Theoretical Computer Science 32 (1984) 279–295
North-Holland

ON THE COMPLEXITY OF INTERSECTION AND CONJUGACY PROBLEMS IN FREE GROUPS

J. AVENHAUS and K. MADLENER

Fachbereich Informatik, Universität Kaiserslautern, 6750 Kaiserslautern, Fed. Rep. Germany

Communicated by R. Book
Received November 1982
Revised January 1984

Abstract. Nielsen type arguments have been used to prove some problems in free groups (e.g., the generalized word problem) [2] to be P-complete. In this paper we extend this approach. Having a Nielsen reduced set of generators for subgroups H and K one can solve a lot of intersection and conjugacy problems in polynomial time in a uniform way.

We study the solvability of (i) $\exists h \in H,\ k \in K: hx = yk$ in F, and (ii) $\exists w \in F: y^{-1}Hw = K$ and characterize the set of solutions. This leads for (i) to an algorithm for computing a set of generators for $H \cap K$ (and a new proof that free groups have the Howson property). For (ii) this gives a fast solution of Moldavanskii's conjugacy problem; an algorithm for computing the normal hull of H then gives a representation of all solutions. All the algorithms run in polynomial time and the decision problems are proved to be P-complete under log-space reducibility.

1. Introduction

Let S be a finite set and $F = \langle S; \emptyset \rangle$ the free group with basis S. If $\underline{S} = \{s, \bar{s} \mid s \in S\}$ is the set of generators and their formal inverses, then any element of F can be represented by a finite word over $\underline{S}$. We denote by $\underline{S}^*$ the set of all finite words over $\underline{S}$, by e the empty word, by $|w|$ the length of a word w and by $\equiv$ the identity on $\underline{S}^*$. For $x, y \in \underline{S}^*$ we write $x = y$ in F if x and y represent the same element in F.

A subgroup H of F will be given by a set of generators: If $U \subset \underline{S}^*$ we denote by $\langle U \rangle$ the subgroup of F generated by U and by $\underline{U}^*$ the set of words $w \equiv u_1 \dots u_n$, $u_i \in \underline{U} := \{u^\varepsilon \mid u \in U, \varepsilon = \pm 1\}$, $n \in \mathbb{N}$. For any word $x \in \underline{S}^*$ we have $x \in \langle U \rangle$ iff $x = w$ in F for some $w \in \underline{U}^*$. For $w \in \underline{U}^*$ as above, let $n = |w|_U$ be the U-length of w and w is called freely reduced in $\underline{U}$, if $u_i \neq u_{i+1}^{-1}$ for all i. For each $x \in \underline{S}^*$ there is a unique freely reduced word $\rho(x)$ with $x = \rho(x)$ in F. It is known that $x = y$ in F iff $\rho(x) \equiv \rho(y)$ [8]. ρ is linear time computable and the presentation of group elements of free groups by freely reduced words is unique.

If $H = \langle U \rangle$ and $x \in H$, then $x = w$ in F for some $w \in \underline{U}^*$. This representation for x may not be unique even if one restricts to freely reduced words in $\underline{U}^*$. U generates H freely (or U is independent) if for every $x \in H$ there is a unique $w \in \underline{U}^*$ freely reduced in $\underline{U}$ with $x = w$ in F. The Nielsen–Schreier theorem states that subgroups

of free groups are again free groups, so a set of free generators for a subgroup H always exists.

In [2] a polynomial time algorithm was presented for computing from $U = \{u_1, \ldots, u_l\}$ a set $V = \{v_1, \ldots, v_m\}$, $m \leq l$, of free generators for $\langle U \rangle$ based on Nielsen's proof of the subgroup theorem. The set V is a Nielsen-reduced set of generators. N-reduced sets of generators for a subgroup H have important properties and were used in [2] to give polynomial time algorithms for some decision problems in free groups which turned out to be polynomially time complete, such as the generalized word problem (i.e., to decide whether $x \in \langle U \rangle$), the equality problem and the isomorphism problem for finitely generated subgroups.

In this paper we continue the study of algorithmic problems related with subgroups of free groups. It turns out that Nielsen type arguments are a powerful tool for solving these problems and that the combinatorial counting arguments are strong enough to give good complexity bounds.

