Kombinatorische Gruppentheorie

Volker Diekert[1]

Sommersemester 2019

[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.

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:

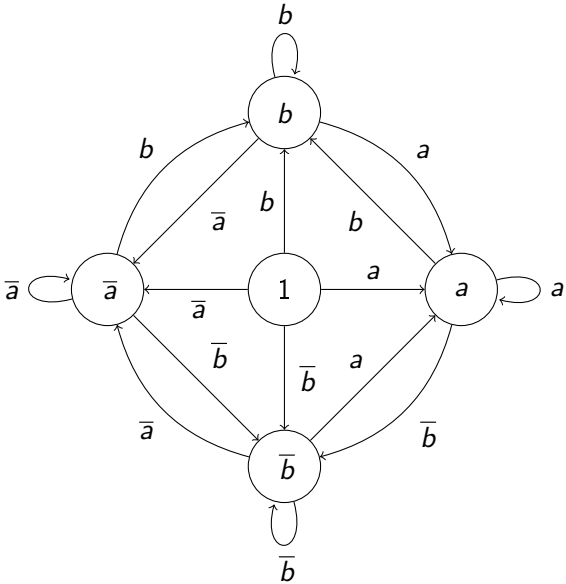
$$\mathrm{Hom}(F(\Sigma), G) = \mathrm{Abb}(\Sigma, G).$$

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.

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

Es reicht zu zeigen, dass irreduzible Nachfolger in Linearzeit berechnet werden können!
Eingabe $w \in \Delta^*$ mit $|w| = n$.

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

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

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 $a \in \Sigma$.

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. □

Graphen

Definition

Ein (ungerichteter) Graph Γ ist gegeben durch:

1.) $X =$ Knoten von Γ.

2.) $Y =$ Kanten von Γ.

3.) $Y \to X \times X$, $y \mapsto (s(y), t(y))$,
$s(y) = \text{source}(y)$, $t(y) = \text{target}(y)$.

4.) Involution: $y \mapsto \overline{y}$ mit $\overline{\overline{y}} = y$, $s(\overline{y}) = t(y)$ $y \neq \overline{y}$ und $t(\overline{y}) = s(y)$.

Wir zeichnen (und zählen!) $\{ y, \overline{y} \}$ als eine Kante und benutzen ggf. Pfeile um die Kanten zu unterscheiden. Ein ungerichteter Graph hat in der Interpretation „gerichtet“ doppelt so viele Kanten.
Merkregel: Aufpassen, was jeweils gemeint ist. Serre zählt daher ungerichtete Kannten gleich doppelt und umgeht damit dieses Problem.

Pfade, geschlossene Wege und Kreise

Definition

1.) Ein *Pfad* besteht aus einer Folge $p = y_1 \cdots y_n$ von Kanten mit $t(y_i) = s(y_{i+1})$ sowie dem Anfangspunkt $s(y_1)$.
Wir setzen $s(p) = s(y_1)$ und $t(p) = t(y_n)$. Ist er doppelpunktfrei, enthält er $n+1$ Knoten und wird häufig mit P_{n+1} bezeichnet.

2.) Ein *geschlossener Weg* ist ein Pfad p mit $s(p) = t(p)$.

3.) Ein *Kreis* ist ein geschlossener Weg $y_1 \cdots y_{n-1}$ ohne *Zurücksetzen*, d.h., $y_{i+1} = \overline{y_i}$ kommt nicht vor.

Man beachte, ist ein Kreis $y_1 \cdots y_n$ ohne Zurücksetzen und $y_1 = \overline{y_n}$, so ist $y_2 \cdots y_{n-1}$ ein geschlossener Weg ohne Zurücksetzen oder der Kreis eine Schlinge.
Enthält Γ einen Kreis, so auch einen doppelpunktfreien Kreis $y_1 = \overline{y_n}$ mit $y_{i+1} \neq \overline{y_i}$ für alle i mod n.

Fundamentalgruppen

Definition

Sei x_0 ein Knoten in Γ, dann bildet die Menge der geschlossene Wege p mit $x_0 = s(p) = t(p)$ eine Gruppe.
Diese wird, modulo $y\,\overline{y} = 1$, als *Fundamentalgruppe* $\pi_1(\Gamma, x_0)$ bezeichnet.

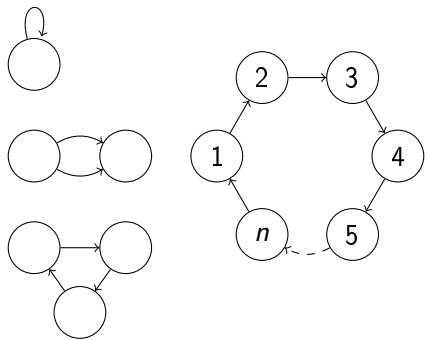
Das Inverse von $p = y_1 \cdots y_m$ ist $\overline{p} = \overline{y_m} \cdots \overline{y}_1$ Gibt es einen Pfad von x_0 nach x_1, so sind $\pi_1(\Gamma, x_0)$ und $\pi_1(\Gamma, x_1)$ isomorph. Insbesondere können wir für zusammenhängende Graphen $\pi_1(\Gamma)$ unabhängig vom Basispunkt x_0 definieren.

