_{i+1}$ *für alle* $i = 1, \ldots, k-1$ *und* $f \sim_{A \cup B} h_1$ *und* $g \sim_{A \cup B} h_k$.
3. $2 \leq m = n$ *und* $\exists 1 \leq i \leq n : f_i \cdots f_n f_1 \cdots f_{i-1} \sim_H g_1 \cdots g_n$.

Beweis Collins' Lemma

Sei $f \sim_G g$. Dann gibt es ein alternierendes Produkt $z = z_1 \cdots z_k$ mit

$$z_1 \cdots z_k \cdot f_1 \cdots f_m \cdot \overline{z_k} \cdots \overline{z_1} = g_1 \cdots g_n?$$

Unter allen Möglichkeiten wählen wir k minimal.
Wir geben jetzt den "generischen Algorithmus" zur Lösung des Konjugationsproblems an. Er beinhaltet weitere Fallunterscheidungen.

Lemma

Seien $z = z_1 \cdots z_k$, $f_1 \cdots f_m$ und $g = g_1 \cdots g_n$ alternierende Produkte und zusätzlich g zyklisch Britton-reduziert. Ferner sei $k \geq 1$ und $z_k \notin H$. Gilt nun

$$z_1 \cdots z_k \cdot f_1 \cdots f_m \cdot \overline{z_k} \cdots \overline{z_1} = g_1 \cdots g_n \in G$$

so ist $z_1 \cdots z_k \cdot f_1 \cdots f_m \cdot \overline{z_k}$ **nicht** Britton-reduziert. Ist ferner $m = 1$, $k > 1$ und z Britton-reduziert, so folgt $z_i \cdots z_k \cdot f_1 \cdot \overline{z_k} \cdots \overline{z_i} \in H$ für alle $2 \leq i \leq k$.

Beweis. Für $n = 1$, also $g = g_1$ kann $z_1 \cdots z_k \cdot f \cdot \overline{z_k} \cdots \overline{z_1}$ nicht Britton-reduziert sein.

Für $n > 1$ ist n gerade und g_1 und g_n liegen in verschiedenen Faktoren, denn g ist zyklisch Britton-reduziert.

Also ist $z_1 \cdots z_k \cdot f \cdot \overline{z_k} \cdots \overline{z_1}$ nicht Britton-reduziert, denn z_1 und $\overline{z_1}$ gehören zum selben Faktor.

Sei jetzt $m = 1$, also $f = f_1$, dann folgt $z_i \cdots z_k \cdot f_1 \cdot \overline{z_k} \cdots \overline{z_i} \in H$ mit Induktion von k nach 2. □

Beweis Collins' Lemma: Fall 1 und 2. $m = 1$

Sei $m = 1$ und $f \not\sim_{A \cup B} g$ (d.h. wir sind nicht in Fall 1). Ohne Einschränkung $f = a \in A$.

Da $g_1 \cdots g_n$ zyklisch Britton-reduziert ist, muss sich $z_k \cdot a \cdot \overline{z_k}$ verkürzen lassen.
Falls $z_k \in A$, dann ist entweder $k = 1$ und $f \sim_A g \in A$ (bereits ausgeschlossen) oder $k \geq 2$ und $z_k \cdot a \cdot \overline{z_k} \in H$.
Also $k \geq 2$; und es muss sich $z_{k-1} \cdot z_k \cdot a \cdot \overline{z_k} \cdot \overline{z_{k-1}}$ zu einem $b \in B$ reduzieren lassen.
Hieraus folgt $a \sim_A h$ für ein $h \in H$. Ersetze a durch h.

Analog für $n = 1$. Für $\min\{m, n\} = 1$ können wir daher $1 \leq m \leq n$ annehmen sowie $f = h_k \in H$. Hieraus folgt $z_k \in B$, da k minimal gewählt wurde.
Für $m = 1$ (analog $n = 1$) finden wir also eine Kette

$$f = a \sim_A h_k \sim_B h_{k-1} \cdots h_2 \sim_C g$$

mit $C \in \{A, B\}$ und daher auch $n = 1$.

Collins' Lemma Fall 3. $2 \leq m \leq n$

Es bleibt der folgende Spezialfall in "Collin's Lemma":

Proposition

Sei $2 \leq m \leq n$ *dann gilt* $f \sim_G g$ *genau dann wenn*

$$\exists 1 \leq i \leq n \exists h \in H : m = n \wedge h \cdot f_i \cdots f_n f_1 \cdots f_{i-1} \cdot h^{-1} = g_1 \cdots g_n.$$

Beweis.

Wegen $m \geq 2$ gilt is m gerade.

Da $g_1 \cdots g_n$ zyklisch Britton-reduziert ist, muss sich $z_k \cdot f_1 \cdots f_m \cdot \overline{z_k}$ verkürzen lassen (siehe Lemma).

Falls z_k nicht aus demselben Faktor wie f_1 kommt, lese alles von rechts nach links und vertausche die Namensgebung von A und B. Daher kommt ohne Einschränkung z_k aus demselben Faktor wie f_1 (d. h. $z_k, f_1 \in A$ oder $z_k, f_1 \in B$).

Beweis Fortsetzung: Ohne Einschränkung $z_k, f_1 \in A$

$z_k, z_k \cdot f_1 \notin H$ ist unmöglich, da sonst

$$z_1 \cdots z_{k-1}[z_k f_1] \cdot f_2 \cdots f_m \cdot \overline{z_k} \cdot \overline{z_{k-1}} \cdots \overline{z_1}$$

Britton-reduziert ist, aber im Gegensatz zu g ungerade Länge hat.
Induktionsanfang $k = 1$: Zwei Fälle:
Ist $z_k = h \in H$, so sind wir fertig: $[hf_1]f_2 \cdots f_{m-1}[f_m h^{-1}] = g_1 \cdots g_n$ und $m = n$.
Sei $z_k \notin H$. Also ist $z_k = hf_1^{-1}$ für ein $h \in H$ und es folgt
$g_1 \cdots g_n = z_k \cdot f_1 \cdots f_m \cdot \overline{z_k} = hf_2 \cdots f_m f_1 h^{-1}$.

Induktionsschritt $k \geq 2$: Dann $z_k \notin H$, da k minimal.

$$\begin{aligned} z_1 \cdots z_k \cdot f_1 \cdots f_n \cdot \overline{z_k} \cdots \overline{z}_1 &= z_1 \cdots z_{k-1} \cdot hf_1^{-1} \cdot f_1 \cdots f_n \cdot f_1 h^{-1} \cdot \overline{z}_{k-1} \cdots \overline{z}_1 \\ &= z_1 \cdots z_{k-2}[z_{k-1}h] \cdot f_2 \cdots f_n \cdot f_1 \cdot [z_{k-1}h]^{-1} \overline{z}_{k-2} \ \cdots \overline{z}_1 \end{aligned}$$

Mit Induktion, da das konjugierende Element kürzer geworden ist können:

$$= h' \cdot f_i \cdots f_n \cdot f_1 \cdot f_2 \cdots f_1 \cdot h'^{-1}. \qquad \text{(nach Induktion)}$$

Merke: die Komposition zweier zyklischer Permutationen ist eine zyklische Permutation.

Das Konjugationsproblem in $G = A \star_H B$ ist lösbar, falls:

1. Das Wortproblem in G ist mittels Britton-Reduktionen lösbar.
2. Die Konjugationsprobleme in A und B sind lösbar.
3. Die Probleme "$\exists h \in H : a \sim_A h$?" und "$\exists h : b \sim_B h$?" sind entscheidbar. (Falls "ja", kann $h \in H$ gefunden werden, sofern A, B und H effektiv aufzählbar sind!)
4. Für $h_1, h_2 \in H$ können wir "$h_1 \sim_G h_2$?" entscheiden.
5. Das Problem "$\exists h \in H : hfh^{-1} = g$?" ist entscheidbar.

Falls H endlich ist, sind damit nur folgende Voraussetzungen notwendig:

- Die Konjugationsprobleme in A und B sind lösbar.

Dies impliziert die Entscheidbarkeit der anderen Probleme (Für 4. beachte: die Gruppe G ist fest, d. h. nicht Teil der Eingabe).