We first consider the problem of deciding whether two elements define the same double coset HwK of two given finitely generated subgroups of F. This problem is equivalent to the solvability of the equation $\exists h \in H, k \in K: uhv = k$ in F for given $u, v \in S^*$. In Section 3, bounds for the length of a shortest solution are derived and a polynomial time algorithm for deciding the solvability and computing a solution of the equation is given. This result is used to solve intersection problems of cosets like $Hu \cap vK \neq \emptyset$, $Hu \cap Kv \neq \emptyset$ and $H \cap K \neq 1$ in polynomial time.

Next we consider the determination of all solutions of the equation above and a representation of the set of solutions. This leads to the problem of computing a set of generators for the intersection of two finitely generated groups. This intersection is finitely generated and an explicit bound for the number of generators is known [3, 4, 5]. In Section 4 we give a new proof of this fact based only on combinatorial arguments and present a polynomial time algorithm for computing a set of generators for the intersection. The algorithm is based on a search in a tree in which nodes are labelled by elements of one subgroup up to a certain length. Conditions for the length of the generators and a search strategy are developed from properties of N-reduced sets to keep the time bound polynomial. Finite representations for $Hu \cap vK$, $Hu \cap Kv$ are derived from the representation of $H \cap K$ by its generators.

In Section 5 we study equations with cosets of subgroups H, K like

$$\exists x, y: Hx \subset yK \quad \text{and} \quad \exists x, y: Hx = yK.$$

Such equations lead to conjugacy problems of subgroups in free groups, i.e.,

$$\exists x: x^{-1}Hx \leq K \quad \text{and} \quad \exists x: x^{-1}Hx = K.$$

These problems were known to be solvable in free groups [7, 5] but only length bounds for minimal solutions were known. We derive the shape of the minimal solutions and use this result to give a polynomial time algorithm for computing all minimal solutions. A representation of all solutions is then computed using a

polynomial time algorithm for computing generators for the normalizer of a finitely generated subgroup.

Finally, in Section 6 we prove by using a result of [2] that the decision problems solved in this paper are polynomially time complete under log-space reducibility.

For the complexity statements and encodings into a fixed alphabet we use the same assumptions as in [2].

This paper is a continuation of [2]. We study problems that can be solved with Nielsen type arguments in a uniform way in polynomial time. For the decision problems we prove the P-completeness, so they can be solved on logarithmic space only if P equals LOG SPACE. We did not intend to give sharp time bounds for the complexity of these problems. A referee pointed out that the Schreier method would probably lead to algorithms that are more efficient than ours.

2. Nielsen reduction

A lot of subgroup problems in free groups can be solved using properties of Nielsen reduced sets [5]. Nielsen proved the subgroup theorem (cf. [5]) by showing that each finite set U can be transformed by a finite sequence of operations into a Nielsen reduced set which freely generates the same subgroup $\langle U\rangle$.

To introduce this concept we define the sets of *great prefixes*, *small prefixes* and *halves* of $U \subset \underline{S}^*$ by

$$\text{GPREF}(U) = \{x \mid \exists y\colon xy \in \underline{U} \text{ and } |x| > |y|\},$$

$$\text{SPREF}(U) = \{x \mid \exists y\colon xy \in \underline{U} \text{ and } |x| \leq |y|\},$$

$$\text{HALF}(U) = \{x \mid \exists y\colon xy \in \underline{U} \text{ and } |x| = |y|\}.$$

A word x is called an *isolated prefix* of $\underline{U}$ if there is exactly one y such that $xy \in \underline{U}$ [8]. So an isolated prefix of $\underline{U}$ determines an $u \in \underline{U}$ uniquely.

2.1. Definition. A set $U \subset \underline{S}^*$ of freely reduced words is *Nielsen reduced* (N-reduced), if (N1) and (N2) hold:

(N1) If $x \in \text{GPREF}(U)$, then x is an isolated prefix of $\underline{U}$.

(N2) If $x\bar{y}^{-1} \in \underline{U}$, $|x| = |y|$, then either x or y is an isolated prefix of $\underline{U}$.

It is easy to see that any N-reduced set is independent and further it has the following important property [8]:

(N3) If $z_1, \ldots, z_p \in \underline{U}$, $z_i \neq z_{i+1}^{-1}$, then $\rho(z_1 \ldots z_p)$ (the free reduction in $\underline{S}^*$) contains a character from any z_i, i.e., there are $x_1, \ldots, x_{p+1}$, $y_1, \ldots, y_p$ such that $z_i \equiv x_i y_i x_{i+1}^{-1}$, $y_i \neq e$ $(1 \leq i \leq p)$ and $\rho(z_1 \ldots z_p) \equiv x_1 y_1 y_2 \ldots y_p x_{p+1}$. In particular, the initial segment of z_1 which remains uncancelled in the free reduction is either a great prefix or a half of z_1 and it is isolated in both cases.

