<u>Todd-Coxeter-Prozedur mit Gröbner-Techniken</u>

(Quelle: Reports on Computer Algebra No. 19, B. Reinert, K. Madlener, T. Mora)
gehalten von: Eva Ludwig am 19.11.'03

1 Notationen:

Sei $\Sigma = \{a_1, ..., a_n\}$ ein Alphabet; $\overline{\Sigma} = \Sigma \cup \Sigma^{-1}$, wobei $\Sigma^{-1} = \{a^{-1} \mid a \in \Sigma\}$. $\overline{\Sigma}^*$ bezeichne alle frei reduzierten Wörter über $\overline{\Sigma}$ (vgl. Abschnitt 2). λ ist immer das leere Wort.
Wir betrachten eine Gruppe $\mathcal{G}$ erzeugt von Σ und den Relatoren R. $\mathcal{U}$ sei eine Untergruppe von $\mathcal{G}$, und $\mathcal{H}$ sei erzeugt von $U \cup N(R)$, wobei U Untergruppe der von Σ erzeugten freien Gruppe $\mathcal{F}$ ist.
Die Operation "$\circ$" ist die Verkettung zweier Wörter in $\mathcal{F}$ mit anschließender freier Reduktion (vgl. Abschnitt 2).
$\mathbb{K}[\mathcal{F}]$ ist der freie Gruppenring, in dem "$\cdot$" die Skalarmultiplikation und "$*$" die Multiplikation zweier Elemente in $\mathbb{K}[\mathcal{F}]$, also zweier Polynome, bezeichnet.
<u>Definition:</u> Seien $f, p \in \mathbb{K}[\mathcal{F}]$ zwei Polynome. f präfix-reduziert p zu q in einem Monom $\alpha \cdot t, \alpha \in \mathbb{K} \setminus \{0\}, t \in \mathcal{F}$ in einem Schritt, bezeichnet mit $p \rightarrow_f^p q$, falls der Leitterm von f ein Präfix von t ist, also $LT(f) \circ w \equiv t$, für ein $w \in \overline{\Sigma}^*$.

2 Nielsen-Reduktion:

Hier soll keine komplette Behandlung der Nielsen-Reduktion erfolgen. Für diesen Vortrag genügt die Kenntnis des Verfahrens und der damit verbundenen Begriffe. Auf einer Teilmenge U einer freien Gruppe $\mathcal{F}$ kann man die elementaren Nielsentransformationen definieren:
(T1) Ersetze ein $u_i \in U$ durch das dazu inverse Element u_i^{-1}
(T2) Ersetze ein $u_i \in U$ durch $u_i \circ u_j$ wobei $i \neq j$
(T3) Streiche alle $u_i \in U$ mit $u_i = \lambda$
In jedem dieser Fälle bleiben alle anderen u_k unverändert. Ein Produkt dieser elementaren Transformationen heißt Nielsen-Transformation.
Es gilt: Wird eine Teilmenge U von $\mathcal{F}$ durch Nielsentransformationen in eine Menge U' umgeformt, so erzeugen U und U' dieselbe Untergruppe. Eine Menge U heißt nielsenreduziert, falls $\forall u, v, w \in U \cup U^{-1}$ gilt:
(N0) $u \neq \lambda$
(N1) $u \circ v \neq \lambda \Rightarrow \mid u \circ v \mid \geq max\{\mid u \mid, \mid v \mid\}$
(N2) $u \circ v \neq \lambda$ und $v \circ w \neq \lambda \Rightarrow \mid u \circ v \circ w \mid > \mid u \mid - \mid v \mid + \mid w \mid$
<u>Beispiel:</u> $U := \{uv, u^{-1}v\} \rightarrow \{v^{-1}u^{-1}, u^{-1}v\} \rightarrow \{v^{-1}u^{-1}, u^{-1}vv^{-1}u^{-1} = x^{-2}\} \rightarrow \{uv, u^2\}$

3 Todd-Coxeter:

Eine Gruppe $G = \langle \Sigma, R \rangle$ kann aufgefasst werden als Quotient der freien Gruppe $\mathcal{F} = \langle \Sigma \rangle$ mit dem Normalteiler $N(R) = \langle \{w \circ r \circ w^{-1} \mid w \in \mathcal{F}, r \in R\} \rangle$.
Der Index $\mid G : U \mid$ einer Untergruppe U von G ist die Anzahl der Rechtsnebenklassen $Ug = \{u \circ g \mid u \in U\}, g \in G$. Dieser ist identisch mit dem