Eine nicht triviale Darstellung der trivialen Gruppe

Behauptung: Die Gruppe

$$G = \langle x, y, z \mid x^{-1}yx = y^2,\ y^{-1}zy = z^2,\ z^{-1}xz = x^2 \rangle$$

ist trivial (d.h. $G = \{1\}$).
Dies ist also die Gruppe H_3 in der folgenden Serie:

$$H_n = \langle x_i : i \in \mathbb{Z}/n\mathbb{Z} \mid x_{i-1}x_i x_{i-1}^{-1} = x_i^2 \ (i \in \mathbb{Z}/n\mathbb{Z}) \rangle$$

Der Beweis $H_3 = \{1\}$ ist konzeptionell einfach: Aufgrund der Semi-entscheidbarkeit des Wortproblems müssen wir nur einen naiven Algorithmus so lange laufen lassen, bis er Beweise für $x = y = z = 1$ findet. Aber ein vernünftiger (d.h. für Menschen lesbarer) Beweis ist nicht einfach zu finden!

Beispiel

Wir nummerieren die Gleichungen

$$x^{-1}yx = y^2 \ (1), \quad y^{-1}zy = z^2 \ (2), \quad z^{-1}xz = x^2 \ (3)$$

und folgern

$$(1) \Rightarrow yxy^{-1} = xy \ (4), \qquad (2) \Rightarrow z^{-1}yz = yz^{-1} \ (5).$$

Daraus erhalten wir

$$\begin{aligned} x^2yz^{-1} &\overset{(3),(5)}{=} z^{-1}xzz^{-1}yz = z^{-1}xyz \\ &\overset{(4)}{=} z^{-1}yxy^{-1}z \\ &= z^{-1}yzz^{-1}xzz^{-1}y^{-1}z \\ &\overset{(5),(3),(5)^{-1}}{=} yz^{-1}x^2zy^{-1} \\ &= yz^{-1}xzz^{-1}xzy^{-1} \overset{2\times(3)}{=} yx^4y^{-1}, \end{aligned}$$

also $z = yx^{-4}y^{-1}xy^2 \in \langle x, y\rangle$, d.h. G wird schon von x und y erzeugt.

Beispiel

Aus (1), (2) und (3) folgt, dass $G = [G, G]$, also auch $G = [[G, G], [G, G]]$. Es genügt also, zu zeigen, dass die zweite Kommutatorgruppe von $G := \langle x, y \rangle$ trivial ist.

Dazu benötigen wir zwei Rechenregeln für Kommutatoren:

1.

$$\begin{aligned}[a, bc] &= abca^{-1}c^{-1}b^{-1} \\ &= aba^{-1}b^{-1}baca^{-1}c^{-1}b^{-1} \\ &= [a, b]b[a, c]b^{-1}\end{aligned}$$

2.

$$\begin{aligned}[ded^{-1}, f] &= ded^{-1}fde^{-1}d^{-1}f^{-1} \\ &= ded^{-1}e^{-1}efde^{-1}d^{-1}f^{-1} \\ &= [d, e][e, fd]\end{aligned}$$

Beispiel

Aus 1. folgt: $[G, G]$ wird von der Menge
$E_1 = \{g[e_1, e_2]g^{-1} \ : \ e_i \in \{x, x^{-1}, y, y^{-1}\}, g \in G\}$ erzeugt. Mit Hilfe von (1) und (4) finden wir

$$E_1 = \{1, [x, y], [x^{-1}, y], [x, y^{-1}], [x^{-1}, y^{-1}]\} = \{1, xy^{-1}x^{-1}, y\}^{\pm 1}.$$

Aus 1. und 2. folgt: $[[G, G], [G, G]]$ wird von der Menge $E_2 = \{[f_1, f_2] \ : \ f_i \in E_1\}$ erzeugt. Es genügt also zu zeigen, dass $[xy^{-1}, y]$ mit y und y^{-1} kommutiert, was mit Hilfe von (4) leicht zu sehen ist.

Siehe auch: Graham Higman: A finitely generated infinite simple group. J. Lond. Math. Soc. 26 (1951), 61–64.

Die Higman-Gruppe H_4

Wir betrachten erneut die folgende Gruppe (mit $n = 4$):

$$G = H_4 = \left\langle x_i : i \in \mathbb{Z}/4\mathbb{Z} \mid x_{i+1} x_i x_{i+1}^{-1} = x_i^2 \ (i \in \mathbb{Z}/4\mathbb{Z}) \right\rangle$$

Theorem (Higman 1951)

Die Gruppe G ist unendlich und besitzt keine echten Untergruppen vom endlichen Index.

Man kann zeigen (etwas länglich), dass H_4 nicht einfach ist. Dies wurde zuerst von Paul Schupp gezeigt, der ein viel stärkeres Resultat zeigte: Jede abzählbare Gruppe kann in einen Quotienten H_4/N eingebettet werden, d.h. HH_4 is SQ-universell.

Keine echten Untergruppen vom endlichen Index

Sei $h : G \to F$ ein Homomorphismus mit F endlich. Angenommen, $h(x_{i+1}) = 1$. Dann auch $h(x_i) = 1$. Also gilt ohne Einschränkung $y_i = h(x_i) \neq 1$ für alle i.
Sei jetzt n_i die Ordnung von y_i in F und p der kleinste Primteiler von $n_1 \cdots n_4$.
Angenommen, $p \mid n_1$. Es gilt

$$y_1 = y_2^{n_2} y_1 y_2^{-n_2} = y_1^{2^{n_2}}.$$

Daher $y_1^{2^{n_2}-1} = 1$ und $p \mid n_1 \mid 2^{n_2} - 1$. Es folgt $p > 2$ und

$$2^{n_2} \equiv 1 \bmod p.$$

Die Ordnung von 2 in $(\mathbb{Z}/p\mathbb{Z})^*$ ist eine Zahl $2 \leq N \leq p-1$. Es folgt $N \mid n_2$ wegen $2^N \equiv 2^{n_2} \equiv 1 \bmod p$.
Widerspruch zur Wahl von p.

Eine unendliche endlich erzeugte einfache Gruppe

Corollary

Es gibt eine unendliche einfache Gruppe mit vier Erzeugenden. Diese kann als Quotient von G realisiert werden.

Beweis. Da G endlich erzeugt ist, besitzt G nach dem Lemma von Zorn einen maximalen Normalteiler H mit $G \neq H$. Der Quotient G/H ist damit einfach und unendlich, da G keine echten Untergruppen vom endlichen Index besitzt. □

Turingmaschinen und das Wortproblem in Monoiden

Übungsaufgabe:
Konstruieren Sie ein endlich dargestelltes Monoid M mit einem unentscheidbaren Wortproblem.
Hinweis: Übersetzen Sie die Arbeitsweise einer deterministischen Turingmaschine in ein stark konfluentes Semi-Thue System.
Die Lösung ist (noch) nicht Teil des Skriptes.

Ziel

Theorem

Es gibt eine endlich dargestellte Gruppe mit unentscheidbarem Wortproblem (und wir können eine solche explizit angeben).

- Formuliert von Dehn (ca. 1910)
- Unabhängig von Novikov und Boone bewiesen (ca. 1955)
- Wir folgen dem vereinfachten Beweis von Stillwell (1982)

Untergruppenproblem $\leq$ Wortproblem in einer HNN Erweiterung

Proposition

Seien G, H f.g. mit $H \leq G$. Dann kann das Problem $w \in H$ auf das Wortproblem $twt^{-1} = w$ in der HNN- Erweiterung

$$\mathrm{HNN}(G, t; \mathrm{id}_H : H \to H)$$

reduziert werden.

Beweis

Wir definieren

$$K := \mathrm{HNN}(G, t; \varphi)$$

mit

$$\varphi = \mathrm{id}_H.$$

Es gilt

$$w \in H \iff twt^{-1} = w$$

□

Wir haben gezeigt: K hat ein unentscheidbares Wortproblem, falls das Problem "$w \in H$?" unentscheidbar ist.

Neues Ziel

Es reicht zu zeigen:

Theorem

Es gibt eine endlich dargestellte Gruppe mit unentscheidbarem Untergruppenproblem.