This property enables one to reconstruct the product $z_1 \dots z_p$ out of the freely reduced word $\rho(z_1 \dots z_p)$: The greatest isolated prefix of $\underline{U}$ which is an initial segment of $\rho(z_1 \dots z_p)$ determines z_1 uniquely [2].

A process that transforms a set U into an N-reduced set V such that $\langle U\rangle = \langle V\rangle$ is called an N-reduction. The following theorem is proved in [2].

2.2. Theorem. *A set $U = \{u_1, \dots, u_p\}$ with $|u_i| \leq n$ can be Nielsen-reduced on a TM in time $O(p^5 n^2)$.*

The idea of the proof is to show that a polynomial number of operations of type

(1) delete u_i from U if $u_i = u_j^{\varepsilon}$ $(\varepsilon = \pm 1)$ or $u_i = e$ in F,

(2) replace u_j by $(u_j u_i^{\varepsilon})$ $i \neq j$, $\varepsilon = \pm 1$,

are enough to transform U into a Nielsen reduced set V.

In order to test whether $x \in \langle U\rangle$, U finite, we first transform U into an N-reduced set V. Property (N3) for V can now be used to decide whether $x \in \langle U\rangle = \langle V\rangle$. More precisely, from [2] we have the following theorem.

2.3. Theorem. *Let $V = \{v_1, \dots, v_m\} \subset \underline{S}^*$ be N-reduced, $|v_i| \leq n$ and $x \in \underline{S}^*$ with $|x| \leq t$. There are functions f_V, g_V computable in time $O(tmn)$ with:*

(a) *$x = f_V(x) g_V(x)$ in F, $f_V(x) \in \underline{V}^*$, $|f_V(x)|_V \leq t$ and $|g_V(x)| \leq t$.*

(b) *$g_V(x)$ has no prefix $z \in \text{GPREF}(V)$.*

(c) *$g_V(x) \in \text{SPREF}(V)$ if there is a $y \in \underline{S}^*$ such that $xy \in \langle V\rangle$ and xy is freely reduced.*

(d) *For any $y \in \underline{S}^*$, if $\langle V\rangle y = \langle V\rangle x$, then $|g_V(x)| \leq |y|$. So $x \in \langle V\rangle$ iff $g_V(x) \equiv e$.*

(e) *For any $y \in \underline{S}^*$, if $\langle V\rangle y = \langle V\rangle x$, then $g_V(x) \equiv g_V(y)$.*

The idea for the proof is to split a maximal factor $f_V(x) \in \underline{V}^*$ from the left of x, leaving $g_V(x)$ with $x = f_V(x) g_V(x)$ in F: If w is freely reduced and $w \equiv xw'$, where $x \in \text{GPREF}(V) \cup \text{HHALF}(V)$ is an isolated prefix of maximal length, then there is a unique $z \in \underline{V}$ with $z \equiv x\bar{y}^{1}$. We have $w = z \cdot yw'$ in F and the process can be repeated with input yw' until no such isolated prefix x is found or two factors z, $\bar{z}^{1}$ appear. Then $f_V(x)$ and $g_V(x) \equiv yw'$ have been computed. Notice that yw' is freely reduced, $y \in \text{SPREF}(V)$ and w' is a suffix of w.

Property (c) will be of great importance because it restricts and gives a test for the set of words which are prefixes of words in $\langle V\rangle$.

In the sequel of the paper we are interested in algorithms for various problems that run in polynomial time measured in the length of the input. To be precise, we define for $U = \{u_1, \dots, u_p\} \subset \underline{S}^*$ the length $|U| = |u_1| + \cdots + |u_p|$ whereas the cardinality of U is denoted by $\|U\|$. Then Theorem 2.2 states that the Nielsen reduction can be done in polynomial time and by Theorem 2.3 the functions $f(V, x) = f_V(x)$ and $g(V, x) = g_V(x)$ can be computed in polynomial time.

