Quotient Tests and Gröbner Bases

Martin Kreuzer
FB Mathematik
Univ. Dortmund
Dortmund, Germany

Alexei Myasnikov
Dept. of Mathematics
McGill University
Montreal, Canada

Gerhard Rosenberger
FB Mathematik
Univ. Dortmund
Dortmund, Germany

Alexander Ushakov
Graduate Center
CUNY
New York, USA

March 15, 2005

Given a finitely presented group $G = \langle X; R\rangle$, the word problem asks to decide effectively whether a given word in the free group $w \in F(X)$ represents the identity element in G or not. Another important computational problem is to check effectively whether G is finite or not. For the "No" parts of these problems, we can use quotient tests. For instance, for the "No" part of the word problem, we can devise a procedure which proves $w \neq_G 1$ or returns `"Dont't know"` if we have an effectively computable group homomorphism $\varphi : G \longrightarrow H$ and if the "No" part of the word problem is decidable in H.

To find a suitable group homomorphism $\varphi : G \longrightarrow H$, we use universal linear representations of G. Special cases of such representations have been used in [12] and [2] for other purposes. Here the universal linear representation $\varrho : G \longrightarrow SL(n, Q_R)$ is constructed as follows. We map each generator x_k of G to a matrix of indeterminates $(a_{i,j}^{(k)})$. In the polynomial ring P having these indeterminates, we form the ideal I_R generated by the entries of the images of the relators in R and by the polynomials $\det(a_{i,j}^{(k)}) - 1$. Letting $Q_R = R/I_R$, we obtain a well-defined linear representation $\varrho : G \longrightarrow SL(n, Q_R)$ which maps x_k to the residue class of $(a_{i,j}^{(k)})$.

At this point Gröbner bases come into play: if we succeed in computing a Gröbner basis of the ideal I_R, we can check effectively whether the matrix of polynolmials $\varrho(w)$ defines the identitiy element in $\varrho(G)$. Moreover, we have several methods available for showig that $\varrho(G)$, and hence G, is an infinite group. For example, Algorithm 6.2 determines the minimal polynomial of a matrix in a matrix ring over an affine algebra. If we find a word w such that the minimal polynomial of $\varrho(w)$ is zero or does not divide a polynomial $z^m - 1$, the element $\varrho(w)$ has infinite order.

In the last two sections we apply these new techniques to several examples. First we study two problems from the Kourovka Notebook [14]. We show the the universal linear representations of size 2×2 of the groups $G_i = \langle a, b; a^i = 1, ab = b^3a^3 \rangle$ are commutative and finite for $i = 5, 7, 9, 11$. This makes is plausible that this could be true for the groups themselves, but is it known that G_9 is infinite. Next we prove that $a \neq 1$ in the groups $H_i = \langle a, b; a^i = 1, ababa = b^2ab^{-1}ab \rangle$ for $i = 5, 10, 15, 20$, and that $\varrho(a) = 1$ in the universal linear representations of size 2×2 of these groups for the other groups H_i with $i \leq 20$. Our third collection of examples are some groups of deficiency zero mentioned in [4]. For these groups, we can show that their universal linear 2×2 representations are all isomorphic to $(\mathbb{Z}/(3))^3$. In fact, the ideals I_R turn out to be identical. However, the Gröbner bases of the ideals corresponding to the universal linear representations of size 3×3 are too difficult to compute at present.

In the last section we apply our methods to the classification of finite generalized triangle resp. tetrahedron groups in [6] and [10], resp. in [20]. For generalized triangle groups, this classification is complete. We show some methods for checking individual cases. For generalized tetrahedron groups, there are five groups for which it is not known whether they are finite or not. Unfortunately, as our Proposition 8.3 and the companying computer calculations show, we cannot expect to prove infinitude for these groups using their universal linear representation of size 2×2, and for size 3×3 we were only able to compute truncated Gröbner bases and deduce some partial results.

It is clear that there is ample room for optimizing the Gröbner basis computations necessary for our algorithms. In view of the ease with which we were able to get new results for some difficult problems, we are optimistic that the Gröbner bases methods we discuss will prove to be useful tools in computational group theory.

Contents

1 The Word Problem in Groups

In this section we briefly discuss the word problem in groups. For a more detailed discussion of decision problems for groups we refer the reader to the surveys [1], [15], and [16].

Let X be a set. Denote by $X^{-1} = \{x^{-1} \mid x \in X\}$ the set of *formal inverses* of elements of X. The map $x \mapsto x^{-1} (x \in X)$ naturally extends to an involution on the set $X^{\pm 1} = X \cup X^{-1}$, where we define $(x^{-1})^{-1} = x$. Denote by $(X^{\pm 1})^*$ the free monoid with basis $X^{\pm 1}$ viewed as the set of all words (including the empty word ε) in the alphabet $X^{\pm 1}$ with concatenation as multiplication. A word $w \in (X^{\pm 1})^*$ is called *reduced* if it does not have subwords of the type yy^{-1} for $y \in X^{\pm 1}$. It is easy to see that the rewriting system

$$yy^{-1} \to \varepsilon, \quad (y \in X^{\pm 1})$$

is complete, so for every word $w \in (X^{\pm 1})^*$ there exists a unique reduced word $\bar{w}$ which can be obtained from w by cancellations $yy^{-1} \to \varepsilon$.

Let $F(X)$ be the set of all *reduced* words in $X^{\pm 1}$ with multiplication $\cdot$ given by concatenation and subsequent reduction. It is known that $F(X)$ is a free group with basis X.

Let $R \subseteq F(X)$ and let $gp_F(R)$ be the normal closure of R in $F(X)$. Then we write

$$G = \langle X; R \rangle \tag{1}$$

for the group $G \cong F(X)/gp_F(R)$. In this setting the set X is called a set of *generators* of G, the set R is called a set of *relators* of G, and the pair $\mathcal{P} = \langle X; R \rangle$ is called a *presentation* of G. A presentation $\mathcal{P} = \langle X; R \rangle$ is *finite* if the sets X and R are both finite. A group G is called *finitely presented* if G has a finite presentation $G = \langle X; R \rangle$. By $\eta : F(X) \to G$ we denote the canonical homomorphism from $F(X)$ onto its quotient $G = F(X)/gp_F(R)$.