Genauer: Wir finden $G = \langle X | \mathcal{R} \rangle$ und $Y \subseteq X$ so, dass für $w \in (X \cup X^{-1})^*$ die Frage $w \overset{?}{\in} \langle Y \rangle \leq G$ unentscheidbar ist.

Vorbereitung der Turingmaschine

Sei T eine Turingmaschine mit unentscheidbarem Halteproblem (z.B. eine universelle TM). Wir verlangen (o.E.):

- Zustände und Bandzeichen sind Teilmengen von $\{0, \ldots, b-1\} \subseteq \mathbb{N}_0$
- Startzustand ist 1
- Blanksymbol ist 0
- T hat nur ein Band
- T ist deterministisch
- T macht nur Rechts- und Linksschritte (keine N-Übergänge)
- T akzeptiert, indem sie alle Bandzeichen löscht und in den Zustand 0 geht

Vorbereitung der Turingmaschine

Stelle eine Konfiguration

$$\cdots 000 u_n u_{n-1} \ldots u_2 u_1 \, q \, v_0 v_1 \ldots v_m 000 \cdots$$

von T durch zwei Zahlen dar:

$$(U, V) := \left(q + \sum_{i=1}^{n} u_i b^i, \quad \sum_{i=0}^{m} v_i b^i \right)$$

Aus den L-Übergängen machen wir

$$(b^2 U + A_\ell, bV + B_\ell) \longrightarrow (bU + C_\ell, b^2 V + D_\ell)$$

und aus den R-Übergängen

$$(bU + A_r, b^2 V + B_r) \longrightarrow (b^2 U + C_r, bV + D_r)$$

mit geeigneten Konstanten A_ℓ, D_ℓ, B_r, C_r (b-när zweistellig) und B_ℓ, C_ℓ, A_r, D_r (b-när einstellig), jeweils durch $\ell \in L$ und $r \in R$ indiziert. Die akzeptierende Konfiguration ist $(0, 0)$.

Konstruktion der Gruppe $H(T)$

Wir starten mit der freien Gruppe $G = \langle x, y, z \rangle$.

Konfiguration $(U, V) \quad \rightsquigarrow \quad$ Gruppenelement $p(U, V) := x^U z y^V$

Naive (aber falsche) Idee: Bilde

$$H(T) := G/\triangleleft x^{b^2U+A_\ell} z y^{bV+B_\ell} = x^{bU+C_\ell} z y^{b^2V+D_\ell} \ (\ell \in L),$$
$$x^{bU+A_r} z y^{b^2V+B_r} = x^{b^2U+C_r} z y^{bV+D_r} \ (r \in R) \triangleright$$

Dann gilt: $(U, V) \vdash^* (0, 0) \quad \Rightarrow \quad p(U, V) = z$ in $H(T)$,
aber die Umkehrung gilt im Allgemeinen nicht!

Konstruktion der Gruppe $H(T)$

Stattdessen erzeugen wir eine Reihe von HNN-Erweiterungen, für jede Regel der TM eine. Wir beginnen z.B. mit einem $\ell \in L$:

$$\begin{aligned} G_1 &:= HNN(G, t_\ell; \varphi_\ell) \\ &= \left\langle x, y, z \mid t_\ell^{-1} x^{b^2} t_\ell = x^b, t_\ell^{-1} x^{A_\ell} z y^{B_\ell} t_\ell = x^{C_\ell} z y^{D_\ell}, t_\ell^{-1} y^b t_\ell = y^{b^2} \right\rangle \end{aligned}$$

Weiter geht es mit dem nächsten $\ell' \in L \setminus \{\ell\}$:

$$G_2 := HNN(G_1, t_{\ell'}; \varphi_{\ell'})$$

usw. und schließlich $H(T) := G_{|L|+|R|}$.

Aber: Sind das überhaupt HNN-Erweiterungen?

Konstruktion der Gruppe $H(T)$

G_1 hat die definierenden Gleichungen

$$t_\ell^{-1}\mathbf{x}^{\mathbf{b}^2}t_\ell = \mathbf{x}^{\mathbf{b}}, t_\ell^{-1}\mathbf{x}^{\mathbf{A}_\ell}\mathbf{z}\mathbf{y}^{\mathbf{B}_\ell}t_\ell = \mathbf{x}^{\mathbf{C}_\ell}\mathbf{z}\mathbf{y}^{\mathbf{D}_\ell}, t_\ell^{-1}\mathbf{y}^{\mathbf{b}}t_\ell = \mathbf{y}^{\mathbf{b}^2}.$$

Zu prüfen ist, ob $\varphi_\ell : x^{b^2} \mapsto x^b, x^{A_\ell}zy^{B_\ell} \mapsto x^{C_\ell}zy^{D_\ell}, y^b \mapsto y^{b^2}$ ein Isomorphismus von Untergruppen in $G = \langle x, y, z\rangle$ ist.

Lemma

Für alle m, n, i, j mit $m, n \neq 0$ ist $\{x^m, x^izy^j, y^n\}$ Basis einer freien Untergruppe von $G = \langle x, y, z\rangle$.

φ_ℓ bildet Basen freier Gruppen bijektiv aufeinander ab, also Iso.

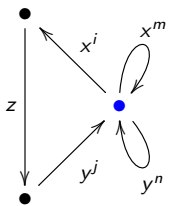
Konstruktion der Gruppe $H(T)$

Lemma

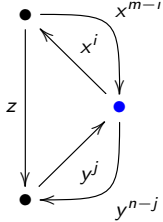
Für alle m, n, i, j mit $m, n \neq 0$ ist $\{x^m, x^i z y^j, y^n\}$ Basis einer freien Untergruppe von $G = \langle x, y, z \rangle$.

Beweis. Wir können $i < m$ und $j < n$ annehmen. Warum?
1.Blumen-Automat, 2.zusammengefaltet und 3.mit Spannbaum:

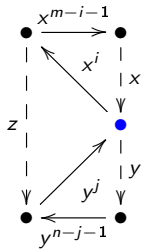
1.



2.



3.



□

$H(T)$ kennt noch die Turingmaschine T

Also: $H(T)$ entsteht durch HNN-Erweiterungen von $G = \langle x, y, z \rangle$ via $\{t_\ell, t_r : \ell \in L, r \in R\}$.

Klar:

$$
\begin{aligned}
& (U, V) \vdash^* (0, 0) \\
\Rightarrow & \exists W \text{ Wort in } \{t_\ell, t_r\} : \ W^{-1} p(U, V) W = p(0, 0) = z \text{ in } H(T) \\
\Rightarrow & p(U, V) \in \langle z, t_\ell, t_r \rangle \leq H(T)
\end{aligned}
$$

Fehlt noch: „$\Leftarrow$"

$H(T)$ kennt noch die Turingmaschine T

Lemma

Sei (U, V) eine Konfiguration von T. Dann ist höchstens einer der Isos $\{\varphi_\ell, \varphi_r : \ell \in L, r \in R\}$ auf $p(U, V)$ anwendbar.

Beweis. Sei $p(U, V) \in \operatorname{dom} \varphi_\ell$, d.h. $x^U z y^V \in \langle x^{b^2}, x^{A_\ell} z y^{B_\ell}, y^b \rangle$.

$\Rightarrow \; U \equiv A_\ell \mod b^2 \wedge V \equiv B_\ell \mod b.$

$\Rightarrow \; U \equiv A_\ell \mod b \wedge V \equiv B_\ell \mod b.$

Analog:

$p(U, V) \in dom\varphi_r \Rightarrow \; U \equiv A_r \mod b \wedge V \equiv B_r \mod b.$

$U \pmod b$ ist der Zustand und $V \pmod b$ das gelesene Zeichen. Die TM ist deterministisch, also ist höchstens einer der Isos $\{\varphi_\ell, \varphi_r : \ell \in L, r \in R\}$ auf $p(U, V)$ anwendbar. □

$H(T)$ kennt noch die Turingmaschine T

Wir definieren die Halteuntergruppe $H_0(T)$ von $H(T)$ durch:

$$\langle p(U,V) : (U,V) \text{ Konfiguration von } T \text{ mit } (U,V) \vdash^* (0,0)\rangle$$

Klar aufgrund des letzten Lemmas: $H_0(T)$ ist abgeschlossen unter allen $\varphi_\ell^{\pm 1}, \varphi_r^{\pm 1}$.