3. Nonempty intersection of cosets

From now on we use the fixed notation

$$U=\{u_1,\dots,u_l\}, \qquad H=\langle U\rangle,$$

$$V=\{v_1,\dots,v_m\}, \qquad K=\langle V\rangle,$$

$$\mathrm{SP}(V,U)=\mathrm{SPREF}(V)\cdot\mathrm{SPREF}(U)^{-1},$$

$$\alpha(V,U)=\|\mathrm{SPREF}(V)\|\cdot\|\mathrm{SPREF}(U)\|.$$

Because of Theorem 2.2 we may assume that U, V are N-reduced. The significance of $\mathrm{SP}(V,U)\subset \underline{S}^*$ and of the number $\alpha(V,U)$ will become clear later on. We note that $\alpha(V,U)$ is polynomial in the length of the input U, V.

Our first problem is to decide whether the intersection of a left and a right coset is nonempty, i.e., whether, for given $x, y\in \underline{S}^*$, $U, V\subset \underline{S}^*$,

$$Hx\cap yK\neq\emptyset.$$

This problem is equivalent to the problem whether two double cosets are equal, for $Hx\cap yK\neq\emptyset$ iff $y\in HxK$ iff $HxK=HyK$.

Let $u\equiv g_U(y)^{-1}$ and $v\equiv g_U(x)$; then by Theorem 2.3 we have $Hx\cap yK\neq\emptyset$ iff the equation

$$\exists h\in H, k\in K:\quad uhv=k \text{ in } F \tag{1}$$

is solvable. Moreover, u^{-1} and v have no prefix in $\mathrm{GPREF}(U)$. We first study the solvability of such equations and the structure of the solutions (h, k).

3.1. Lemma. *Let U, V be N-reduced and $u, v\in \underline{S}^*$ freely reduced such that u^{-1} and v have no prefix in $\mathrm{GPREF}(U)$. If there is a $w\in \underline{U}^*$ freely reduced in $\underline{U}^*$ with*

$$uwv\in K, \qquad |w|_U\geq\alpha(V,U),$$

then there exist $w', w''\in \underline{U}^*$ with $w=w'w''$ in F,

$$uw''v\in K, \qquad |w''|_U<|w|_U,$$

$$uw'\bar{u}^{-1}\in K, \qquad |w'|_U<2\cdot\alpha(V,U).$$

Proof. Let $w\equiv z_1\dots z_p$, $z_i\in \underline{U}$, $z_i\not\equiv z_{i+1}^{-1}$, $p\geq\alpha(V,U)$ and $uwv\in K$. Since $\bar{u}^{-1}$ and v have no prefix in $\mathrm{GPREF}(U)$ and because of property (N3) of N-reduced sets there is a decomposition

$$u\equiv u_0x_0^{-1}, \qquad z_i\equiv x_{i-1}y_ix_i^{-1}, \qquad v\equiv x_pv_0$$

with $\rho(uwv)\equiv u_0y_1\dots y_pv_0$, $\rho(uz_1\dots z_i)\equiv u_0y_1\dots y_ix_i^{-1}$ and $x_i\in\mathrm{SPREF}(U)$ for $i=0,1,\dots,p$. We have $u_0y_1\dots y_pv_0\in K$ so $w_i:\equiv g_V(u_0y_1\dots y_i)\in\mathrm{SPREF}(V)$ by Theorem 2.3(c). It is easy to see that $g_V(uz_1\dots z_i)\in\mathrm{SPREF}(V)\cdot\mathrm{SPREF}(U)^{-1}=\mathrm{SP}(V,U)$.

Now $p \geq \alpha(V, U) = \|\text{SPREF}(V)\| \cdot \|\text{SPREF}(U)\|$, so there must exist $0 \leq i < j \leq \alpha(V, U)$ such that $w_i \equiv w_j$ and $x_i \equiv x_j$. By Theorem 2.3(a), $u_0 y_1 \dots y_t = k_t w_t$ in F with $k_t \equiv f_V(u_0 y_1 \dots y_t) \in K$ for $t = 0, 1, \dots, p$. This gives

$$\begin{aligned} uz_1 \dots z_i &= u_0 y_1 \dots y_i \bar{x}_i^1 = k_i w_i \bar{x}_i^1 = k_i w_j \bar{x}_j^1 \\ &= k_i k_j^{-1} k_j w_j x_j^{-1} = k_i k_j^{-1} uz_1 \dots z_j \quad \text{in } F. \end{aligned}$$

It is now easy to verify that the statements of the lemma hold with $w' \equiv z_1 \dots z_j (z_1 \dots z_i)^{-1}$ and $w'' := z_1 \dots z_i z_{j+1} \dots z_p$. □

By Lemma 3.1, equation (1) has a solution iff there is a 'short' solution $w_0 \in M = \{w \in \underline{U}^* \mid w \text{ freely reduced in } \underline{U}, |w|_U \leq \alpha(V, U)\}$ such that $uw_0 v \in K$. This gives a fast nondeterministic algorithm for deciding the solvability of (1): Select a $w \in M$ and verify $uwv \in K$. By Theorem 2.2 this can be done in polynomial time. But the naive deterministic algorithm that tests $uwv \in K$ for all $w \in M$ is too expensive since $\|M\|$ is exponential in $|U| + |V|$.