A finite presentation $\langle X; R \rangle$ has *decidable Word Problem* if the set $gp_F(R)$ is recursive. Equivalently, the Word Problem (WP) is decidable in G (with respect to the presentation $G = \langle X; R \rangle$) if for every word $w \in F(X)$ one can effectively decide whether $\eta(w) = 1$ in G or not. Sometimes instead of $\eta(w) = 1$ in G we write $w =_G 1$, or simply $w = 1$. It is not hard to see that if WP is decidable in G with respect to one finite presentation then WP is decidable in G with respect to every finite presentation of G. Therefore, we often refer to G as a group with decidable word problem without mentioning any particular presentation.

It is convenient to partition the word problem over a group $G = \langle X; R \rangle$ into two parts: the "Yes" part and the "No" part:

$$\mathrm{WP}_{Yes} = \{w \in F(X) \mid w =_G 1\}$$
$$\mathrm{WP}_{No} = \{w \in F(X) \mid w \neq_G 1\}$$

We consider *partial decision algorithms* for each part separately. Here a procedure A is said to be a *partial decision algorithm* for the "Yes" (resp. "No") part in G if for every input word $w \in F(X)$ the procedure A halts and returns `"Yes"` (resp. `"No"`) only if $w \in \mathrm{WP}_{Yes}$ (resp. $w \in \mathrm{WP}_{No}$), otherwise A either does not stop, or A stops and returns `"Don't know"`.

2 Quotient Tests

In this section we discuss *quotient tests*. They yield partial decision algorithms for the "No" part of the word problem. Quotient tests provide one

of the key methods for designing decision algorithms for groups. They are based on the following simple idea:

Let $\varphi : G \to H$ be a group homomorphism from G to a group H. Then the following implication holds for every element $u \in F(X)$:

$$\varphi(u) \neq_H 1 \implies u \neq_G 1.$$

Now suppose that the group H is provided with a generating set Y such that WP is decidable in H with respect to Y. Suppose also that the homomorphism φ is given by the images of elements $x \in X$ which are described by some words $u_x \in F(Y)$, i.e. for which we have $u_x =_H \varphi(x)$. In this case one can design a partial decision algorithm A for the "No" part of WP in G as follows:

Given a word $w \in F(X)$, the procedure A performs the substitution $\sigma : x \to u_x$ in w and applies the decision procedure B for WP in H to the resulting word $\sigma(w)$. If B stops on $\sigma(w)$ and says "No", then A stops and says "No", in all other cases A does not stop. The procedure A is called the *quotient test* for WP in G with respect to the homomorphism $\varphi : G \to H$.

The computational complexity of general quotient tests in groups has been studied recently in [7] and [8].

3 Linear Representations of Groups

A homomorphism $\varrho : G \to GL(n, K)$ from a group G to the general linear group $GL(n, K)$ of invertible matrices of size $n \times n$ over a commutative unitary ring K is called a *linear representation* of G. Usually, the ring K is assumed to be a field, but we do not not need this assumption here. Similarly, one can introduce linear representations of G in the special linear group $SL(n, K)$. For purely technical reasons we usually prefer linear representations in $SL(n, K)$, even though everything goes through for representations in $GL(n, K)$, or even more generally, in any linear algebraic group.

Let $G = \langle X; R \rangle$ be a finite presentation of a group G, where $X = \{x_1, \ldots, x_s\}$ and $R = \{r_1, \ldots, r_t\} \subseteq F(X)$. Every linear representation

$$\varrho : G \to SL(n, K)$$

is completely determined by the set $\varrho(X) = \{\varrho(x_1), \ldots, \varrho(x_s)\}$ of images of the elements of X in $SL(n, K)$. Letting $\varrho(x_k) = (a_{i,j}^{(k)}) \in SL(n, K)$, we have

$$x_k \overset{\varrho}{\longmapsto} \begin{pmatrix} a_{(1,1)}^{(k)} & \ldots & a_{(1,n)}^{(k)} \\ \\ a_{(n,1)}^{(k)} & \ldots & a_{(n,n)}^{(k)} \end{pmatrix} \tag{2}$$

Since $\varrho(r) = 1$ in $SL(n, K)$ for every $r \in R$, the elements $a_{i,j}^{(k)} \in K$ form a solution of the following system $S_R = 0$ of polynomial equations with integer coefficients:

$$\begin{array}{l} \det(\varrho(x)) - 1 = 0 \quad (x \in X); \\ (\varrho(r))_{i,j} - \delta_{i,j} = 0 \quad (r \in R, \quad i, j = 1, \ldots, n) \end{array} \tag{3}$$

where $(\varrho(r))_{i,j}$ is the (i, j) entry of the matrix $\varrho(r)$, viewed as a polynomial in the entries of the matrices $\varrho(x)$ $(x \in X)$. Here we let $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise.

Clearly, every solution $a = (a_{i,j}) \in K^{sn^2}$ of the system $S_R = 0$ gives rise to a linear representation $\varrho_a : G \to SL(n, K)$. Hence linear representations of a finitely presented group $G = \langle X; R \rangle$ in $SL(n, K)$ can be viewed as K-rational points of the variety V_R in K^{sn^2} defined by the system $S_R = 0$. This variety is called the *variety of representations* of G. For a detailed discussion of this variety, see [12].

Remark 3.1. *(Optimization of the System $S_R = 0$)*
Computationally, it is more advantageous to consider a slightly modified version of the system $S_R = 0$ defined in (3).

Suppose we have an equation $r = r' \circ r''$ in G. Since ϱ is a homomorphism, it follows that $\varrho(r) = 1$ in $SL(n, K)$ if and only if $\varrho(r')\varrho(r'') = 1$, and this is equivalent to $\varrho(r') = \varrho((r'')^{-1})$. Therefore the system $S_R = 0$ is equivalent to the system obtained from S_R by removing the equations corresponding to $\varrho(r) = 1$ and adding equations corresponding to $\varrho(r') = \varrho((r'')^{-1})$.