Index der Untergruppe $\mathcal{H} = \langle U \cup N(R) \rangle$ in der freien Gruppe $\mathcal{F}$, was wir später benötigen. Die Todd-Coxeter-Prozedur liefert nun den Index $\mid G : U \mid$, falls dieser endlich ist, und die zugehörige Multiplikationstafel:
Voraussetzung: $G = \langle \Sigma, R \rangle$, $U \subseteq \overline{\Sigma}^*$, jedes Erzeugende $a \in \Sigma$ tritt in mindestens einer definierenden Relation auf.
Regeln: 1. Die Relatoren operieren trivial.
2. Die Erzeugenden von U lassen die Nebenklasse $U\lambda$,λ das leere Wort, fest.
3. Die Operationen auf der Menge der Nebenklassen sind transitiv.
Prozedur: In jedem Schritt wird eine Menge I von Restklassenrepräsentanten betrachtet, zu Beginn $I = \{\lambda\}$. Das Verfahren lässt sich am einfachsten tabellarisch aufschreiben: Für jede Relation wird eine Tabelle angelegt, wobei in der ersten und letzten Spalte die Repräsentanten aus I in der auftretenden Reihenfolge stehen und in jeder der dazwischenliegenden Spalten jeweils der Repräsentant steht, der durch Rechtsmultiplikation mit dem ersten/zweiten/usw. Buchstaben der Relation aus dem Eintrag der vorigen Spalte entsteht. Es wird zeilenweise gearbeitet. Hierbei gilt:
1. Setze zwei Repräsentanten gleich, wenn dies aus einer der Regeln folgt.
2. Lasse den neuen Repräsentanten stehen und schreibe ihn in I, nur falls 1. nicht möglich ist. (Neue Repräsentanten ergeben sich beim Auffüllen der Zeilen.)
Die Prozedur endet, wenn alle Tabellen vollständig und widerspruchsfrei gefunden wurden, und alle Regeln erfüllt sind.
Endlichkeit: Dieses Verfahren endet, falls der Index $\mid G : U \mid$ endlich ist. Dann kann man aus den Tabellen die Multiplikationstafel und den Index $\mid G : U \mid$ bzw. $\mid \mathcal{F} : \mathcal{H} \mid$ ablesen.
Beispiel: $G = \langle a, b \mid a^3, b^3, abab \rangle$, $U = \{a\}$. Um Eindeutigkeit der Restklassenrepräsentanten zu erhalten nutzen wir die lexikographische Ordnung mit $a < b < a^{-1} < b^{-1}$.

a	
λ	λ

Dies bedeutet: Die Erzeugenden von U lassen Uλ fest: $\lambda a = \lambda$.

	a	a	a	
1.				
λ	λ	λ	λ	
b	b^{-1}	$b^{-1}a = ba^{-1}$	b	
b^{-1}	$b^{-1}a = ba^{-1}$	b	b^{-1}	
ba^{-1}	b	b^{-1}	ba^{-1}	

	b	b	b	
2.				
λ	b	$b^2 = b^{-1}$	λ	
b	b^{-1}	λ	b	
b^{-1}	λ	b	b^{-1}	
ba^{-1}	ba^{-1}	ba^{-1}	ba^{-1}	

	a	b	a	b
3.				
λ	λ	b	ba=b^{-1}	λ
b	b^{-1}	λ	λ	b
b^{-1}	ba^{-1}	$ba^{-1}b = ba^{-1}$	$ba^{-1}ba = b$	b^{-1}
ba^{-1}	b	b^{-1}	ba^{-1}	ba^{-1}

Betrachte zunächst jeweils die erste Zeile, $I = \{\lambda\}$: In Tabelle 2 ergibt sich durch rückwärtslesen von der letzten in die vorletzte Spalte $\lambda b^{-1} = b^2$ und in Tabelle 3 $\lambda b^{-1} = ba$ als neue Regeln. Außerdem tritt in Tabelle 2 ein b auf. Wir fügen also b und b^{-1} zu I hinzu. Dann ist λ abgearbeitet und wir betrachten das nächst größere Erzeugende b in der jeweils zweiten Zeile, wobei die neuen Regeln direkt angewendet werden: Aus Tabelle 1 folgt $ba^{-1} = b^{-1}a$, im Weiteren wird das bzgl. der Ordnung kleinere der beiden verwendet. Jetzt ist $I = \{\lambda, b, b^{-1}, ba^{-1}\}$. In den weiteren Tabellen ergibt sich nichts neues mehr, also betrachten wir b^{-1} in der dritten Zeile: Wir erhalten in der dritten Tabelle durch Rückwärtslesen zunächst von der letzten zur vorletzten Spalte und dann zu der davor: $[b = (b^2)^{-1} =]b^{-2} = ba^{-1}ba$ und $ba^{-1} = bab^{-1}$, so dass keine neuen Elemente zu I hinzukommen. In der letzten Zeile wird nun ba^{-1} betrachtet und wir erhalten vollständige und wohldefinierte Tabellen, wobei alle Regeln erfüllt sind.

4 Umformung in Gröbner-Basis

In kommutativen Polynomringen entspricht die Gröbner-Basis eines Ideals der Basis des zugehörigen Quotientenringes. Diese natürliche Basis kann berechnet werden, und man erhält ebenfalls eine Multiplikationstafel. Mit binomialen Polynomen können diese Einträge als Terme aufgefasst werden. Die Ausgabe entspricht der von Todd-Coxeter.

Die Eingabe wird binomial kodiert. Statt wie bei Todd-Coxeter die Menge der Relatoren R und die Menge der Untergruppenerzeugenden von U anzugeben, nutzt man die kodierten Mengen $F_R = \{r - 1 \mid r \in R\}$ und $F_U = \{u - 1 \mid u \in U\}$. Dann überprüft man, ob die Untergruppe erzeugt von $U \cup N(R)$ in $\mathcal{F}$ endlich erzeugt ist. Wir wissen, wenn dies der Fall ist, ist das Zugehörigkeitsproblem mit einer Präfix-Gröbner-Basis lösbar. Da dies in vorigen Vorträgen behandelt wurde, gehe ich an dieser Stelle nicht näher darauf ein.

Die Berechnung einer monomialen-reduzierten Präfix-Gröbner-Basis geschieht wie folgt:

<u>Definition:</u> Eine Menge $F \subseteq \mathbb{K}[\mathcal{F}]$ heißt präfix-reduziert, falls kein Polynom in F durch ein anderes Polynom in F präfix-reduzierbar ist.