Let $<$ be an order on $\underline{U}$. We extend this order to $\underline{U}^*$ by

$$\begin{aligned} w_1 < w_2 \text{ iff } & |w_1|_U < |w_2|_U \text{ or} \\ & |w_1|_U = |w_2|_U \text{ and } w_1 \text{ is less than } w_2 \text{ in the} \\ & \text{lexicographical order on } \underline{U}^* \text{ defined by } <. \end{aligned}$$

We organize M in an ordered tree T as follows: T has root e and any node w has sons $wu_i^{\pm}$. Then a breadth first traversal of T visits the $w \in M$ in order $<$. To get a polynomial algorithm we have to avoid the full search in T. The next lemma gives conditions which guarantee that a subtree with root w must not be traversed.

3.2. Lemma. *Let U, V, u, v be as in Lemma 3.1.*

(a) *If $w, w' \in \underline{U}^*$, ww' freely reduced in $\underline{U}$ and $uww'v \in K$, then $g_V(uw) \in \text{SP}(V, U)$.*

(b) *If $w, w' \in \underline{U}^*$ and $g_V(uw) \equiv g_V(uw')$, then for all $w'' \in \underline{U}^*$ we have $uww''v \in K$ iff $uw'w''v \in K$.*

Proof. (a) Let $ww' \equiv z_1 \dots z_p$, $w \equiv z_1 \dots z_q$, $q \leq p$, with $z_i \in \underline{U}$, $z_i \neq z_{i+1}^{-1}$ and $uww'v \in K$. We noticed already in the proof of Lemma 3.1 that $g_V(uw) \in \text{SPREF}(V) \cdot \text{SPREF}(U)^{-1} = \text{SP}(V, U)$.

(b) By Theorem 2.3 there are $k, k' \in K$ such that $uw = k g_V(uw)$, $uw' = k' g_V(uw')$ in F. If $g_V(uw) \equiv g_V(uw')$, then $uww''v \cdot (uw'w''v)^{-1} \in K$, so $uww'v \in K$ iff $uw'w''v \in K$. □

We now present our algorithm for deciding whether (1) has a solution. Let u, v, U, V be as in Lemma 3.1. We traverse the tree T breadth first in the following way: Suppose we visit node w. If $g_V(uw) \notin \text{SP}(V, U)$, then by part (a) of Lemma 3.2 no descendant ww' of w can satisfy $uww'v \in K$, so the subtree with root w may be cancelled. If another node w' with $g_V(uw) \equiv g_V(uw')$ was visited earlier, then by part (b) a descendant of w leads to a solution of (1) iff a descendant of w' leads to

a solution. Since the search in the subtree with root w' goes on, the subtree with root w can be cancelled. It turns out that this algorithm needs only a polynomial number of tests of the form "$uwv \in K$?".

The precise algorithm is given below. We do not build up all the tree T. Instead, we maintain a list L with entries $(w, g_V(uw))$ for any node w visited so far. The pth entry is referred to by $L_p = (L'_p, L''_p)$. The pointers i and j refer to the actual and to the currently last element in the list, respectively. If node w is actual, all sons wu_i^{ε} are created and put into the list, except those which can be cancelled according to Lemma 3.2. The algorithm has input x, y, U, V to decide whether $Hx \cap yK \neq \emptyset$. First x, y are transformed to v, u to meet the hypotheses of Lemma 3.1.