Notice that the polynomial equations corresponding to $\varrho(r') = \varrho((r'')^{-1})$ have smaller degree than those coming from $\varrho(r) = 1$. The smallest degrees will be obtained when the relators in R are divided in the middle, i.e. when each $r \in R$ is represented as $r = r' \circ r''$ such that the lengths of the words representing r' and r'' differ at most by one.

Example 3.2. *(The System $S_R = 0$ for a Baumslag Solitar Group)* Consider the group $G = \langle\ x_1, x_2\ ;\ x_1 x_2 x_1^{-1} x_2^{-2}\ \rangle$. Here a linear representation $\mu : G \to SL(2, K)$ is given by

$$x_1 \overset{\varrho}{\longmapsto} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad x_2 \overset{\varrho}{\longmapsto} \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

We divide the only relator of G into halves and get $x_1 x_2 \circ x_1^{-1} x_2^{-2}$. Then we have $\varrho(x_1 x_2) = \varrho(x_2^2 x_1)$ in $SL(2, K)$, and therefore

1. $\det(\varrho(x_1)) = ad - bc = 1$.
2. $\det(\varrho(x_2)) = eh - fg = 1$.
3. $\varrho(x_1 x_2) = \varrho(x_2^2\, x_1)$ which yields the matrix equality

$$\begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} = \begin{pmatrix} ae^2 + afg + acf + cfh & be^2 + bfh + def + dfh \\ age + ahg + cgf + ch^2 & bge + bhg + dgf + dh^2 \end{pmatrix}$$

Thus the system $S_R = 0$ is given by

$$\begin{aligned} S_R = \ & \{ad - bc - 1, \\ & eh - fg - 1, \\ & ae + bg - (ae^2 + afg + acf + cfh), \\ & af + bh - (be^2 + bfh + def + dfh), \\ & ce + dg - (age + ahg + cgf + ch^2), \\ & cf + dh - (bge + bhg + dgf + dh^2)\}. \end{aligned}$$

Notice that had we constructed a system using $\varrho(r) = 1$, the last four polynomials would be of degree five.

4 Universal Linear Representations

In this section we discuss a general method for constructing linear representations of finitely presented groups.

Let G be a group, and let K and L be commutative unitary rings. A ring homomorphism $\varphi : K \to L$ induces a group homomorphism $\varphi' : SL(n, K) \to SL(n, L)$. We say that a linear representation $\varrho : G \to SL(n, K)$ is *universal*

if for every linear representation $\varrho' : G \to SL(n, L)$ there exists a ring homomorphism $\varphi : K \to L$ such that $\varrho' = \varphi' \circ \varrho$, i.e. such that the following diagram is commutative:

$$\begin{array}{ccc} G & \stackrel{\varrho}{\to} & SL(n,K) \\ & \searrow^{\varrho'} & \downarrow^{\varphi'} \\ & & SL(n,L) \end{array}$$

Similarly, one can introduce universal linear representations of G in the general linear groups $GL(n, K)$.

Remark 4.1. More generally, we can define universal linear representations with respect to a given class of rings. For example, let $\mathcal{C}_F$ be the class of all unitary commutative algebras L over a fixed field F. We say that a linear representation $\varrho : G \to SL(n, K)$ is $\mathcal{C}_F$-*universal* if $K \in \mathcal{C}_F$ and for every linear representation $\varrho' : G \to SL(n, L)$ with $L \in \mathcal{C}_F$ there exists a homomorphism of F-algebras $\varphi : K \to L$ such that $\varrho' = \varphi' \circ \varrho$.

In the following we want to determine the universal linear representation of a finitely presented group $G = \langle X; R\rangle$ explicitly. Let $S_R = 0$ be the polynomial system of equations (3) in sn^2 indeterminates which defines the variety of representations of G in $SL(n, K)$ for every ring K. We use

$$T = \{y_{ij}^{(k)} \mid k = 1, \ldots, s, \quad i, j = 1, \ldots, n\}$$

to denote these indeterminates. Furthermore, let I_R be the ideal in $\mathbb{Z}[T]$ generated by the set of polynomials S_R, and let the commutative unitary ring Q_R be defined by

$$Q_R = \mathbb{Z}[T]/I_R.$$

Proposition 4.2. Let $G = \langle X; R\rangle$ be a finitely presented group, and let $Q_R = \mathbb{Z}[T]/I_R$ be constructed as above. Then the group homomorphism $\varrho : G \to SL(n, Q_R)$ defined by

$$x_k \stackrel{\varrho}{\longmapsto} \begin{pmatrix} y_{(1,1)}^{(k)} & \cdots & y_{(1,n)}^{(k)} \\ & & \\ y_{(n,1)}^{(k)} & \cdots & y_{(n,n)}^{(k)} \end{pmatrix} \tag{4}$$

is a universal linear representation of G.

Proof. This follows directly from the construction. □

The group homomorphism $\varrho : G \to SL(n, Q_R)$ is called a *universal linear representation* of G. Similarly, for a fixed field F one can construct a representation

$$\varrho_F : G \to SL(n, Q_{F,R})$$

of G in the special linear group over the ring $Q_{F,R} = F[T]/I_R$. Clearly, the map ϱ_F is a $\mathcal{C}_F$-universal representation of G.

5 Linear Quotient Tests for WP

Quotient tests of the type $\varphi : G \to SL(n, K)$ are called *linear quotient tests*. Obviously, it suffices to consider only quotient tests with respect to universal linear representations. We refer to such tests as *universal linear quotient tests*.

Algorithm 5.1. *(Universal Linear Quotient Test)*
INPUT: A finite presentation $G = \langle X; R\rangle$, a word $w = x_{i_1} \cdots x_{i_\ell} \in F(X)$, and $n \in \mathbb{N}$.
OUTPUT: `"No"` if $\varphi(w) \neq 1$ where $\varphi : G \to SL(n, Q_R)$ is the universal linear representation of G, `"Don't know"` otherwise.
COMPUTATIONS:

1) Compute the set of polynomial equations S_R according to (3).

2) Compute a Gröbner basis for I_R in $\mathbb{Q}[T]$.