Bäume

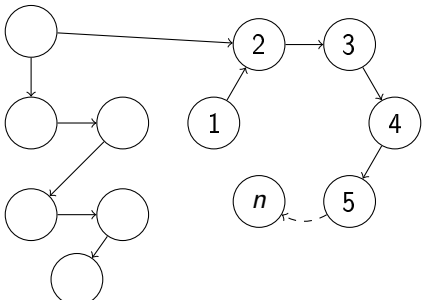
Definition

Ein *Baum* ist ein zusammenhängender kreisfreier Graph.

Keine Bäume sind:



Ein Baum



Cayley-Graphen

Definition

Sei G eine Gruppe und $\Sigma \subseteq G$. Der *Cayley-Graph* $\mathcal{C}(G, \Sigma)$ ist der folgende gerichtete Graph mit Knotenmenge G und Kantenmenge $G \times \Sigma$, wobei $s(g, a) = g$ und $t(g, a) = ga$ gelten soll.
Wir setzen ferner $\overline{(g, a)} = (ga, \overline{a})$ mit $\overline{a} = a^{-1}$ und lesen $\mathcal{C}(G, \Sigma)$ auch als ungerichteten Graphen mit Kantenmenge $G \times \Delta$.
Hier ist $\Delta = \Sigma \cup \Sigma^{-1}$.

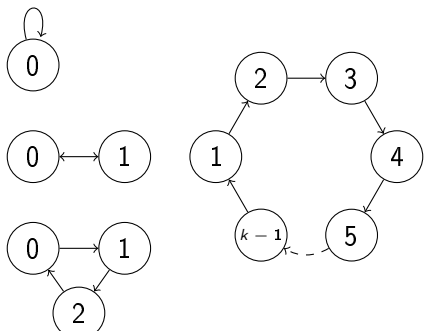
Eine Kante (g, a) verbindet die Knoten g und ga und kann daher als ungerichtete Kante auch mit der Menge $\{g, ga\}$ identifiziert werden.
Etwas allgemeiner

Definition

Sei Δ ein Alphabet mit Involution, $\pi : \Delta \to G$ eine Abbildung mit $\pi(\overline{a}) = \pi(a)^{-1}$.
Dann kann der *Cayley-Graph* $\mathcal{C}(G, \pi)$ vollkommen analog definiert werden.

Cayley-Graphen zyklischer Gruppen

Sei $\Sigma = \{a\}$ und $G = \mathbb{Z}/n\mathbb{Z} = a^*/a^n = 1$ für $n = 1, 2, 3, \ldots, k$ mit $k > 4$.