<u>Definition:</u> Eine Menge $F \subseteq \mathbb{K}[\mathcal{F}]$ heißt schwach-präfix-saturiert, falls $\forall p \in F, w \in \mathcal{F}$ gilt: $p * w \overset{*}{\to}{}^{p}_{F} 0$.

<u>Satz:</u> Die Menge $F \subseteq \mathbb{K}[\mathcal{F}]$ ist genau dann Präfix-Gröbner-Basis des von ihr erzeugten rechtsseitigen Ideals, wenn sie präfix-reduziert und schwach-präfix-saturiert ist.

Die letzte Eigenschaft kann man sichern, indem man die saturierende Menge für ein Polynom so wählt, dass jedes rechte Vielfache des Polynoms in einem Schritt auf 0 präfix-reduzierbar ist durch ein Polynom aus der saturierenden Menge. In freien Gruppen bestehen diese saturierenden Mengen aus höchstens zwei Polynomen, genannt can und $acan$. Bei Binomen $u - v$ erhalten wir $can(u - v)$ durch (u.U. mehrmaliges) Kürzen des Leitterms u mit dem Inversen des letzten Buchstabens von u. Dies wiederholt man solange, bis der Leitterm seine führende Position verliert. Nun ist das vorletzte Binom der Kürzungskette $can(u - v)$, das letzte ist $acan(u - v)$, also genau das Binom, dass man aus $can(u - v)$ durch Kürzen des Leitterms unter Verlust seiner führenden Position erhält. Dann ist $can(u-v) = xa - y$ und $acan(u-v) = (xa-y) \circ a^{-1}$ mit $x, y \in \mathcal{F}, a, a^{-1} \in \overline{\Sigma}$. Dann existiert $w \in \mathcal{F}$ so, dass $u \equiv xaw, y = v \circ w^{-1}, LT(can(u-v)) = LT((u-v) \circ w^{-1}) = u \circ w^{-1} \equiv xa$ und $LT(acan(u-v)) = LT((u-v) \circ w^{-1}a^{-1} = v \circ w^{-1}a^{-1} \equiv ya^{-1}$.

Prozedur: Gegeben: endliche Menge $F \subseteq \mathbb{K}[\mathcal{F}]$.
Finde: monomiale-reduzierte Präfix-Gröbner-Basis G des durch F erzeugten rechtsseitegen Ideals.
1. Beginne mit $G := \{can(f), acan(f) \mid f \in F\}$.
2. Solange ein $g \in G$ existiert mit $LT(g)$ ist präfix-reduzierbar durch $G \setminus \{g\}$ führe Schritte 3 bis 5 aus.
    3. Nehme dieses g aus G.
    4. Berechne die mit G präfix-reduzierte Normalform von g, und nenne diese f. Für $f \neq 0$ normiere den Leitkoeffizienten auf 1.
    5. Falls $f \neq 0$ füge $can(f)$ und $acan(f)$ zu G hinzu.

Satz Sei $U \subseteq \mathcal{F}$ endl. Teilmenge, G monomiale-reduzierte Präfix-Gröbner-Basis des rechtsseitigen Ideals erzeugt von F_U in $\mathbb{K}[\mathcal{F}]$. Dann ist $X_G = \{uv^{-1} \mid u - v \in G\}$ nielsen-reduziert für U (vgl. Doktorarbeit B. Reinert).
Die zu untersuchende Frage ist nun: Ist die evtl. unendlich erzeugte Untergruppe $\mathcal{H} = \langle U \cup N(R) \rangle \subseteq \mathcal{F}$, wobei $R \neq \varnothing$, tatsächlich endlich erzeugt? Hierzu benötigen wir noch einige Aussagen:
Notation: Für $F \subseteq \mathbb{K}[F]$ bezeichnet $ideal(F)$ das beidseitige Ideal und $ideal_r(F)$ das rechtsseitige Ideal erzeugt von F in $\mathbb{K}[F]$.
Äquivalent sind: Für $F \subseteq \mathbb{K}[\mathcal{F}]$:
1. F ist Präfix-Gröbner-Basis von $ideal_r(F)$ und $ideal_r(F) = ideal(F)$.
2. F ist Präfix-Gröbner-Basis von $ideal_r(F)$ und für alle $w \in \mathcal{F}$, $p \in F$ ist $w * p \in ideal_r(F)$.
3. F ist Präfix-Gröbner-Basis von $ideal_r(F)$ und für alle $a \in \overline{\Sigma}$, $p \in F$ ist $a * p \in ideal_r(F)$.
Auf dieser Aussage fußt der nun folgende Algorithmus.

5 Restklassenaufzählung mit Gröbner-Techniken:

Gegeben sind wie vorher: Gruppe $\mathcal{G}$ erzeugt von $\Sigma = \{a_1, ..., a_n\}$ mit den Relatoren R. $\mathcal{U}$ sei eine Untergruppe von $\mathcal{G}$, und $\mathcal{H}$ sei erzeugt von $U \cup N(R)$, wobei U Untergruppe der von Σ erzeugten freien Gruppe $\mathcal{F}$ ist.

Eingabe: - eine Kodierung von R und U als binomiale Mengen $F_r = \{r - 1 \mid r \in R\}$ und $F_U = \{u - 1 \mid u \in U\}$
außerdem genutzt: - $N \subseteq \mathcal{F}$ die Menge der potentiellen Restklassenrepräsentanten von $\mathcal{H}$ in $\mathcal{F}$
- $B \subseteq \mathcal{F}$ die Testmenge für mögliche Restklassenrepräsentanten von $\mathcal{H}$ in $\mathcal{F}$
- $H \subseteq K[\mathcal{F}]$ wird zum Vergrößern der Erzeugendenmenge der Untergruppe genutzt um eine Erzeugendenmenge von $\mathcal{H}$ zu erhalten
- $G \subseteq K[\mathcal{F}]$ die monomiale Präfix-Gröbner-Basis, die benutzt wird um zu entscheiden, ob die Kandidaten aus B Restklassenrepräsentanten sind oder nicht.