3) Compute $\varphi(w) = \varphi(x_{i_1}) \cdots \varphi(x_{i_\ell})$.

4) Let $\varphi(w) = (f_{i,j})_{i,j=1}^n$. Check whether the polynomial $f_{i,j} - \delta_{i,j}$ belongs to the ideal I_R for all $1 \leq i, j \leq n$ by reducing it modulo the Gröbner basis. If all $f_{i,j} - \delta_{i,j}$ belong to the ideal I_R, return `"Don't know"`, otherwise return `"No"`.

Similarly, given a field F, we can construct a $\mathcal{C}_F$-universal linear quotient test.

6 Linear Quotient Tests for Infinitude

A further question which can be studied using Gröbner bases is whether a finitely presented group $G = \langle X; R\rangle$ is finite or infinite. There are several methods available but it is not yet clear how often they apply. The first method uses the following observation.

Remark 6.1. Let $\varphi : G \longrightarrow SL(n, K)$ be a group homomorphism to a special linear group over a unitary commutative ring K. If there exists a word $w \in F(X)$ such that the matrix $W = \varphi(w)$ has infinite order in $SL(n, K)$ then G is infinite.

Again we may obviously restrict our attention to the case $K = Q_R$, i.e. to the universal linear representation. Moreover, if $\varphi(G)$ is infinite then usually almost every element will have infinite order, so that we can try short words first.

In view of this remark we have to compute the minimal polynomial of a matrix in $SL(n, Q_R)$ or $SL(n, Q_{F,R})$. Since this ring is not commutative, the usual computer algebra methods (see e.g. [9], Cor. 3.6.4) do not apply. The following algorithm solves our task using Gröbner basis theory.

Algorithm 6.2. *(Minimal Polynomial of a Matrix)*
INPUT: A matrix $W = (w_{i,j}) \in \mathrm{Mat}(n, K)$ where $K = F[y_1, \ldots, y_m]/I$ is an affine algebra over some field F.
OUTPUT: The minimal polynomial $f \in F[z]$ of W over F, or zero if W is algebraically independent.
COMPUTATIONS:

1) In $F[y_1, \ldots, y_m, z]^n$, form the submodule U generated by the column vectors of $W - z \cdot \mathcal{I}_n$ and by the elements of $I \cdot F[y_1, \ldots, y_m, z]^n$. (Here $\mathcal{I}_n$ denotes the identity matrix of size n.)

2) Using standard Gröbner basis techniques (see e.g. [9], Sect. 3.2), compute the ideal $V = U : \langle e_1, \ldots, e_n\rangle = \bigcap_{i=1}^{n} U : \langle e_i\rangle$ in $F[y_1, \ldots, y_m, z]$. Here $\{e_1, \ldots, e_n\}$ denotes the canonical basis of $F[y_1, \ldots, y_m, z]^n$.

3) Using elimination, compute $V \cap F[z]$ and return a monic generator of this principal ideal.

Proof. First we equip the $F[y_1, \ldots, y_m]$-module $Q_{F,R}^n$ with an additional $F[z]$-module structure by letting $z \cdot e_i = W \cdot e_i = w_{1,i}e_1 + \cdots + w_{n,i}e_n$. We

want to compute the annihilator of this $F[z]$-module. To this end, we consider it as an $F[y_1, \ldots, y_m, z]$-module and observe that it has a presentation $F[y_1, \ldots, y_m, z]^n/U$. Hence it suffices to compute the annihilator of this $F[y_1, \ldots, y_m, z]$-module and intersect this annihilator with $F[z]$. □

Notice that the matrix W may have infinite order even when this algorithm returns a non-zero polynomial. We can check this easily by examining whether f divides a polynomial of the form $z^m - 1$. This algorithm admits a number of optimizations and variations. Let us point out some possibilities.

Remark 6.3.

1. It is possible to compute the colon ideals $U : \langle e_i \rangle$ in step 2) individually and intersect them at the end. We can use an elimination ordering for $\{y_1, \ldots, y_m\}$. As soon as one of the annihilators contains a non-zero element of $F[z]$ we test whether it is contained in all annihilators. If that holds true, we know that the order of W is finite.

2. Some of the indeterminates y_i can be specialized to random elements of F. If the minimal polynomial of W is zero after this specialization, it was zero before. In practice, this technique is quite effective, but requires great care in judging which indeterminates y_i can be specialized without harm.

3. In some cases it is easier to construct a suitable subgroup of G, consider its universal linear representation, and find an element of infinite order there.

The following test simplifies the check for infinitude by looking at the diagonal elements of W only. It seems this test is usually weak, but still it may work sometimes.

Algorithm 6.4. *(Diagonal Quotient Test for Infinitude)*
INPUT: A finitely presented group $G = \langle X; R \rangle$, and its $\mathcal{C}_F$-universal linear representation $\varphi : G \longrightarrow SL(n, Q_{F,R})$ where F is a field.
OUTPUT: `"Yes"` for some cases when $\varphi(G)$ has infinite order, `"Don't know"` otherwise.
COMPUTATIONS:

1) Compute the set of polynomial equations $S_R \subseteq F[y_{i,j}^{(k)}]$ as in (3).

2) Repeat the following steps 3) – 5) for $k = 1, \ldots, s$.

3) Let $W_k = (y_{i,j}^{(k)})$ be the matrix corresponding to $\varphi(x_k)$.

4) For $\ell = 1, \ldots, n$, choose a term ordering such that $y_{\ell,\ell}^{(k)}$ is the biggest indeterminate. Compute a Gröbner basis of I_R with respect to this term ordering and check whether it contains a leading term of the form $(y_{\ell,\ell}^{(k)})^N$ for some $N > 0$.

5) If one of the Gröbner bases contains no leading term of the form $(y_{\ell,\ell}^{(k)})^N$ for some $N > 0$, return `"Yes"`.

6) Return `"Don't know"`.