Lemma
In $H(T)$ gilt: $\langle G\rangle \cap \langle H_0(T) \cup \{t_\ell, t_r : \ell \in L, r \in R\}\rangle = H_0(T)$

Beweis. „$\supseteq$" ist klar. „$\subseteq$": Sei w ein Wort in $H_0(T) \cup \{t_\ell, t_r : \ell \in L, r \in R\}$ und v ein Wort in x, y, z mit $w = v$ in $H(T)$. Durch Britton-Reduktionen lassen sich alle t's in w eliminieren. Dabei werden nur φ's auf Elemente aus $H_0(T)$ angewandt. Es folgt $w \in H_0(T)$. □

$H(T)$ kennt noch die Turingmaschine T

Lemma

Sei (U, V) eine Konfiguration von T. Dann gilt

$$p(U,V) \in \langle z, t_\ell, t_r \ (\ell \in L, r \in R)\rangle \iff (U,V) \vdash^* (0,0).$$

Beweis.

$$\begin{aligned} p(U,V) \in &\langle z, t_\ell, t_r \ (\ell \in L, r \in R)\rangle \\ &\subseteq \langle H_0(T) \cup \{t_\ell, t_r : \ell \in L, r \in R\}\rangle \\ \overset{\text{letztes Lemma}}{\Rightarrow} &p(U,V) \in H_0(T) \overset{\text{Def. von } H_0(T)}{\Rightarrow} (U,V) \vdash^* (0,0) \end{aligned}$$

Zusammen:

$$(U,V) \vdash^* (0,0) \quad \Leftrightarrow \quad p(U,V) \in \langle z, t_\ell, t_r \ (\ell \in L, r \in R)\rangle \leq H(T),$$

d.h. $H(T)$ hat ein unentscheidbares Untergruppenproblem bzgl. der endlich erzeugten Untergruppe $H = \langle z, t_\ell, t_r \ (\ell \in L, r \in R)\rangle$. □ Fertig!

Unentscheidbarkeit des Isomorphieproblems

Ausgehend von der Unentscheidbarkeit des Wortproblems in

$$K(T) = \mathrm{HNN}(H(T), k; \mathrm{id}_{\langle z, t_\ell, t_r \ (\ell \in L, r \in R)\rangle})$$

kann man weiter zeigen, dass viele natürliche Probleme für endlich dargestellte Gruppen unentscheidbar sind.
Wir beweisen dies in den Übungen für das Isomorphieproblem:
Gegeben $G_1 = \langle \Sigma_1 | \Delta_1 \rangle$ und $G_2 = \langle \Sigma_2 | \Delta_2 \rangle$. Frage: $G_1 \cong G_2$?

Unentscheidbarkeit des Isomorphieproblems

Zeigen Sie, dass das Isomorphieproblem für endlich dargestellte Gruppen unentscheidbar ist:

1. Sei H eine Gruppe, in welcher alle Elemente $\neq 1$ unendliche Ordnung haben. Sei G eine HNN-Erweiterung von H. Dann haben auch in G alle Elemente $\neq 1$ unendliche Ordnung.
2. Sei $K = \langle a_1, \ldots, a_m | \Delta \rangle$ eine endlich dargestellte Gruppe mit unentscheidbarem Wortproblem, in der alle von 1 verschiedenen Elemente unendliche Ordnung haben. Zu jedem Wort w über den Erzeugern a_i definieren wir eine Gruppe

   $$K_w := \langle a_1, \ldots, a_m, t_1, \ldots, t_m \mid \Delta, t_i^{-1} w t_i = a_i (i = 1, \ldots, m) \rangle.$$

   Zeigen Sie: Es ist $w = 1$ in K genau dann, wenn K_w isomorph zur freien Gruppe vom Rang m ist.
3. Folgern Sie die Unentscheidbarkeit des Isomorphieproblems für endlich dargestellte Gruppen.

Higman Einbettung (1961)

Theorem

Eine endlich erzeugte Gruppe G kann genau dann in eine endlich dargestellte Gruppe eingebettet werden, wenn G aufzählbar repräsentiert werden kann.

Beweis: Siehe Lyndon-Schupp.

Higman-Neumann-Neumann Einbettung (1949)

Theorem

Jede abzählbare (endlich dargestellte) Gruppe C kann in eine (endlich dargestellte) Gruppe U eingebettet werden, welche von zwei Elementen mit unendlicher Ordnung erzeugt wird.

Es sei $(c_i)_{i \in I}$ eine Liste von Erzeugern von C mit $I \subseteq \mathbb{N}$ und $c_0 = 1$.

Higman-Neumann-Neumann Einbettung: Beweis

Wir haben

$$C \hookrightarrow C * F(a,b)$$
$$\hookrightarrow U := HNN\left(C * F(a,b), t; \left\{ t^{-1}b^{-i}ab^{i}t = c_i a^{-i}ba^{i} \;\middle|\; i \in I \right\}\right)$$

und die HNN-Erweiterung wird wegen $b = c_0 b = t^{-1}at$ von a und t erzeugt.
Beide Elemente haben unendlicher Ordnung.

Es genügt also zu zeigen, dass das oben Definierte wirklich eine HNN-Erweiterung ist, d.h. dass

$$\left\{ b^{-i}ab^{i} \;\middle|\; i \in I \right\} \qquad \text{und} \qquad \left\{ c_i a^{-i}ba^{i} \;\middle|\; i \in I \right\}$$

Basen freier Untergruppen von $C * F(a,b)$ sind.

Higman-Neumann-Neumannen: Beweis

$\left\{ b^{-i}ab^i \;\middle|\; i \in I \right\}$ und $\left\{ a^{-i}ba^i \;\middle|\; i \in I \right\}$ sind schon Basen freier Untergruppen in $F(a,b)$, siehe z.B. das Kapitel über Stallings-Automaten.

Um zu sehen, dass auch $\{c_i a^{-i}ba^i : i \in I\}$ Basis einer freier Untergruppen in $C * F(a,b)$ ist, betrachte den Homomorphismus

$$a^{-i}ba^i \mapsto \varphi(a^{-i}ba^i) = c_i a^{-i}ba^i \qquad \text{für } i \in I$$

und die natürliche Projektion

$$\pi : C * F(a,b) \to F(a,b).$$

Dann gilt $\pi(\varphi(a^{-i}ba^i)) = a^{-i}ba^i$ für alle $i \in I$, und φ ist injektiv. Nach Definition ist φ surjektiv, also ein Isomorphismus. Dieser bildet Basen auf Basen ab.

Unentscheidbarkeit und entscheidbare Eigenschaften

Der Satz von Rice besagt, dass nicht-triviale Eigenschaften rekursiv aufzählbarer Sprachen unentscheidbar sind.

Gilt ein analoger Satz in der Gruppentheorie?

Gibt es nicht-triviale Eigenschaften endlich präsentierter Gruppen, die entscheidbar sind? Antwort: ja! Entscheidbar ist etwa, ob die Faktorkommutatorgruppe $G/[G,G]$ isomorph zu $\mathbb{Z}$ ist.

Unentscheidbar ist dagegen, ob G und $G/[G,G]$ isomorph sind, denn dies ist ein Beispiel für eine Markov-Eigenschaft.

In diesem Abschnitt seien alle Gruppen endlich präsentiert

Eine Eigenschaft P von Gruppen heißt **Markov-Eigenschaft**, falls:

1. Es gibt eine Gruppe G_1 mit P.
2. Es gibt eine Gruppe G_2, die nicht Untergruppe einer Gruppe mit P ist.

Beispiele für Markov-Eigenschaften:

- Nicht-triviale Eigenschaften, die auf Untergruppen übergehen, z. B.
  - Torsionsfreiheit,
  - Entscheidbares Wortproblem,
  - Trivialität, Endlichkeit, Freiheit, Kommutativität, Nilpotenz.
- Nichttriviale Eigenschaften, die Markov-Eigenschaften implizieren, sind selbst Markov-Eigenschaften. Die letztgenannten Eigenschafen implizieren die Entscheidbarkeit des Wortproblems.
- Einfachheit (Beachte: aufzählbar präsentierte, einfache Gruppen haben ein entscheidbares Wortproblem, also kann eine Gruppe mit unentscheidbarem Wortproblem nicht in eine endlich präsentierte, einfache Gruppe eingebettet werden)

Theorem

Markov-Eigenschaften sind unentscheidbar.