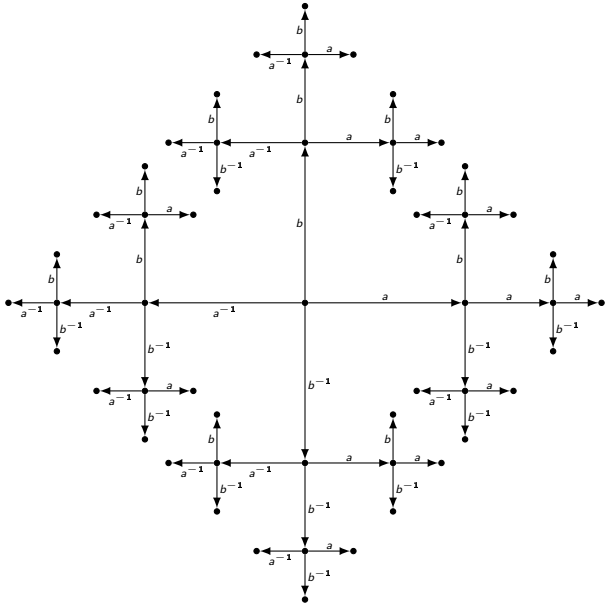


Zwei Cayley-Graphen für $\mathbb{Z}/2\mathbb{Z}$

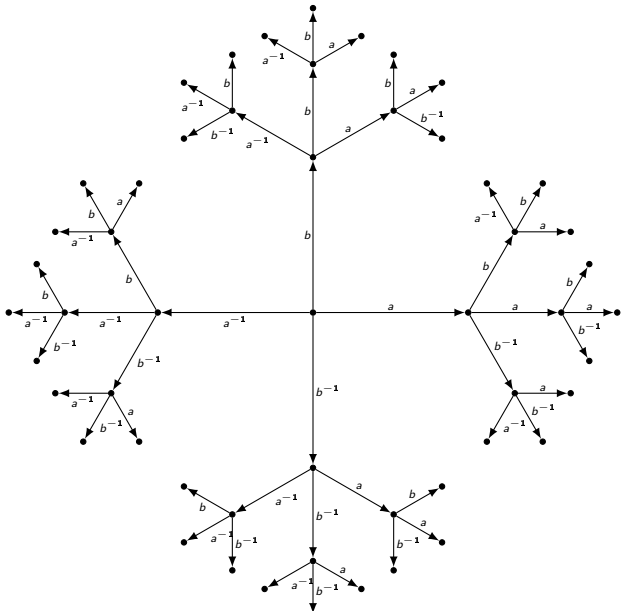
Sei $\Sigma = \{a\}$ und $G = \mathbb{Z}/2\mathbb{Z}$.

Sei $\Sigma = \{a\}$, $\Delta = \{a, \overline{a}\}$, $a \neq \overline{a}$ und $G = \mathbb{Z}/2\mathbb{Z}$.

Cayley-Graphen freier Gruppen sind Bäume



Bäume sind schwierig zu zeichnen



$\mathcal{C}(G, \Sigma)$ codiert Eigenschaften von G

Bemerkung

1. *Wegen* $\Sigma \subseteq G$ *hat* $\mathcal{C}(G, \Sigma)$ *keine Mehrfachkanten.*
2. $\mathcal{C}(G, \Sigma)$ *ist zusammenhängend genau dann, wenn* Σ *die Gruppe* G *erzeugt.*
3. $\mathcal{C}(G, \Sigma)$ *ist schlingenfrei genau dann, wenn* $1 \notin \Sigma$.
4. $\forall g \in G\ \forall a \in \Sigma:\ g \cdot (h, a) \neq \overline{(h, a)} \iff \forall a \in \Sigma:\ a^2 \neq 1$

Interessant (für uns) sind daher (vor allem) zusammenhängende und schlingenfreie Graphen ohne Mehrfachkanten, auf deren Kanten eine Gruppe G ohne *Inversion* operiert.

Ungerichtete Cayley-Graphen

Häufig reicht es, nur ungerichtete Graphen zu betrachten:

Definition

Sei G eine Gruppe und $\Sigma \subseteq G$. Der *Cayley-Graph* $\mathcal{C}(G, \Sigma)$ ist der ungerichtete Graph mit Knotenmenge G und Kantenmenge

$$E = \{\, \{g, ga\} \mid g \in G, a \in \Sigma \,\}.$$

Es gilt $E \subseteq \binom{G}{2}$, falls $1 \notin \Sigma$.

Gruppenoperationen auf Graphen

Definition

1. Eine Gruppe G operiert auf eine Menge X vermöge $\cdot : G \times X \to X$, wenn gilt:

$$1_G \cdot x = x \text{ und } \quad (gh) \cdot x = g \cdot (h \cdot x).$$

2. Sie operiert auf einem Graphen Γ, wenn sie auf der Knotenmenge X und Kantenmenge Y operiert und es gilt:

$$g \cdot s(y) = s(g \cdot y), \quad g \cdot t(y) = t(g \cdot y) \quad g \cdot \overline{y} = \overline{g \cdot y}.$$

Gruppenoperationen auf Cayley-Graphen

Eine Gruppe G operiert auf dem Cayley-Graphen $\mathcal{C}(G, \Sigma)$ durch Linkstranslation: $g \cdot h = gh$ und $g \cdot (h, a) = (gh, a)$.
Beachte,

$$g \cdot (h, a) = \overline{(h, a)} \iff (gh, a) = (ha, \overline{a}) \iff a^2 = 1 \wedge g = hah^{-1}.$$

Interpretieren wir $\mathcal{C}(G, \Sigma) = (G, E)$ ungerichtet, so gilt

$$g \cdot \{ h, ha \} = \{ gh, gha \}.$$

Freiheit ohne Inversion

Definition

Eine Gruppe G operiert auf einem Graphen Γ mit Knotenmenge X und Kantenmenge Y *frei (und ohne Inversion)*, wenn für $g \neq 1$ gilt:

1. $g \cdot x \neq x$,
2. $g \cdot y \neq \overline{y}$.

Es gilt $a^2 \neq 1$ für alle $a \in \Sigma$ genau dann, wenn G auf dem Cayley-Graphen $\mathcal{C}(G, \Sigma)$ frei und ohne Inversion operiert. Denn für $g \neq 1$ gilt
$\{ gh, gha \} = \{ h, ha \} \iff gh = ha \;\&\; gha = h \implies a^2 = 1$. Die Umkehrung ist klar.

Bemerkung

G operiert frei und ohne Inversion auf Γ, wenn G frei auf der Knotenmenge und frei auf der ungerichteten Kantenmenge $\{ \{y, \overline{y}\} \mid y \in Y \}$ operiert.