Ausgabe: Zwei Möglichkeiten:
1. $R = \varnothing$: Dann endet der Prozedur mit Ausgabe der monomialen Präfix-Gröbner-Basis G. Diese ermöglicht das Untergruppenproblem für U in $\mathcal{F}$ zu lösen und Schreier-Restklassen-Repräsentanten aufzuzählen.
2. $R \neq \varnothing$: Der Prozedur zählt alle Restklassenrepräsentanten von der von $U \cup N(R)$ in $\mathcal{F}$ erzeugten Untergruppe auf. Terminiert er, so liefert er die Menge aller Restklassenrepräsentanten von $\mathcal{H}$ in $\mathcal{F}$ und die Multiplikationstafel für diese mit den Elementen in $\overline{\Sigma}$.

Prozedur: $R = \varnothing$?
JA$\longrightarrow$ Die Präfix-Gröbner-Basis von F_U wird berechnet (vgl. 1.Output)
NEIN$\longrightarrow$ Beginne Restklassenaufzählung mit $N = \{\lambda\}$, $B = \{a \mid a \in \overline{\Sigma}\}$. Die Menge G enthält die monomiale Präfix-Gröbner-Basis, mit der man das Untergruppenproblem für die von $U \cup R$ erzeugte Untergruppe lösen kann.
Solange $B \neq \varnothing$ führe folgende Schritte aus:
- Entferne τ aus B, wobei $\tau \in B$ das kleinste Element bzgl. der genutzten Ordnung ist. Falls τ nicht präfix-reduzierbar bzgl. G ist, ergänze τ in N und füge alle Randelemente τa in B ein ($a \in \overline{\Sigma}\backslash\{(l(\tau))^{-1}\}, l(\tau)^{-1}$ bezeichnet das Inverse des letzten Buchstabens von τ).
- Berechne die Hilfsmenge $H = \{\tau * (r-1) \mid r \in R\}$.
- Berechne die monomiale Präfix-Gröbner-Basis von $G \cup H$. Nun ist das Untergruppenproblem für die von $U \cup R \cup \{\tau \circ r \circ \tau^{-1} \mid r \in R\}$ erzeugte Untergruppe lösbar. Dieser Schritt stellt die Annäherung an die von $U \cup N(R)$ erzeugte Untergruppe dar.
- Entferne alle bzgl. G präfix-reduzierbaren Wörter aus N.
Die Prozedur endet, sobald $B = \varnothing$.

Prozedur: Erweiterte Todd-Coxeter-Simulation
Gegeben: $F_r = \{r-1 \mid r \in R\}$, die Menge binomialer Kodierungen der Relatoren, und $F_U = \{u-1 \mid u \in U\}$, die Menge binomialer Kodierungen der Untergruppenerzeugenden.
1. Setze für $N := \varnothing$.
2. Falls $R = \varnothing$, berechne G als Präfix-Gröbner-Basis von F_U.
   Sonst setze $N := \{\lambda\}$
   B:={a| $a \in \overline{\Sigma}$}
   $G := Präfix - Gröbner - Basis(F_R \cup F_U)$
3. Solange $B \neq \varnothing$ führe Schritte 4 und 5 aus, sonst gib G und N aus.
   4. Wähle $\tau := min_>(B)$, und entferne τ aus B.
   5. Falls τ nicht präfix-reduzierbar bzgl. G, so setze
      $N := N \cup \{\tau\}$
      $B := B \cup \{\tau a \mid a \in \overline{\Sigma}\backslash\{l(\tau)^{-1}\}\}$
      $H := \{\tau * (r-1) \mid r-1 \in F_R\}$
      $G := Präfix - Gröbner - Basis(G \cup H)$
      $S := \{w \in N \mid w\, ist\, präfix - reduzierbar\, mit\, G\}$
      $N := N\backslash\{S\}$

Beispiel: Wir rechnen nochmal dasselbe Beispiel wie bei der Todd-Coxeter-Prozedur: $\Sigma = \{a,b\}, R = \{aaa, abab, bbb\}, U = \{a\}$. Wir nutzen wie vorher die lexikographische Ordnung mit $a < b < a^{-1} < b^{-1}$.
$F_R = \{aaa-1, abab-1, bbb-1\}, F_U = \{a-1\}$.

Wir starten die Prozedur:

I

1 $N := \varnothing$

2 $R \neq \varnothing, N := \{\lambda\}, B := \{b^{-1}, a^{-1}, b, a\}$
$G_{\mathrm{I}} = PGB(F_R \cup F_U) =$
$\{a-1, a^{-1}-1, b^2-b^{-1}, b^{-2}-b, b^{-1}a^{-1}-b, ba-b^{-1}\}$

3 $B \neq \varnothing$

4 $\tau = a$ $B = \{b^{-1}, a^{-1}, b\}$

5 τ ist reduzierbar mit $a-1$

II

4 $\tau = b$ $B = \{b^{-1}, a^{-1}\}$

5 τ ist nicht reduzierbar: $N := \{\lambda, b\}, B := \{b^{-1}, a^{-1}, ba^{-1}, b^2, ba\}$
$H_{\mathrm{II}} = \{baaa-b, babab-b, bbbb-b\}$
$G_{\mathrm{II}} = PGB(G_{\mathrm{I}} \cup H_{\mathrm{II}})$
$= \{b^2-b^{-1}, b^{-2}-b, a-1, a^{-1}-1, b^{-1}a^{-1}-b, ba-b^{-1}, b^{-1}a-ba^{-1}, ba^{-2}-b^{-1}\}$
$S = \varnothing, N$ bleibt