Proof. If the algorithm returns `"Yes"` then the matrix $W_k = (y_{i,j}^{(k)})$ under consideration has infinite order in $\varphi(G)$. Namely, if W_k has a finite order N then the leading term of the (ℓ, ℓ)-entry of W_k^N is $(y_{\ell,\ell}^{(k)})^N$. Since there are no polynomials in I_R to reduce such a leading term, the element $W_k = \varphi(x_k)$ generates an infinite cyclic group. □

If this diagonal quotient test does not work initially because the elements x_i have finite orders in G, we can change the presentation of G suitably and apply it again.

Remark 6.5. Another simple approach which works occasionally is to determine the minimal polynomial of $\det(\varphi(w))$ for some word $w \in F(X)$ which is expected to be of infinite order in $G = \langle X; R \rangle$. Obviously we have to use the universal representation $\varphi : G \longrightarrow GL(n, Q_R)$ in this case. If we have $\varphi(w)^N = 1$ in $GL(n, Q_R)$ for some $N > 1$ then $\det(\varphi(w))^N = 1$ holds in Q_R. Thus if $\det(\varphi(w))$ has infinite order in Q_R then w has infinite order.

7 Some Examples

In this section we put our algorithms to work and study some difficult or otherwise inaccessible group presentations.

In following we let $G = \langle a, b, ...;\ r_1 = \cdots = r_t = 1 \rangle$ be a finitely presented group and $\varphi_n : G \longrightarrow GL(n, Q_R)$ its universal representation of size n. The images of the generators will be denoted by $x = \varphi_n(a)$, $y = \varphi_n(b)$, $z = \varphi_n(c)$, $w = \varphi_n(d)$.

7.1 From the Kourovka Notebook (1)

For $i \geq 2$ consider the groups

$$G_i = \langle a, b\,;\ a^i = 1,\ ab = b^3a^3 \rangle.$$

They appeared in the Kourovka Notebook [14] in Problem 7.7 (a question of R.G. Burns for $i = 9$) and Problem 8.10 (D.L. Johnson's question for $i = 7, 9, 15$). The task is to decide whether G_i is finite for $i = 5, 7, 9, \ldots$. For $i = 9$ and $i = 15$ the groups are known to be infinite (see [17] for $i = 9$, [21] for $i = 15$, and also [19] for $i = 9, 15$). Whether G_7 is finite or not is an open question. Our computations give the following partial results for these groups.

Lemma 7.1. *If $\varphi_n(G_i)$ (or G_i) is commutative, it is a finite group of order $2i$.*

Proof. Since $xy = y^3x^3 = x^3y^3$ implies $(xy)^2 = x^2y^2 = 1$, the group $\varphi_n(G_i)$ is a commutative group generated by two elements of order i and 2, respectively. □

Remark 7.2. Using $n = 2$ and the representation $\varphi_2(G_i) = \langle x, y, z, w; xz = zx = 1,\ x^{(i+1)/2} = z^{(i-1)/2},\ xy = y^3x^3,\ yw = wy = 1 \rangle$, we can compute a truncated Gröbner basis of I_R to show that we have $xy = yx$ in the groups $\varphi_2(G_i)$ for $i = 5, 7, 9, 11$. Therefore these groups are commutative and finite.

7.2 From the Kourovka Notebook (2)

The following series of groups appeared in the Kourovka Notebook [14] as Problem 11.10.b. Let

$$\begin{aligned} H_i &= \langle a, b\,;\ a^i = 1,\ b^{-2}ab^2 = a(b^{-1}ab)a^{-1}(b^{-1}a^{-1}b) \rangle \\ &= \langle a, b\,;\ a^i = 1,\ ababa = b^2ab^{-1}ab \rangle \end{aligned}$$

for $i \geq 2$. We want to examine the question whether $a = 1$ in H_i. By [14], it is known that $a \neq 1$ in H_5.

Remark 7.3. First we use $n = 2$. To describe $\varphi_2(H_i)$, we use the monoid representation $\langle x, y, z; x^i = 1,\ xz = zx = 1,\ xyxyx = y^2xzxy \rangle$. By computing the complete Gröbner bases of I_R, we can show that $x \neq 1$ in $\varphi_2(H_i)$ for $i = 5, 10, 15, 20$. Consequently, we have $a \neq 1$ in H_5, H_{10}, H_{15}, and H_{20}.

In the groups $\varphi_2(H_i)$ with $i \in \{2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19\}$, we have $x = \varphi_2(a) = 1$. Furthermore, if we use $n = 3$, we can show that in the subgroup $\varphi_3(H_2)$ of $GL(3, Q_R)$ we also have $x = 1$.

7.3 Some Groups of Deficiency Zero

The following groups appeared in [5], page 63. It is still unknown whether they are finite or not. Our Gröbner basis techniques yield the following partial results.

Example 7.4. Consider the group

$$F_{11} = \langle a, b, c\,;\ cac^{-1}b^{-1}aba,\ bacba^{-1}c^{-1}b,\ cb^{-1}acbca^{-1}\rangle$$

For practical computations, we present the group $\varphi_n(F_{11})$ by

$$\varphi_n(F_{11}) = \langle x, y, z\,;\ xyxzx = yz,\ y^2xzy = zx,\ xy^2 = yzyxz^2\rangle$$

To obtain the third equation, we use $yzyxz^2 = xyxzxyxz^2 = xyxzyzx^{-1}z = xy^2$.

The question whether this group is finite or infinite is still open. However, the reduced Gröbner basis with respect to `DegRevLex` of the ideal I_R for the universal representation $\varphi_2 : F_{11} \longrightarrow SL(2, Q_R)$ can be calculated. It has 117 elements and enables us to check that $\varphi_2(F_{11}) \cong \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3)$.

Example 7.5. Consider the group

$$F_{12} = \langle a, b, c\,;\ acab^{-1}c^{-1}ab,\ b^2a^{-1}c^{-1}acb,\ ca^{-1}b^{-1}cabc\rangle$$

For practical computations, we present $\varphi_n(F_{12})$ as

$$\varphi_n(F_{12}) = \langle x, y, z\,;\ xyxzx = zy,\ xzy^3 = zx,\ zxyz^2 = yx\rangle$$

The reduced Gröbner basis with respect to `DegRevLex` of the ideal I_R for the universal representation $\varphi_2 : F_{12} \longrightarrow SL(2, Q_R)$ can be calculated and show that this ideal agrees with the ideal of $\varphi_2(F_{11})$. Hence we have $\varphi_2(F_{12}) \cong \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3)$. A Gröbner basis of the ideal of $\varphi_3(F_{12})$ is difficult to compute. A partial computation has so far revealed five equations of degree three and 31 equations of degree four.