Wir folgen dem Beweis aus Lyndon-Schupp.

Unentscheidbarkeit von Markov-Eigenschaften

Wir starten mit einer Gruppe H mit unentscheidbarem Wortproblem und einem Element $w \in H$. Ziel ist es, eine Gruppe G_w zu konstruieren, die genau dann die Eigenschaft P hat, wenn $w \neq 1$ in H.

Wir beginnen mit der Higman-Neumann-Neumann-Einbettung

$$G_2 * H * F(x) \hookrightarrow U = \langle u_1, u_2 \rangle$$

mit torsionsfreien Elementen u_1 und u_2 und bilden dann den Turm von HNN-Erweiterungen

$$K := \langle U, y_1, y_2, z \mid y_i^{-1} u_i y_i = u_i^2,\ z^{-1} y_i z = y_i^2\ (i = 1, 2) \rangle.$$

Unentscheidbarkeit von Markov-Eigenschaften

Nun betrachten wir die bereits bei der Higman Gruppe H_4 untersuchte Gruppe

$$G_{rst} = \langle r, s, t \mid s^{-1}rs = r^2,\ t^{-1}st = s^2 \rangle \cong \mathbf{BS}_{1,2} *_{\mathbb{Z}} \mathbf{BS}_{1,2}.$$

r und t eine erzeugen freie Untergruppe vom Rang 2. Schließlich setzen wir

$$G_w := \langle K * G_{rst} * G_1;\ r = z,\ t = [w, x] \rangle$$

Bemerkung

1. *Die Konstruktion der Gruppe G_w geht auf Rabin zurück.*
2. *Die Gruppe G_w ist endlich dargestellt.*
3. *Die Gruppe G_w hat (für $G_1 = 1$) nur 6 Erzeugende.*
4. *Das Trivialitätsproblem ist also für Gruppen mit 6 Erzeugenden unentscheidbar.*

Unentscheidbarkeit von Markov-Eigenschaften

$$G_2 * H * F(x) \hookrightarrow U = \langle u_1, u_2 \rangle$$
$$K = \langle U, y_1, y_2, z \mid y_i^{-1} u_i y_i = u_i^2,\ z^{-1} y_i z = y_i^2\ (i = 1, 2) \rangle$$
$$G_w = \langle K * G_{rst} * G_1;\ r = z,\ t = [w, x] \rangle$$

Fall 1: $w \neq 1$ in H. Dann ist $\{z, [w, x]\}$ Basis einer freien Untergruppe vom Rang 2 in K, ebenso wie $\{r, t\}$ in G_{rst}, und:

$$G_w = K *_{F_2} G_{rst} * G_1.$$

Wegen $G_2 \hookrightarrow U \hookrightarrow K \hookrightarrow G_w$ hat G_w nicht die Eigenschaft P.

Unentscheidbarkeit von Markov-Eigenschaften

$$G_{rst} = \langle r, s, t \mid s^{-1}rs = r^2,\ t^{-1}st = s^2 \rangle$$
$$G_2 * H * F(x) \hookrightarrow U = \langle u_1, u_2 \rangle$$
$$K = \langle U, y_1, y_2, z \mid y_i^{-1}u_i y_i = u_i^2,\ z^{-1}y_i z = y_i^2\ (i = 1, 2) \rangle$$
$$G_w = \langle K * G_{rst} * G_1;\ r = z,\ t = [w, x] \rangle$$

Fall 2: $w = 1$ in H. Dann ist $t = [w, x] = 1$, und damit:

$$t = 1 \implies s = 1 \implies r = 1 \implies z = 1$$
$$\implies y_i = 1 \implies u_i = 1 \implies G_w = G_1$$

Damit hat $G_w = G_1$ die Eigenschaft P.

Der Satz von Hall

Theorem (Hall, 1968)

Jede abzählbare Gruppe C kann in eine einfache Gruppe mit 6 Erzeugenden eingebettet werden.

Korollar (aus Higman 61 und Hall 68)

Es gibt eine einfache Gruppe mit 6 Erzeugenden, die (bis auf Isomorphie) alle aufzählbar repräsentierbaren Gruppen als Untergruppen enthält.

Beweis. Das freie Produkt $P = \star_{i \in \mathbb{N}} P_i$ über alle endlich dargestellten Gruppen abzählbar. Sei G einfach mit 6 Erzeugenden und $P \leq G$. Sei jetzt H aufzählbar repräsentierbar, nach Higman gibt es ein P_i mit $H \leq P_i$. Daher gilt $H \leq P_i \leq P \leq G$. □

Vorbereitung des Beweises von Hall 68, Teil I

Proposition

Jede abzählbare Gruppe C ist Untergruppe einer abzählbaren Gruppe H, in der alle Elemente gleicher Ordnung konjugiert sind.

Beweis. Für eine Gruppe G bezeichne $(a_i, b_i)_{i \in I}$ die Liste aller Paare gleicher Ordnung (die nicht in G konjugiert sind) und

$$G^* = \langle G, t_i \ (i \in I) \mid t_i^{-1} a_i t_i = b_i \rangle.$$

Es gilt $G \hookrightarrow G^*$ und in G^* sind alle Elemente aus G mit gleicher Ordnung konjugiert. Setze jetzt $G_0 := C$ und $G_{n+1} := G_n^*$ für $n \geq 0$. Dann hat

$$H = \bigcup_{n \geq 0} G_n$$

die gewünschte Eigenschaft. □

Vorbereitungen II

Proposition

Jede abzählbare Gruppe C kann in eine einfache (und divisible) Gruppe G eingebettet werden.

Ohne Einschränkung enthalte C Elemente jeder Ordnung (sonst ersetze C durch $C * (*_n \mathbb{Z}/n\mathbb{Z})$). Seien U und G Gruppen mit

$$C \hookrightarrow C * F(x) \hookrightarrow U \hookrightarrow G,$$

wobei U von zwei Elementen u_1, u_2 unendlicher Ordnung erzeugt werde und in G alle Elemente gleicher Ordnung konjugiert seien.
Wir können annehmen, dass G abzählbar ist.

Einfachheit von G

1. G ist einfach: Sei $1 \neq z \in N \trianglelefteq G$. Aufgrund der Eigenschaften von C und G gibt es ein zu z konjugiertes und von 1 verschiedenes Element in C. Wir können daher annehmen, dass $1 \neq z \in N \cap C$.

Dann gilt $[x, z] = xzx^{-1}z^{-1} \in N$ und $[x, z]$ hat unendliche Ordnung in $C * F(x)$. Also gibt es t_1, t_2 mit $t_i^{-1} u_i t_i = [x, z]$. Es folgt $u_i \in N$, also $C \leq U \leq N$.

Sei nun $g \in G$ beliebig. Dann ist g konjugiert zu einem Element aus C und damit zu einem Element in N.
Also ist $g \in N$ und damit $G/N = 1$.

Zur Divisibilität

2. G ist divisibel: Zu zeigen ist, dass zu jedem $1 \neq x \in G$ mit der Ordnung m $(2 \leq m \leq \infty)$ und zu jedem $n \geq 1$ ein z mit $x = z^n$ existiert.