III

4 $\tau = a^{-1}$ $B = \{ba^{-1}, b^2, ba, b^1\}$

5 a^{-1} ist reduzierbar mit $a^{-1}-1$

IV

4 $\tau = b^{-1}$ $B = \{ba^{-1}, b^2, ba\}$

5 b^{-1} ist nicht reduzierbar: $N := \{\lambda, b, b^{-1}\}$
$B := \{ba^{-1}, b^2, ba, b^{-2}, b^{-1}a^{-1}, b^{-1}a\}$
$H_{\mathrm{IV}} = \{b^{-1}aaa-b^{-1}, b^{-1}abab-b^{-1}, bb-b^{-1}\}$
$G_{\mathrm{IV}} = PGB(G_{\mathrm{II}} \cup H_{\mathrm{IV}})$
$= \{b^2-b^{-1}, b^{-2}-b, a-1, a^{-1}-1, b^{-1}a^{-1}-b, ba-b^{-1}, b^{-1}a-ba^{-1}, ba^{-2}-b^{-1}, b^{-1}a-ba^{-1}, ba^{-1}b-ba^{-1}, ba^{-1}b^{-1}-ba^{-1}\}$
$S = \varnothing, N$ bleibt

V

4 $\tau = b^{-1}a$ $B = \{ba^{-1}, b^2, ba, b^{-2}, b^{-1}a^{-1}\}$

5 $b^{-1}a$ ist reduzierbar mit $b^{-1}a-ba^{-1}$

VI

4 $\tau = b^{-1}a^{-1}$ $B = \{ba^{-1}, b^2, ba, b^{-2}\}$

5 $b^{-1}a^{-1}$ ist reduzierbar mit $b^{-1}a^{-1}-b$

VII

4 $\tau = b^{-2}$ $B = \{ba^{-1}, b^2, ba\}$

5 b^{-2} ist reduzierbar mit $b^{-2}-b$

VIII

4 $\tau = ba$ $B = \{ba^{-1}, b^2\}$

5 ba ist reduzierbar mit $ba-b^{-1}$

IX

4 $\tau = b^2$ $B = \{ba^{-1}\}$

5 b^2 ist reduzierbar mit b^2-b^{-1}

X

4 $\tau = ba^{-1}$ $B = \varnothing$

5 ba^{-1} ist nicht reduzierbar: $N := \{\lambda, b, b^{-1}, ba^{-1}\}$
$B := \{ba^{-2}, ba^{-1}b, ba^{-1}b^{-1}\}$
$H_{\mathrm{X}} = \{ba^2 - ba^{-1}, b^2ab - ba^{-1}, ba^{-1}b^3 - ba^{-1}\}$
$G_{\mathrm{X}} = PGB(G_{\mathrm{IV}} \cup H_{\mathrm{X}})$
$= \{b^2 - b^{-1}, b^{-2} - b, a - 1, a^{-1} - 1, b^{-1}a^{-1} - b, ba - b^{-1}, b^{-1}a - ba^{-1}, ba^{-2} - b^{-1}, b^{-1}a - ba^{-1}, ba^{-1}b - ba^{-1}, ba^{-1}b^{-1} - ba^{-1}, b^{-1}a - ba^{-1}, ba^{-1}b - ba^{-1}, ba^{-1}b^{-1} - ba^{-1}\}$
$S = \varnothing, N$ bleibt

XI 3 $B = \varnothing$, die Prozedur endet.
Ausgabe: $N := \{\lambda, b, b^{-1}, ba^{-1}\}$
$G := \{b^2 - b^{-1}, b^{-2} - b, a - 1, a^{-1} - 1, b^{-1}a^{-1} - b, ba - b^{-1}, b^{-1}a - ba^{-1}, ba^{-2} - b^{-1}, b^{-1}a - ba^{-1}, ba^{-1}b - ba^{-1}, ba^{-1}b^{-1} - ba^{-1}, b^{-1}a - ba^{-1}, ba^{-1}b - ba^{-1}, ba^{-1}b^{-1} - ba^{-1}\}$

Berechnungen der Präfix-Gröbner-Basen:

I. Berechne *can* und *acan* der Binome aus F_R und F_U:

$a^3 - 1 \xrightarrow{a^{-1}} a^2 - a^{-1} \xrightarrow{a^{-1}} a - a^{-2}$

$abab - 1 \xrightarrow{b^{-1}} aba - b^{-1} \xrightarrow{a^{-1}} ab - b^{-1}a^{-1}$

$b^3 - 1 \xrightarrow{b^{-1}} b^2 - b^{-1} \xrightarrow{b^{-1}} b - b^{-2}$

$a - 1 \xrightarrow{a^{-1}} 1 - a^{-1}$

Zunächst ist also $G_{\mathrm{I}} = \{a^2 - a^{-1}, a^{-2} - a, aba - b^{-1}, b^{-1}a^{-1} - ab, b^2 - b^{-1}, b^{-2} - b, a - 1, a^{-1} - 1\}$. Durch Reduzieren innerhalb von G_{I} erhält man:

$a^2 - a^{-1} \xrightarrow{(a-1)*a} a - a^{-1} \xrightarrow{(a^{-1}-1)} 1 - a \xrightarrow{a-1} 0$