Example 7.6. Consider the group

$$F_{13} = \langle a, b, c; acab^{-1}c^{-1}ab,\ acbc^{-1}ba^{-1}b,\ b^{-1}abc^2a^{-1}c\rangle$$

Using the equations $abc^2baca = abc^2a^{-1}cb = b^2$ and $abacbacb = abacab^{-1}c = c^2$, we see that we can present $\varphi_n(F_{13})$ in the form

$$\varphi_n(F_{13}) = \langle x, y, z; xyxzx = zy,\ xyz^2yxzx = y^2,\ xyxzyxzy = z^2\rangle$$

The reduced `DegRevLex`-Gröbner basis of the ideal corresponding to the representation $\varphi_2 : F_{13} \longrightarrow SL(2, Q_R)$ turn out to be the same as for $\varphi_2(F_{11})$ and $\varphi_2(F_{12})$. Hence we get $\varphi_2(F_{13}) \cong \mathbb{Z}/(3) \times \mathbb{Z}/(3) \times \mathbb{Z}/(3)$ once again.

Apparently, it is not known whether this group is finite or not, and the Gröbner basis for $\varphi_3(F_{13})$ is difficult to compute.

8 Classification of Finite Generalized Triangle and Tetrahedron Groups

In this section we want to connect some methods used in the classifications of finite generalized triangle and tetrahedron groups with our Gröbner basis techniques and report on some partial additional results. Generalized triangle groups and tetrahedron groups play an important role in the theory of one-relator products of cyclics as well as in the theory of 3-dimensional hyperbolic orbifolds, especially for those with small covolume. A *generalized triangle group* is a group having a presentation

$$G = \langle a, b\,;\ a^p = b^q = R(a,b)^r = 1 \rangle$$

where $p, q, r \geq 2$ and $R(a, b)$ is a cyclically reduced word involving both a and b, and not a proper power in the free product of cyclics. A generalized tetrahedron group is a triangle of groups, i.e. a colimit of a triangle of groups with injective homomorphisms, with generalized triangle groups as vertices, and with cyclic groups as edge groups (see [3]). Both generalized triangle groups and tetrahedron groups admit *essential* representations into (projective) linear groups, that is representations such that the images of the generators and relators have the respective orders. This fact has been used to classify finite generalized triangle and tetrahedron groups.

For generalized triangle groups, the classification was achieved in [6] and [10]. Here we describe two typical cases.

Example 8.1. In order to examine the group $D_1 = \langle a, b\,;\ a^2 = b^3 = (abababab^2abab^2ab^2)^2 = 1 \rangle$, we look at its commutator subgroup D_1'. The group D_1' is generated by $x = b$ and $y = aba$, and in these generators it has a presentation

$$D_1' = \langle x, y\,;\ x^3 = y^3 = xy^{-1}x^{-1}yxyx^{-1}yx^{-1}y^{-1}xyxy^{-1} = 1 \rangle$$

In [10] it was shown that D_1' has an essential representation $\varphi_3 : D_1' \longrightarrow GL(3,F)$ where $F \supset \mathbb{Q}$ is an algebraic number field containing an element γ which satisfies $\gamma^6 - 3\gamma^3 + 1 = 0$. Moreover, the element $\varphi_3(xy)$ has infinite order.

Using the methods of this paper, we can compute a reduced Gröbner basis of the ideal corresponding to the universal representation $\varphi_2 : D_1' \longrightarrow SL(2,Q_R)$. Algorithm 6.2 then shows that minimal polynomial of $\varphi_2(xy)$ is $z^7 - 2z^6 + 3z^5 - 4z^4 + 4z^3 - 3z^2 + 2z - 1$, and therefore this matrix has order 20. However, if we repeat the calculation for $\varphi_3 : D_1' \longrightarrow SL(3,Q_R)$, we get that $\varphi_3(xy)$ has minimal polynomial 0, i.e. infinite order.

Example 8.2. To show that the group

$$D_2 = \langle a, b \,;\; a^3 = b^3 = (a^{-1}b^{-1}ababa^{-1}b)^2 = 1 \rangle$$

is infinite, we use the following method from [11]. Let N be the normal closure of $\{b\}$ in D_2. Then N has index 3 and a presentation

$$N = \langle x, y, z \,;\; x^3 = y^3 = z^3 = (z^{-1}xyx)^2 = (x^{-1}yzy)^2 = (y^{-1}zxz)^2 = 1 \rangle$$

The subgroup N has an essential representation $\bar{\varphi}_2 : N \longrightarrow PSL(2,\mathbb{C})$ for which the element $\bar{\varphi}_2(xy)$ has infinite order.

If we compute the universal representation $\varphi_2 : N \longrightarrow SL(2,Q_R)$, it turns out that the image of N is trivial. To simulate a representation in $PSL(2,\mathbb{C})$, we can use the base field $F = \mathbb{Z}/(2)$. In this way we achieve the equality of the identity matrix and its negative. The Gröbner basis of the corresponding ideal I_R can be computed easily. Then we can apply Algorithm 6.2 and check that the image of xy in this universal representation has order 28. It is an open question how we can treat PSL-representations such as $\bar{\varphi}_2$ using our methods.

In the paper [20], G. Rosenberger and M. Scheer classified the finite generalized tetrahedron groups, except for five groups for which it is still unknown whether they are finite or not. The following proposition is useful for studying the universal representations of size 2×2 of these groups.

Proposition 8.3. Let K be a commutative unitary ring, and let $u, v \in SL(2,K) \setminus \{1, -1\}$.