Wähle ein $y \in C$ mit $ord(y) = mn$ (also $ord(y) = \infty$ falls $m = \infty$). Dann gilt

$$ord(y^n) = m = ord(x).$$

Also existiert ein $t \in G$ mit $t^{-1}xt = y^n$ und damit $x = (tyt^{-1})^n$. Also erfüllt $z = tyt^{-1}$ die Bedingung. □

Beweis des Satzes von Hall

Zu zeigen ist:
Jede abzählbare Gruppe C kann in eine einfache Gruppe mit 6 Erzeugenden eingebettet werden.
Wie in der vorangegangenen Proposition betten wir C in eine einfache Gruppe S ein.
Desweiteren konstruieren wir die HNN $F(x) * S \hookrightarrow U = \langle u_1, u_2 \rangle$ sowie

$$K := \langle U, y_1, y_2, z \mid y_i^{-1} u_1 y_i = u_i^2,\ z^{-1} y_i z = y_i^2\ (i = 1, 2) \rangle$$
$$G_w := \langle K * G_{rst} \mid r = z,\ t = [w, x] \rangle$$

für ein $1 \neq w \in S$.
Betrachte einen maximalen Normalteiler $1 \neq N \trianglelefteq G_w$ mit $N \neq G_w$. Angenommen $S \cap N \neq 1$. Da S einfach ist, folgt $N \cap S = S$, also $w \in N$. Wie in Fall 2 im Beweis der Unentscheidbarkeit von Markov-Eigenschaften folgt $G_w / N = 1$, Widerspruch.
Also gilt $S \cap N = 1$ und damit $S \hookrightarrow G_w / N$. □

Der Satz von Hall

Der im Beweis verwendete maximale Normalteiler N ist im Allgemeinen nicht effektiv konstruierbar:

Theorem
Sei G einfach und endlich erzeugt mit einer rekursiv aufzählbaren Menge von Relationen. Dann hat G ein entscheidbares Wortproblem.

Beweis. Die Aussage ist für $G{=}\{1\}$ trivialerweise richtig.
Sei also $G \neq \{1\}$. Sowohl G als auch $\langle G;\ w = 1\rangle$ haben rekursiv aufzählbare Präsentationen. Damit sind die Probleme $w \stackrel{?}{=} 1$ in G und $\langle G;\ w = 1\rangle \stackrel{?}{=} \{1\}$ semi-entscheidbar. Letzteres ist äquivalent zu $w \neq 1$ in G, da die nicht-triviale Gruppe G einfach ist. Somit ist das Wortproblem entscheidbar. □

Folgerungen

Sei H eine endlich präsentierte Gruppe:

$$H = \langle x_1, \cdots, x_n \mid r_1 = \cdots = r_m = 1 \rangle$$

Definiere:

$$L_H := \langle (x_i, x_i), (1, r_j) \ (1 \leq i \leq n, 1 \leq j \leq m) \rangle \leq F_n \times F_n.$$

Mit Induktion folgt $(u, v) \in L_H \quad \Longrightarrow \quad u = v$ in H.
Für die andere Richtung beachte, mit $(x_i, x_i), (1, r_j) \in L_H$ gilt auch
$(x_i, x_i)^{-1}(1, r_j)(x_i, x_i) = (1, x_i^{-1} r_j x_i) \in L_H$.
Ist also R der von den r_j erzeugte Normalteiler, so gilt $\{1\} \times R \subseteq L_H$ und damit:

$$u = v \text{ in } H \quad \Longrightarrow \quad (u, v) \in L_H$$

Folgerung: Der Satz von Mihailova

Korollar (Satz von Mihailova)

Das Untergruppenproblem für $F_2 \times F_2$ ist unentscheidbar.

Beweis. Es sei H eine endlich dargestellte Gruppe mit unentscheidbarem Wortproblem. Die Gruppen $L_H \leq F_n \times F_n$ sind endlich erzeugt. Wegen $F_n \leq F_2$ können wir $L_H \leq F_2 \times F_2$ annehmen.
Wie oben gesehen, gilt $1 = w$ in $H \iff (1, w) \in L_H$.

□

Folgerung: Unentscheidbarkeit von $L_H = F_6 \times F_6$

Ferner gilt:

$$\begin{aligned} L_H = F_n \times F_n &\Leftrightarrow \forall u, v: \ (u, v) \in L_H \\ &\Leftrightarrow \forall u, v: \ u = v \text{ in } H \\ &\Leftrightarrow H = 1 \end{aligned}$$

Rabins Konstruktion der Gruppen G_w liefert (mit $G_1 = 1$) eine Klasse von endlich präsentierten Gruppen H mit jeweils 6 Erzeugern, für die $H \stackrel{?}{=} 1$ unentscheidbar ist. Also ist die Frage $G \stackrel{?}{=} F_n \times F_n$ für endlich erzeugte Untergruppen G von $F_n \times F_n$ für $n \geq 6$ unentscheidbar.

Einrelatorgruppen

Im Folgenden sei $\Sigma = \{ a, b, c, \dots \}$ und $\Delta = \Sigma \cup \overline{\Sigma}$.
Ein Wort $w \in \Delta^*$ schreiben wir als Wort über Σ mit Exponenten in $\mathbb{Z}$.
Ist z^m ein Faktor von w, so sagen wir, dass z^m vorkommt. Wir schreiben als Kurzform $z \in \alpha(w)$, falls z in w vorkommt.
Die Exponentensumme $\sigma_z(w)$ zählt die Summe der Exponenten von $z \in \Sigma$, die in w vorkommen.

Beispiel. $w = ba^2b^{-1}a^{-1}c^{42}a^{-1}b^{-1}$

Es kommen a, b, c in w vor und es gilt

$$\sigma_a(w) = 0 \quad \sigma_b(w) = -1 \quad \sigma_c(w) = 42.$$

Es bezeichne r ein zyklisch reduziertes Wort und

$$G = F(\Sigma) / \{ r = 1 \}$$

eine Einrelatorgruppe.

Der Freiheitssatz von Magnus und die Entscheidbarkeit des Wortproblems

Theorem (Klassische Form)

Sei r zyklisch reduziert und $G = F(\Sigma)/\{r = 1\}$ sowie $e \in \alpha(r)$.
(e wie „entfernen“)
Es sei K die von $\Sigma_e = \Sigma \setminus \{e\}$ erzeugte Untergruppe in G.

1.) *Die Gruppe K ist frei mit Basis Σ_e.*

2.) *Das Wortproblem von G ist entscheidbar.*

Beweis. Wir zeigen die Freiheit von K mit Basis $\Sigma \setminus \{e\}$ und ein stärkeres Entscheidbarkeitsresultat mit Induktion nach r. Zunächst formulieren wir dieses Resultat. □

Theorem (Rationale Form der Entscheidbarkeit)

Es sei $\Delta = \Sigma \cup \overline{\Sigma}$ *und* $\Delta_e = \Delta \setminus \{e, \overline{e}\}$.
Es gibt einen Algorithmus, der das folgende Problem löst:
Eingabe:

1.) *Ein zyklisch reduziertes* $r \in \Delta^*$.
2.) *Ein Buchstabe* $e \in \alpha(r)$.
3.) *Ein Wort* $w \in \Delta^*$.
4.) *Eine reguläre (rationale) Menge* $L \subseteq \Delta_e^*$.

Wir lesen $w \in G$ *und* $L \in \mathrm{Rat}(K) \subseteq \mathrm{Rat}(G) = \mathrm{Rat}(F(\Sigma)/\{r = 1\})$.
Frage: *Gilt* $w \in L$*?*

Beachte, das Wortproblem ist der Spezialfall $L = \{1\}$.

Beweis des Satzes von Magnus

Wir zeigen simultan die Freiheit von K und das obige Entscheidbarkeitsresultat mit Induktion nach $|r|$.
Für $|r| = 0$ ist die Aussage trivial. Sei als nächstes $r = e^n$ für ein $n > 0$. Dann ist G das freie Produkt von der freien Gruppe $K = F(\Sigma_e)$ und der zyklischen Gruppe $\mathbb{Z}/n\mathbb{Z}$. Die Behauptung folgt, da $\mathrm{Rat}(G)$ eine effektive Boolesche Algebra ist.
(Benois-Beweis für freie Produkte freier und endlicher Gruppen.)

Ab jetzt: $r \neq e^n$ für alle e und n.

Seien also $a, b \in \alpha(r)$, $a \neq b$ und $e = a$ oder $e = b$. Wir können die obigen Behauptungen für alle kürzeren r annehmen. Wir schreiben $\Sigma = \{ a, b, c, \dots \}$.

Fallunterscheidungen

1.) $\exists t \in \Sigma : \sigma_t(r) = 0$. Ohne Einschränkung $t = a$ und $e \in \{a, b\}$.

2.) Ohne Einschränkung $\sigma_a(r) \neq 0 \neq \sigma_b(r)$ und $e = b$.