$a^{-2} - a \xrightarrow{(a^{-1}-1)*a^{-1}} a^{-1} - a \xrightarrow{(a^{-1}-1)} 1 - a \xrightarrow{a-1} 0$

$b^{-1}a^{-1} - ab \xrightarrow{(a-1)*b} b^{-1}a^{-1} - b$ (Reduzieren nur im zweiten Monom möglich)

$aba - b^{-1} \xrightarrow{(a-1)*ba} ba - b^{-1}$

Bei den letzten beiden nicht auf 0 reduzierbaren Binomen muß man nun erneut *can* und *acan* bilden, erhält aber nur jeweils das andere Binom, so daß beide in G_I eingefügt werden müssen. Die zu 0 reduzierbaren Binome werden gestrichen. Dann folgt: $G_{\mathrm{I}} = \{b^2 - b^{-1}, b^{-2} - b, a - 1, a^{-1} - 1, b^{-1}a^{-1} - b, ba - b^{-1}\}$

II. $G_{\mathrm{II}} = PGB(G_{\mathrm{I}} \cup H_{\mathrm{II}})$. Die schon betrachteten Binome bleiben erhalten und werden nur beim weiteren Reduzieren nochmal betrachtet. Berechne zunächst wieder *can* und *acan* von H_{II}:

$ba^3 - b \xrightarrow{a^{-1}} ba^2 - ba^{-1} \xrightarrow{a^{-1}} ba - ba^{-2}$

$babab - b \xrightarrow{b^{-1}} baba - 1 \xrightarrow{a^{-1}} bab - a^{-1} \xrightarrow{b^{-1}} ba - a^{-1}b^{-1}$

$b^4 - b \xrightarrow{b^{-1}} b^3 - 1 \xrightarrow{b^{-1}} b^2 - b^{-1} \xrightarrow{b^{-1}} b - b^{-2}$

Beim Reduzieren ergibt sich folgendes: Die Binome $b^2 - b^{-1}$ und $b^{-2} - b$ sind schon in G_{I} enthalten, brauchen also nicht berücksichtigt werden. Zwei weitere Binome reduzieren auf 0 und können somit gestrichen werden, und die ersten beiden können in reduzierter Form in G_{II} verbleiben:

$bab - a^{-1} \xrightarrow{(ba-b^{-1})*b} 1 - a^{-1} \xrightarrow{a^{-1}-1} 0$

$a^{-1}b^{-1} - ba \xrightarrow{(a^{-1}-1)*b} b^{-1} - ba \xrightarrow{ba-b^{-1}} 0$

$ba^2 - ba^{-1} \xrightarrow{(ba-b^{-1})*a} b^{-1}a - ba^{-1}$

$ba^{-2} - ba \xrightarrow{ba-b^{-1}} ba^{-2} - b^{-1}$ (Reduzieren ist nur im zweiten Monom möglich)

$G_{\mathrm{II}} = \{b^2 - b^{-1}, b^{-2} - b, a - 1, a^{-1} - 1, b^{-1}a^{-1} - b, ba - b^{-1}, b^{-1}a - ba^{-1}, ba^{-2} - b^{-1}\}$

X. $G_{\mathrm{X}} = PGB(G_{\mathrm{II}} \cup H_{\mathrm{X}})$. Berechne zunächst wieder *can* und *acan* von H_{X}:
$ba^2 - ba^{-1} \xrightarrow{a^{-1}} ba - ba^{-2}$
$b^2ab - ba^{-1} \xrightarrow{b^{-1}} b^2a - ba^{-1}b^{-1}$
$ba^{-1}b^3 - ba^{-1} \xrightarrow{b^{-1}} ba^{-1}b^2 - ba^{-1}b^{-1} \xrightarrow{b^{-1}} ba^{-1}b - ba^{-1}b^{-2}$
Beim weiteren Reduzieren ergeben sich noch drei Binome für G_{X}, die übrigen reduzieren auf 0.
$ba^{-2} - ba \xrightarrow{ba^{-2}-b^{-1}} b^{-1} - ba \to 0$
$ba^2 - ba^{-1} \xrightarrow{(ba-b^{-1})*a} b^{-1}a - ba^{-1}$
$b^2ab - ba^{-1} \xrightarrow{(b^2-b^{-1})*ab} b^{-1}ab - ba^{-1} \xrightarrow{(b^{-1}a-ba^{-1})*b} ba^{-1}b - ba^{-1}$
$ba^{-1}b^{-1} - b^2a \xrightarrow{(b^2-b^{-1})*a} ba^{-1}b^{-1} - b^{-1}a \xrightarrow{b^{-1}a-ba^{-1}} ba^{-1}b^{-1} - ba^{-1}$ (Reduktion im ersten Monom ist nicht möglich)
$ba^{-1}b^{-2} - ba^{-1}b \xrightarrow{(ba^{-1}b^{-1}-ba^{-1})*b^{-1}} ba^{-1}b^{-1} - ba^{-1}b \xrightarrow{ba^{-1}b^{-1}-ba^{-1}} ba^{-1} - ba^{-1}b \xrightarrow{ba^{-1}b-ba^{-1}} 0$
$ba^{-1}b^2 - ba^{-1}b^{-1} \xrightarrow{(ba^{-1}b.ba^{-1})*b} ba^{-1}b - ba^{-1}b^{-1} \xrightarrow{(ba^{-1}b^{-1}-ba^{-1}} ba^{-1}b - ba^{-1} \to 0$
Es folgt: $G_{\mathrm{X}} = \{b^2 - b^{-1}, b^{-2} - b, a - 1, a^{-1} - 1, b^{-1}a^{-1} - b, ba - b^{-1}, b^{-1}a - ba^{-1}, ba^{-2} - b^{-1}, b^{-1}a - ba^{-1}, ba^{-1}b - ba^{-1}, ba^{-1}b^{-1} - ba^{-1}, b^{-1}a - ba^{-1}, ba^{-1}b - ba^{-1}, ba^{-1}b^{-1} - ba^{-1}\}$