1. If $\mathrm{tr}(u) = 0$ then $u^2 = -1$.

2. If $u^2 = -1$ then $(\mathrm{tr}(u))^2 = 0$.

3. If $u^2 = 1$ then $(\mathrm{tr}(u))^2 = 4$.

4. For all $k \geq 1$ and all $\alpha_i, \beta_j \in \mathbb{N}$, we have

$$\mathrm{tr}(u^{\alpha_1} v^{\beta_1} \cdots u^{\alpha_k} v^{\beta_k}) = \mathrm{tr}(u^{-\alpha_1} v^{-\beta_1} \cdots u^{-\alpha_k} v^{-\beta_k}).$$

Proof. First we show (1). We let $u = \left(\begin{smallmatrix} u_1 & u_2 \\ u_3 & u_4 \end{smallmatrix}\right)$ and calculate

$$u^2 = \begin{pmatrix} u_1^2 + u_2 u_3 & u_2(u_1 + u_4) \\ u_3(u_1 + u_4) & u_4^2 + u_2 u_3 \end{pmatrix} = \begin{pmatrix} u_1(u_1 + u_4) - 1 & u_2(u_1 + u_4) \\ u_3(u_1 + u_4) & u_4(u_1 + u_4) - 1 \end{pmatrix}$$

because we have $\det(u) = u_1 u_4 - u_2 u_3 = 1$. Therefore $\mathrm{tr}(u) = u_1 + u_4 = 0$ implies $u^2 = -1$.

To prove (2), we note that $u_1(u_1+u_4) = u_4(u_1+u_4) = 0$ by the hypothesis, and hence $(u_1 + u_4)^2 = 0$. Consequently, we get $(\mathrm{tr}(u))^2 = (u_1 + u_4)^2 = 0$. Similarly, claim (3) follows from $u_1(u_1 + u_4) = u_4(u_1 + u_4) = 2$.

Finally, we prove (4). We proceed by induction on k and use the general formula

$$\mathrm{tr}(AB^{-1}) = (\mathrm{tr}(A))\,(\mathrm{tr}(B)) - \mathrm{tr}(AB)$$

for $A, B \in SL(2, K)$. We certainly have $\mathrm{tr}(u^{-\alpha_1} v^{-\beta_1}) = \mathrm{tr}(u^{\alpha_1} v^{\beta_1})$. For $k \geq 2$, we find

$$\begin{aligned}
&\mathrm{tr}(u^{-\alpha_1} v^{-\beta_1} \cdots u^{-\alpha_k} v^{-\beta_k}) = \\
&\quad = \mathrm{tr}(u^{-\alpha_1} v^{-\beta_1})\ \mathrm{tr}(u^{-\alpha_2} v^{-\beta_2} \cdots u^{-\alpha_k} v^{-\beta_k}) - \mathrm{tr}(v^{\beta_1} u^{\alpha_1 - \alpha_2} v^{-\beta_2} \cdots u^{-\alpha_k} v^{-\beta_k}) \\
&\quad = \mathrm{tr}(u^{\alpha_1} v^{\beta_1})\ \mathrm{tr}(u^{\alpha_2} v^{\beta_2} \cdots u^{\alpha_k} v^{\beta_k}) - \mathrm{tr}(u^{\alpha_1 - \alpha_2} v^{\beta_2} \cdots u^{\alpha_k} v^{\beta_k - \beta_1}) \\
&\quad = \mathrm{tr}(u^{\alpha_1} v^{\beta_1} \cdots u^{\alpha_k} v^{\beta_k})
\end{aligned}$$

This concludes the proof. □

Therefore we have to expect many additional relations in $\varphi_2(T)$ where T is the group under consideration. In fact, the following examples are based on our computer calculations and show that all representations of size 2×2 of the five groups are finite.

Example 8.4. Consider the group

$$T_1 = \langle a, b, c\,;\ a^2 = b^3 = c^3 = (ac)^2 = (bc)^2 = (ababab^2abab^2ab^2)^2 = 1\rangle$$

First we use the universal representation $\varphi_2 : T_1 \longrightarrow GL(2, Q_R)$. For the group $\varphi_2(T_1)$, we can use the computation of a trucated Groebner basis of I_R to show $(xy)^2 = (yx)^2 = 1$. Thus we have

$$\varphi_2(T_1) = \langle x, y, z; x^2 = y^3 = z^3 = (xy)^2 = (yz)^2 = (xz)^2 = 1\rangle$$

This group is clearly finite. In fact, it is easy to see that it has 24 elements and is a double cover of the alternating group A_4.

However, the question whether the image of the universal representation $\varphi_3 : T_1 \longrightarrow GL(3, Q_R)$ is finite or infinite is still open.

Example 8.5. The second group on the Rosenberger-Scheer list is

$$T_2 = \langle a, b, c\,;\ a^2 = b^5 = c^2 = (ac)^2 = (bc)^2 = (abab^3ab^2ab^4ab)^2\rangle$$

Using the modified presentation

$$\begin{aligned}\varphi_n(T_2) = \langle x, y, z \quad ;\quad & x^2 = y^5 = z^2 = 1,\ xz = zx,\ zyz = y^4,\\ & yxyxy^3xy^2xy^4xy = xyxy^3xy^2xy^4x\rangle\end{aligned}$$

and a truncated Gröbner basis computation, we get $(xy)^2 = (yx)^2 = 1$ for the universal representation $\varphi_2 : T_2 \longrightarrow GL(2, Q_R)$. Hence every word in $\varphi_2(T_2)$ can be written in the form $x^\varepsilon\, w$ with $\varepsilon \in \{0, 1\}$ and a word w involving only y and z. Since $\langle y, z\,;\ y^5 = z^2 = (yz)^2 = 1\rangle$ is known to be a finite triangle group, the group $\varphi_2(T_2)$ is finite, too.

For the universal representation $\varphi_3 : T_2 \longrightarrow GL(3, Q_R)$, it appears to be difficult to compute a Gröbner basis of I_R.

Example 8.6. The third group considered by Rosenberger and Scheer is

$$T_3 = \langle a, b, c\,;\ a^3 = b^5 = c^3 = (ac)^2 = (b^2c)^2 = (aba^2b^2)^2\rangle$$

For practical computations, we present the group $\varphi_n(T_3)$ by

$$\varphi_n(T_3) = \langle x, y, z\,;\ x^3 = y^5 = z^3 = 1,\ xzx = z^2,\ y^3 = zy^2z,\ yx^2y^2xy = x^2y^3x\rangle$$

In this way, the defining equations of the universal ideal have degrees ≤ 7. For the representation $\varphi_2 : T_3 \longrightarrow GL(2, Q_R)$, a truncated Gröbner basis

computation yields the equations $x = y = z = 1$. Hence this representation is trivial.