Wir wollen G als HNN-Erweiterung schreiben bzw. in eine HNN-Erweiterung einbetten. Daher wählen wir neue Erzeugende t und y. Im ersten Fall setzen wir $\alpha = 0$ und $\beta = 1$, im zweiten Fall setzen wir $\alpha = \sigma_a(r)$ und $\beta = \sigma_b(r)$. Wir interpretieren einheitlich

$$a = t^{\beta}, \qquad b = yt^{-\alpha}.$$

Im ersten Fall ist $a = t$ und $\beta = y$ nur eine Umbenennung von Buchstaben.
Wir lesen $r = r(a, b, c, \ldots)$ und definieren s durch das Wort

$$s = r(t^{\beta}, yt^{-\alpha}, c, \ldots) \in F(t, y, c, \ldots).$$

Klar ist $\sigma_t(s) = 0$.
Ferner, wird s zyklisch reduziert so kommt y weiterhin vor. Dies ist klar für $\alpha = 0$ und $\beta = 1$. Im zweiten Fall folgt dies wegen $\sigma_y(s) = \sigma_b(r) = \beta \neq 0$.
Beachte, t kann verschwinden, etwa für $r = baba$ gilt $s = y^2$.

Wechsel zu $F(t, y, c, \ldots)/\{s = 1\}$

Wir definieren jetzt eine Gruppe G' durch

$$G' = F(t, y, c, \ldots)/\{s = 1\}$$

und einen Homomorphismus $\varphi : G \to G', \quad a \mapsto t^\beta, b \mapsto yt^{-\alpha}$. Wegen $s = r(t^\beta, yt^{-\alpha}, c, \ldots)$ ist dies wohldefiniert.

Für $\alpha = 0$ und $\beta = 1$ ist $G = G'$ bis auf die Umbenennung der Buchstaben. I. Allg. ist dies nicht richtig, aber immerhin eine Einbettung (wie wir gleich sehen werden).
Wegen $\sigma_t(s) = 0$ ist $\sigma_t : G' \to \mathbb{Z}$ wohldefiniert und damit ist $\langle t \rangle$ torsionsfrei in G'; und da $\varphi(a) = t^\beta$ und $\beta \neq 0$ ist auch $\langle a \rangle$ torsionsfrei in G.
Damit können wir das amalgamierte Produkt definieren:

$$G \star_{a=t^\beta} \langle t \rangle .$$

Die Abbildung $\varphi(a) = t^\beta$, $\varphi(b) = yt^{-\alpha}$ kann jetzt kanonisch zu einen surjektiven Homomorphismus fortgesetzt werden:

$$\widehat{\varphi} : G \star_{a=t^\beta} \langle t \rangle \to G'.$$

$G \star_{a=t^\beta} F(t) = G'$

Definiere

$$\psi(t) = t, \quad \psi(y) = bt^\alpha, \quad \psi(c) = c, \ldots$$

Dann ist $\psi(s) = r$ in $G \star_{a=t^\beta} \langle t \rangle$; also ist ψ ein Homomorphismus von G' nach $G \star_{a=t^\beta} F(t)$. Es ist

$$\psi\widehat{\varphi}(t) = t, \quad \psi\widehat{\varphi}(a) = t^\beta = a, \quad \psi\widehat{\varphi}(b) = b, \quad \psi\widehat{\varphi}(c) = c, \ldots$$

Damit ist $\widehat{\varphi}$ auch injektiv und ein Isomorphismus. Insbesondere ist $\varphi : G \to G'$ injektiv und für alle $L \in \mathrm{Rat}(G)$ die Äquivalenz:

$$w \in L \in \mathrm{Rat}(G) \iff \varphi(w) \in \varphi(L) \in \mathrm{Rat}(G')$$

Reduktion von G auf G'

Wir setzen $\Sigma' = (\Sigma \setminus \{ a, b \}) \cup \{ y, t \}$ und betrachten jetzt die folgende Fallunterscheidung:

1.) $e = b$:
Die von Σ_b erzeugte Untergruppe in G wird auf $\langle t^\beta, c, \ldots \rangle$ in G' abgebildet. Der Buchstabe y kommt in s vor, auch wenn s zyklisch reduziert wird. Die Untergruppe $\langle t^\beta, c, \ldots \rangle$ ist frei mit Basis $\{ t^\beta, c, \ldots \}$, falls $\langle t, c, \ldots \rangle$ frei mit Basis $\{ t, c, \ldots \}$ ist. Ferner gilt $\varphi(\mathrm{Rat}(\Delta_b)) \subseteq \mathrm{Rat}((\Delta'_y)$.

2.) $e = a$:
Dies war der Fall $\sigma_a(r) = 0$, also $a = t$ und $y = b$. Dann ist s nur eine Umbennung von r, also ist s schon zyklisch reduziert und t kommt in s vor.

Wir können also G' in beiden Fällen als Ausgangssituation betrachten. Der Gewinn ist $\sigma_t(s) = 0$, aber s kann länger geworden sein. Zu betrachten sind $e = y$ und $e = t$.

Wir können s zyklisch reduzieren und annehmen, dass y und t vorkommen

Sei für einen Moment F die freie Gruppe $F(t, y, c, \ldots)$. Dann ist $s \in F$ mit $\sigma_t(s) = 0$.
Wir reduzieren s zyklisch und schreiben für das neue Wort in Δ'^* wieder s. Falls t nicht mehr in s vorkommt gilt $|s| \leq |r| - 1$, da a in r vorkommt.
Also gilt in diesem Fall $|s| < |r|$ und wir sind fertig!
Dies passiert etwa für $r = baba$, dann ist

$$s = (yt^{-2})t^2(yt^{-2})t^2 = y^2.$$

Ohne Einschränkung gilt jetzt:

1. s ist zyklisch reduziert.
2. y und t kommen in s vor.
3. s beginnt mit dem Buchstaben y.

Umschreiben der Relation s

Das (zyklisch reduzierte) Wort $s \in \Delta'^*$ hat eine eindeutige Darstellung
$yt^{\varepsilon_1} a_2\ t^{\varepsilon_2} \cdots a_k t^{\varepsilon_k}$ mit $y, a_i \in \Delta'_t$ und $\varepsilon_i \in \mathbb{Z}$.
Wegen $\sigma_t(s) = 0$, so finden wir Zahlen j_i mit $j_2 = \varepsilon_1$ und $j_k = \varepsilon_1 + \cdots + \varepsilon_{k-1}$ in der Art, dass wir s in F wie folgt umschreiben können:

$$s = y(t^{j_2} a_2 t^{-j_2}) \cdots (t^{j_k} a_k t^{-j_k}) \in F$$

Für jeden Buchstaben z wählen wir ein $\mu(z)$ minimal und $m(z)$ maximal, dass die Faktoren $(t^{\mu(z)} z^{\pm 1} t^{-\mu(z)})$ und $(t^{m(z)} z^{\pm 1} t^{m(z)})$ in der Schreibweise von s erscheinen.
Beachte $\mu(y) \le 0 \le m(y)$, da $y = (t^0 y t^{-0})$.
Da t vorkommt, gilt ferner $\mu(z) < 0$ oder $0 < m(z)$ für ein z.
Für $z \in \Delta'_t$ und $\min\{0, \mu(z)\} \le i \le \max\{m(z), 0\}$ setzen wir: $z_i = t^i z t^{-i}$.
Wir erhalten damit ein neues endliches Alphabet $\Delta \times I$ mit
$\{ z_i \mid z \in \Delta'_t,\ \min\{0, \mu(z)\} \le i \le \max\{m(z), 0\} \} \subseteq \Delta_t \times I$ für ein $I \subseteq \mathbb{Z}$.
Wir setzen

$$\hat{s} = y_0 a_{2,j_2} \cdots a_{k,j_k}$$

Beispiel

$$s = yt^2y^{-1}t^{-3}c^{42}t^1y^{-1}$$

Dann gilt für das entsprechende Wort $\hat{s}$:

$$\hat{s} = y_0 y_2^{-1} c_{-1}^{42} y_0^{-1}.$$

Es ist $I = \{-1, \ldots, 42\}$.