Vergleicht man jetzt die erhaltene Ausgabe mit der Ausgabe von Todd-Coxeter, so stellt man fest, dass die Gröbner-Basis Relationen dem nicht-trivialen Teil der Multiplikationstafel entsprechen. Umgeschrieben lauten sie: $b \circ b = b^{-1}, b^{-1} \circ b^{-1} = b, \lambda \circ a = \lambda, \lambda \circ a^{-1} = 1, b^{-1} \circ a^{-1} = b, b \circ a = b^{-1}, b^{-1} \circ a = b \circ a^{-1}, b \circ a^{-1} \circ a^{-1} = b^{-1}, b^{-1} \circ a = b \circ a^{-1}, b \circ a^{-1} \circ b = b \circ a^{-1}, b \circ a^{-1} \circ b^{-1} = b \circ a^{-1}, b^{-1} \circ a = b \circ a^{-1}, b \circ a^{-1} \circ b = b \circ a^{-1}, b \circ a^{-1} \circ b^{-1} = b \circ a^{-1}$. Die trivialen Relationen müssen noch ergänzt werden, um die Multiplikationstafel zu vervollständigen.

6 Eigenschaften:

<u>Satz:</u> Für $R \neq \varnothing$ endet die Prozedur nur, falls $B = \varnothing$ erreicht wird. Dann ist $N = \varnothing$ oder N ist ein vollständiges präfix-abgeschlossenen Restklassenrepräsentantensystem, und N enthält alle Elemente von $\mathcal{F}$, die nicht bzgl. der letzten Präfix-Gröbner-Basis G präfix-reduzierbar sind.
Beweis: Für $R = \varnothing \Rightarrow N = \varnothing$, sonst $N \neq \varnothing$. N ist immer präfix-abgeschlossen, da B immer alle Randelemente zu $\tau \in N$ enthält und S diese Eigenschaft nicht zerstört. Noch zu zeigen ist also, dass N alle Repräsentanten enthält.
Nach der Schleife erhalten wir N_n, B_n und G_n. Für diese und ein $w \in \mathcal{F}$, das nicht mit G_n präfix-reduzierbar ist (falls w präfix-reduzierbar, so ist w schon in einer Restklasse enthalten), gilt eine der folgenden Bedingungen:
1. $w \in N_n$
2. $w \in B_n : w \equiv w_1 a$, wobei $w_1 \in N_n,\ a \in \overline{\Sigma}$
3. $w \equiv w_1 a w_2$, wobei $w_1 a \in B_n$ ein Randelement, und $w_2 \in \mathcal{F}$

Für die erste Eingabe ist dies erfüllt. Für einen beliebigen späteren Schritt gelte die Aussage für $n-1$: Nehme $\tau \in B_{n-1}$:
1.Fall: τ ist präfix-reduzierbar mit $G_{n-1} \rightsquigarrow N_n = N_{n-1}, B_n = B_{n-1} \setminus \{\tau\}, G_n = G_{n-1}$. Dann gilt die Behauptung, da τ nicht Präfix eines bzgl. G_n nicht präfix-

reduzierbaren Elementes ist.
2.Fall: τ ist nicht präfix-reduzierbar mit $G_{n-1} \rightsquigarrow N_n = N_{n-1} \cup \{\tau\} \setminus S_n, B_n = (B_{n-1} \setminus \{\tau\}) \cup \{\tau \circ a \mid a \in \overline{\Sigma} \setminus \{l(\tau)^{-1}\}\}, G_n = Präfix-Gröbner-Basis(G_{n-1} \cup H)$.
Für ein nicht mit G_n präfix-reduzierbares w gilt nun: w ist ebenfalls mit G_{n-1} nicht präfix-reduzierbar, da nach Konstruktion die Menge der mit G_{n-1} präfix-reduzierbaren Elemente eine Teilmenge der mit G_n präfix-reduzierbaren Elemente ist. Es gilt also einer der Fälle:
1. $w \in N_{n-1}$ und w nicht präfix-reduzierbar mit G_n. Letzteres zeigt, dass $w \notin S_n$ also $w \in N_n$.
2. $w \in B_{n-1}$ mit $w \equiv w_1 a$ wobei $a \in \overline{\Sigma}, w_1 \in N_{n-1}$. Also $w_1 \notin S_n$, woraus folgt $w_1 \in N_n$, also $w \in B_n$.
3. $w \equiv w_1 a w_2$, wobei $w_1 a \in B_{n-1}(w_1 \in N_{n-1}), w_2 \in \mathcal{F}$. Also wiederum $w_1 \notin S_n$, also $w_1 \in N_n$ und $w_1 a \in B_n$.