For the representation $\varphi_3 : T_3 \longrightarrow GL(3, Q_R)$, a truncated Gröbner basis computation yields $\mathrm{tr}(x^2) = \mathrm{tr}(z)$ and $\mathrm{tr}(z^2) = \mathrm{tr}(x)$.

Example 8.7. Next we consider the group

$$T_4 = \langle a, b, c\,;\ a^3 = b^5 = c^2 = (ac)^2 = (bc)^2 = (a^2ba^2b^2abab^{-1})^2 = 1\rangle$$

To get equations of low degree, we use the presentation

$$\begin{aligned}\varphi_n(T_4) = \langle x, y, z \quad ;\quad & x^3 = y^5 = z^2 = 1,\ zxz = x^2,\ zyz = y^4,\\ & yx^2y^2xyxy^4x^2y = xyx^2y^4x^2y^3x\rangle\end{aligned}$$

A computation of a Gröbner basis for the ideal I_R corresponding to the universal representation $\varphi_2 : T_4 \longrightarrow SL(2, Q_R)$ yields $x = y = 1$ and $z = \pm 1$. Hence $\varphi_2(T_4)$ is the group with two elements. Notice that we used $SL(2, Q_R)$ here, since the computation for $GL(2, Q_R)$ is more involved.

Example 8.8. Finally, we want to examine the group

$$T_5 = \langle a, b, c\,;\ a^3 = b^3 = c^3 = (ac)^2 = (bc^{-1})^2 = (ababa^{-1}b^{-1})^2 = 1\rangle$$

A more balanced presentation of this group is

$$\begin{aligned}\varphi_n(T_5) = \langle x, y, z \quad ;\quad & x^3 = y^3 = z^3 = 1,\ xzx = z^2,\ yz^2 = zy^2,\\ & xyxyx^2y^2x = yxy^2x^2y^2\rangle\end{aligned}$$

Using the representation $\varphi_2 : T_5 \longrightarrow GL(2, Q_R)$, a truncated Gröbner basis computation of I_R shows $y = z$ and $x^2 = y$. Hence $\varphi_2(T_5)$ is the group with three elements.

The Gröbner basis of the universal ideal corresponding to the representation $\varphi_3 : T_5 \longrightarrow GL(3, Q_R)$ is harder to compute. A truncated computation yields several equalities in $\varphi_3(T_5)$, for instance $\mathrm{tr}(y) = \mathrm{tr}(z)$. However, it is not clear whether $\varphi_3(T_5)$ is finite or not.

References

[1] S.I. Adian and V.G. Durnev, *Algorithmic problems for groups and semigroups,* Uspekhi Mat. Nauk. **55** (2000), 3–94; translation in Russian Math. Surveys **55** (2000), 207–296.

[2] G.W. Brumfiel and H.M. Hilden, *SL(2) Representations of Finitely Presented Groups*, Contemp. Math. **187**, Amer. Math. Soc., Providence, 1995

[3] B. Fine and G. Rosenberger, *Algebraic Generalization of Discrete Groups*, Marcel Dekker, New York, 1999.

[4] G. Havas, D.F. Holt, P.E. Kenne and S. Rees, *Some challenging group presentations,* J. Austral. Math. Soc. **67** (1999), 137–163.

[5] G. Havas, M. F. Newman, and E. A. O'Brien, *Groups of deficiency zero,* DIMACS Series in Discrete Mathematics and Theoretical Computer Science **25**, 1996.

[6] J. Howie, V. Metaftsis, and R.M. Thomas, *Finite generalized triangle groups*, Trans. Amer. Math. Soc. **347** (1995), 3613-3624.

[7] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain, *Generic-case complexity and decision problems in group theory*, J. of Algebra **264** (2003), 665–694.

[8] I. Kapovich, A. Myasnikov, P. Schupp, and V. Shpilrain, *Average-case complexity for the word and membership problems in group theory*, Adv. Math. (to appear)

[9] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 1*, Springer, Heidelberg 2000.

[10] L. Levai, G. Rosenberger, and B. Souvignier, *All finite generalized triangle groups*, Trans. Amer. Math. Soc. **347** (1995), 3625–3627.

[11] F. Levin and G. Rosenberger, *On free subgroups of generalized triangle groups, Part II*, in: Group Theory, World Scientific 1993, 206–228.

[12] A. Lubotzky and A.R. Magid, *Varieties of representations of finitely generated groups*, AMS Memoirs **336**, Amer. Math. Soc, Providence 1985

[13] R. Lyndon and P. Schupp, *Combinatorial Group Theory*, Springer, New York 1977.

[14] V.D. Mazurov and E.I. Khukhro (eds.), *Open problems in group theory: The Kourovka Notebook*, Institute of Mathematics, Novosibirsk, 2002.

[15] C.F. Miller III, *On Group-theoretic Decision Problems and their Classification,* Ann. of Math. Studies **68**, Princeton University Press, Princeton 1971.

[16] C.F. Miller III, *Decision problems for groups – Survey and reflections*, in: G. Baumslag and C.F. Miller III (eds.), *Algorithms and Classification in Combinatorial Group Theory*, Springer, New York 1992, pp. 1–60.

[17] M.F. Newman, *Proving a group infinite*, Arch. Math. **54** (1990), 209–211.

[18] M.F. Newman, *private communication*, 2005.

[19] M.I. Prishchepov, *Aspherisity, atorisity and symmetrically presented groups*, Commun. in Alg. **23** (1995), 5095–5117.

[20] G. Rosenberger and M. Scheer, *Classification of finite generalized tetrahedron groups,* Contemp. Math. **296** (2002), 207–229.

[21] D.J. Seal, *The orders of the Fibonacci groups*, Proc. Roy. Soc. Edinburgh, Sect. A **92** (1982), 181–192.