Die Relation $\hat{s}$ ist zyklisch reduziert

Lemma
Es gilt:

1.) $|\hat{s}| < |r|$.

2.) $\hat{s} = y_0 a_{1,j_1} a_{2,j_2} \cdots a_{k,j_k}$. *ist zyklisch reduziert,*

Beweis. Die Aussage $|\hat{s}| < |r|$ ist trivial, da alle t fehlen.
Angenommen, eine zyklische Vertauschung von $\hat{s}$ enthält den Faktor $a_{i,j}\,\overline{a_{i,j}}$. Dann entspricht dies einem Faktor $(t^j a_i t^{-j})(t^j \overline{a_i} t^{-j}) = a_i\,\overline{a_i}$ in einem zu s zyklisch äquivalenten Wort. Aber s ist nach Annahme zyklisch reduziert. □

Die freien Gruppen A und B

Wir definieren $I(z) = \{\, i \in \mathbb{Z} \mid \min\{0, \mu(z)\} \leq i \leq \max\{m(z), 0\} \,\}$.
Es gilt $0 \in I(z)$. Betrachte ab jetzt die Gruppe

$$H = F(y_i, c_i, \ldots; i \in I(z))/\hat{s}$$

Wir setzen $L = \{\, z_i \mid i \in I(z), i < \max\{m(z), 0\} \,\}$ und
$U = \{\, z_i \mid i \in I(z), \min\{0, \mu(z)\} < i \,\}$.
Man beachte, es gibt ein $\mu(z) < 0$ oder $m(z) > 0$, daher ist weder L noch U leer. (Es kam ein t vor, daher $\mu(z) < 0$ oder $m(z) > 0$.)
Für $m(z) > 0$, gilt $z_0 \in L$ und $z_{m(z)} \in U$.
Ferner gilt $y_{\mu(y)} \notin U$ und analog $y_{m(y)} \notin L$.
Mit Induktion sind die Gruppen $A = \langle z_i \in L \rangle$ und $B = \langle z_i \in U \rangle$ frei mit den entsprechenden Basen und $z_i \mapsto z_{i+1}$ induziert einen Isomorphismus zwischen diesen freien Untergruppen.

HNN mit t

Definiere die HNN-Erweiterung H' von H mit t mittels $\varphi : A \to B, z_i \mapsto z_{i+1}$. Also

$$H' = \mathrm{HNN}(H, t; A, B, \varphi) = \langle H, t \rangle \,/\, \left\{ t z_i t^{-1} = z_{i+1} \;\middle|\; z_i \in A \right\}$$

Es gibt kanonische Homomorphismen:

1.) $\psi : H \to G'$ mittels $z_i \mapsto t^i z t^{-i}$, denn dieser bildet $\hat{s}$ auf $s \in F(\Sigma')$ ab.

2.) Wir erweitern dies zu einer Surjektion $\psi : H' \to G'$ mittels $t \mapsto t$.

3.) Die Umkehrabbildung ψ' wird durch $\psi'(z) = z_0$ und $\psi'(t) = t$ gegeben. Die Relationen $t z_i t^{-1} = z_{i+1}$ zeigen $\psi'(\psi(z_i)) = z_i$.

4.) Damit können wir schreiben: $G' = H'$.

5.) Es gilt $G \leq H'$ aber i.Allg. nicht $G \leq H$.

Das Wortproblem für G' ist lösbar

Das Wortproblem für H' ist lösbar mit Brittons Lemma, denn

1.) Das Wortproblem für H ist induktiv entscheidbar.

2.) φ ist effektiv berechenbar.

3.) „$w \in A$?“ und „$w \in B$?“ können wir induktiv entscheiden, da dies rationale Mengen der gewünschten Form sind.

Wir müssen aber mehr zeigen: Es bleibt zu entscheiden, ob „$w \in L$?“ gilt.

Fall $e = t$

Die Frage „$w \in L$?“ für $L \in \mathrm{Rat}(G')$ übersetzt sich in „$\psi'(w) \in L' = \psi'(L)$?“, wobei $L' \in \mathrm{Rat}(\langle \{ y_0, c_0, \dots \} \rangle) \subseteq \mathrm{Rat}(H)$ liegt (wegen $e = t$). Da $\mu(z) < 0$ oder $0 < m(z)$ für ein z gilt, können wir dies Problem induktiv lösen, indem wir zunächst mittels einer Britton-Reduktion $\psi'(w) \in H$ nachweisen.
Ferner ist wegen $\mu(z) < 0$ oder $0 < m(z)$ die Gruppe $\langle \{ y_0, c_0, \dots \} \rangle$ eine freie Untergruppe von H mit Basis $\{ y_0, c_0, \dots \}$.
Also ist auch $\langle \{ y, c, \dots \} \rangle$ eine freie Untergruppe von G' mit Basis $\{ y, c, \dots \}$.

Fall $e = y$

Betrachte die kanonische Abbildung $\pi : F(\Sigma'_y) \to G'$. Das Bild ist die Gruppe

$$K = \langle \{\, t, c_0, \dots \} \rangle = \langle \{\, t, c_i, \dots ; i \in I(z) \,\} \rangle \,.$$

Sei $\pi(v) = 1$ für ein frei reduziertes Wort v. Dann muss $\sigma_t(v) = 0$ gelten, da $\sigma_t(s) = 0$ gilt.
Genau wie wir s in $\hat{s}$ umgeschrieben haben, kann $\pi(v)$ in $\hat{v}$ umgeschrieben werden.
Nach dem obigen Verfahren ist $\hat{v}$ ein Britton reduziertes Wort in t und $\{\, c_i, \dots ; i \in I(c) \,\}$, da in v kein y vorkommt. Die Untergruppe $\{\, c_i, \dots ; i \in I(c) \,\}$ ist frei in H, also auch frei in G'. Daher ist $\hat{v}$ das leere Wort und v besteht nur aus t.
Wegen $\sigma_t(v) = 0$ ist dann v ebenfalls leer.
Also ist π ein kanonischer Isomorphismus zwischen $F(\Sigma'_e)$ und K. Die Gruppe K ist frei.

Rationale Mengen, $y = e$

Sei $w \in \Delta'^*$ und $R \in \mathrm{Rat}(K) = \mathrm{Rat}(F(\Sigma'_e))$.
Aus $w \in R$ folgt $w \in K$ und für $w \in K$ können wir $w \in R$ testen, da rationale Mengen in freien Gruppen eine effektive Boolesche Algebra bilden.
Das Problem ist, wir müssen hierfür ein Wort aus Δ'^* zunächst in ein Wort aus K umzurechnen!

Rationale Mengen, $y = e$

Sei zunächst $u \in \Delta_y'^*$ frei reduziert. Dies impliziert, dass die Britton-Reduktion von u stets nur aus c_i und t besteht.
Schreibe jetzt w in Britton reduzierter Form. Für $w \in H$ sind wir fertig, denn es reicht jetzt, $w \in F(c_i; i \in I(c))$ zu testen.
Ohne Einschränkung beginnt w mit einem Faktor $w_0 t$. Ist also w äquivalent zu einem (Britton reduzierten) $u \in \Delta_y'^*$, so beginnt auch u mit $u_0 t$ und u_0 benutzt nur c_i.
Beachte, $u_0^{-1} u$ beginnt mit t. Ferner ist $u_0^{-1} w$ das gleiche Element in der HNN wie $u_0^{-1} u$. Wegen $t z_i = z_{i+1} t$ folgt $u_0^{-1} w_0 \in B$. Insbesondere, $w_0 \in F(c_i; i \in I(c)) \cdot B$, was wir testen können, da sich alles in der freien Gruppe abspielt, die $y_{\mu(y)}$ nicht benutzt. Im positiven Fall gilt $w_0 t = w_0' v t$ mit $w_0' \in F(c_i; i \in I(c))$ mit $v \in B$. Ferner ist $w_0' t \in K$.
Es gilt $w = w_0' t v' w''$ und $w' = v' w'' = t^{-1} {w'}_0^{-1} w$, wobei $v' = \varphi^{-1}(v)$ ist.
Es reicht daher $w' \in K$ zu testen. Die Britton-Reduktion von w' enthält genau ein t weniger. Wir können mit Induktion das gewünschte Ergebnis erhalten.