□

Satz: Falls die Prozedur endet, ist $\mathcal{H} := \langle U \cup N(R) \rangle$ endlich erzeugt.
Beweis: Für $R = \varnothing$ folgt $\mathcal{H} = \langle U \rangle$.
Für $R \neq \varnothing$ gilt bei Terminierung: G ist Präfix-Gröbner-Basis, die das Untergruppenzugehörigkeitsproblem für $\mathcal{H}' = \langle U \cup \{x \circ r \circ x^{-1} \mid x \in N, r \in R\} \rangle$ in $\mathcal{F}$ löst.
Zu zeigen ist nun: $\mathcal{H}' = \mathcal{H} = \langle U \cup N(R) \rangle$ in $\mathcal{F}$, also $\forall w \in \mathcal{F}, r \in R : w \circ r \circ w^{-1} \in \mathcal{H}'$.
Annahme: $\mathcal{H}' \neq \mathcal{H} \Rightarrow$ Es existiert ein bzgl. ">" minimales $w \in \mathcal{F}$ so, dass für ein $r \in R : w \circ r \circ w^{-1} \notin \mathcal{H}'$
1.Fall: w irreduzibel $\Rightarrow w \in N$, da die anderen Fälle für $B = \varnothing$ nicht mehr auftreten $\Rightarrow w \circ r \circ w^{-1} \in \mathcal{H}'$ Widerspruch
2.Fall: w reduzibel, also $w \equiv w_1 w_2 : w_1 = LT(w_1 - v)$ wobei $w_1 - v$ Polynom in G. Es gilt $w_1 v^{-1} \in \mathcal{H}'$, (da $w_1 v^{-1}$ mit $(w_1 - v) \circ v^{-1}$ reduziert werden kann). Ausserdem $w > v \circ w_2$. Schreibe $w \circ r \circ w^{-1} = w_1 v^{-1} \circ (v \circ w_2) \circ r \circ (v \circ w_2)^{-1} \circ (w_1 v^{-1})^{-1}$. Da w minimal war, gilt $(v \circ w_2) \circ r \circ (v \circ w_2)^{-1} \in \mathcal{H}' \Rightarrow w \circ r \circ w^{-1} \in \mathcal{H}'$, da $w_1 v^{-1}, (w_1 v^{-1})^{-1} \in \mathcal{H}'$. Widerspruch.

□

Folgerung: Bei Terminierung gilt:
1. $\mathcal{H} = \langle U \cup N(R) \rangle$ in $\mathcal{F}$ ist endlich erzeugt durch $\{uv^{-1} \mid u - v \in G\}$ (Beweis siehe Doktorarbeit B.Reinert).
2. Desweiteren ist das Untergruppenproblem für $\mathcal{H}$ durch Präfix-Reduktion mit G lösbar.
3. G enthält die jeweiligen Gleichungen, die auch durch Todd-Coxeter erzeugt werden. Diese kodieren die Multiplikationstafel der Restklassenerzeugenden wie folgt: Für alle $xa - y \in G, x, y \in \mathcal{F}, a \in \overline{\Sigma}$ sind x, y Restklassenrepräsentanten und es gilt $x \circ a = y$.

In Abschnitt 3 haben wir gesehen, dass die Todd-Coxeter Prozedur genau dann endet, wenn $\mathcal{H}$ endlichen Index hat, und dies ist auch für die Erweiterte-Todd-Coxeter-Simulation der Fall:
Satz: Die Prozedur Erweiterte-Todd-Coxeter-Simulation endet genau dann, wenn die von $U \cup N(R)$ erzeugte Untergruppe endlichen Index in $\mathcal{F}$ hat.

Beweis: $\mathcal{H} = \langle U \cup N(R) \rangle$ habe in $\mathcal{F}$ endlichen Index.
Für $R = \varnothing$ ist nichts zu zeigen. Die Restklassenrepräsentantenmenge erhält man zum Beispiel durch Aufzählen der Elemente, die nicht bzgl. der letzten erhaltenen Präfix-Gröbner-Basis des rechten Ideals von F_U präfix-reduzierbar sind.
$R \neq \varnothing$ und es gilt $\mathcal{F}$ endlich erzeugt. Es folgt $\mathcal{H}$ endlich erzeugt. Also hat $\mathcal{H}$ ein endliches präfix-abgeschlossenes Rechtsnebenklassenrepräsentantensystem S, und für $s \in S, a \in \overline{\Sigma}$ und alle $s \circ a$ existiert nur ein $s_a \in S$ so, dass $s \circ a \in \mathcal{H}s_a$. Da für ein $h \in \mathcal{H}$ $s \circ a = h \circ s_a$, gilt $s \circ a \circ s_a^{-1} = h \in \mathcal{H}$. Die Menge $\{s \circ a \circ s_a^{-1} \mid s \in S, a \in \overline{\Sigma}\}$ erzeugt $\mathcal{H}$. Diese Menge ist enthalten im Erzeugnis der Menge $\{s \circ a \circ r \circ s_a^{-1}, s \circ r \circ s^{-1} \mid s \in S, a \in \overline{\Sigma}, r \in R\}$, da $s \circ a \circ s_a^{-1} = (s \circ a \circ r \circ s_a^{-1}) \circ (s_a \circ r^{-1} \circ s_a^{-1})$. Also ist auch die Menge $\{s \circ a \circ r \circ s_a^{-1}, s \circ r \circ s^{-1} \mid s \in S, a \in \overline{\Sigma}, r \in R\}$ eine erzeugende Menge für $\mathcal{H}$.
Daher endet die Prozedur spätestens, nachdem sie alle Kandidaten $s \circ a, s \in S$ kontrolliert hat.

$\square$

<u>Vergleich:</u> In der Gruppentheorie ist die Todd-Coxeter-Prozedur eigenständig. Auf Gröbner-Basis-Techniken umgeschrieben stellt man jedoch fest, dass sie nur einen Spezialfall der Gröbner-Basis-Berechnung darstellt.