Algorithm INTERSECT
Input: $x, y \in \underline{S}^*$, U, V N-reduced.
Output: Solution $h \in \underline{U}^*$ with $\bar{y}^1 hx \in K$ or "no solution".
Method:
(1) $u \Leftarrow g_U(y)^{-1}$; $v \Leftarrow g_U(x)$;
(2) **if** $uv \in K$ **then** $h \Leftarrow f_U(y) f_U(x)^{-1}$ is solution, **stop**;
(3) $u \Leftarrow g_V(u)$; $v \Leftarrow g_V(v^{-1})^{-1}$;
(4) **if** $u \notin \mathrm{SP}(V, U)$ **or** $\bar{v}^1 \notin \mathrm{SP}(V, U)$ **then** "no solution", **stop**;
(5) $i \Leftarrow 1$; $j \Leftarrow 1$; $L_1 \Leftarrow (e, u)$;
(6) **while** $i \leq j$ **do**
(7) **begin** for all $z \in \underline{U}$ with L'_i does not end with $\bar{z}^1$ **do**
(8) **begin** $w \Leftarrow g_V(L''_i z)$;
(9) **if** $wv \in K$ **then** $h \Leftarrow f_U(y) \cdot L'_i z \cdot f_U(x)^{-1}$ is a solution, **stop**;
(10) **if** $w \in \mathrm{SP}(V, U)$ and w is not yet second component in the list
(11) **then** $j \Leftarrow j+1$; $L_j \Leftarrow (L'_i z, w)$
(12) **end**;
(13) $i \Leftarrow i+1$
(14) **end**;
(15) **stop** "no solution".

3.3. Lemma. *Algorithm* INTERSECT *is correct and runs on input x, y, U, V with $|x|$, $|y| \leq t$, $|u_i|$, $|v_j| \leq n$ for $i = 1, \ldots, l$ and $j = 1, \ldots, m$ in time $O(tn \cdot (l+m) + l^3 m^2 n^5)$.*

Proof. We assume that the $z \in \underline{U}$ in line (7) are taken in order $<$. It is easy to see that the following loop invariant holds: If $p \leq j$, then $L'_p \in \underline{U}^*$ is freely reduced in $\underline{U}$, $uL'_p v \notin K$, $L''_p \in \mathrm{SP}(V, U)$ and $uL'_p = kL''_p$ in F for some $k \in K$. Moreover, if $p \neq q \leq j$, then $L''_p \neq L''_q$. Since $\mathrm{SP}(V, U)$ has at most $\alpha(V, U)$ elements we have at any time $j \leq \alpha(V, U)$; so the algorithm stops.

We now prove the correctness. If the algorithm stops with output h, then $h \in H$ is a solution according to the loop invariant. If it stops in line (4), then there is no solution according to Lemma 3.2. So it remains to show that there is no solution if the algorithm stops in line (15). Assume contrarily that there is an $h \equiv z_1 \ldots z_p \in M$

such that $uhv \in K$. We may assume that h is minimal in the order $<$. Let r be maximal such that $h_0 \equiv z_1 \dots z_r$ is the first component of a list element. Then $r < p$ by the loop invariant and $g_V(uh_0z_{r+1}) \in \mathrm{SP}(V, U)$ by Lemma 3.2. When h_0 is actual, i.e., $L_i' \equiv h_0$, there is a list element $L_q \equiv g_V(L_i'' z_{r+1})$, for otherwise the algorithm would stop in line (9) or h_0z_{r+1} would be put to the list since $g_V(L_i'' z_{r+1}) \equiv g_V(uh_0z_{r+1}) \in \mathrm{SP}(V, U)$ by Theorem 2.2(e). So $L_q'' = kL_i'' z_{r+1}$ in F for some $k \in K$ and, by the loop invariant, $uL_q' = k_1 L_q'' = k_2 L_i'' z_{r+1} = k_3 uL_i' z_{r+1} = k_3 uz_1 \dots z_{r+1}$ in F for some k_1, k_2, $k_3 \in K$. Now, for $\hat{h} \equiv L_q' z_{r+2} \dots z_p$ we have $u\hat{h}v = k_3 uhv \in k_3 K = K$. But $L_q' < h_0 z_{r+1}$ since L_q' was visited earlier than h_0z_{r+1}, so $\hat{h} \equiv L_q' z_{r+2} \dots z_p < h_0 z_{r+1} z_{r+2} \dots z_p \equiv h$. This is a contradiction to the fact that h was minimal with $uhv \in K$.

It remains to prove the time bound. The preconditioning (up to the **while**-loop) takes

$$\mathrm{O}(lnt) + \mathrm{O}(mnt) + \mathrm{O}(mnt) + \mathrm{O}(\alpha(V, U) \cdot n) = \mathrm{O}(nlt(l+m) + lmn^2)).$$

The computations in the **while**-loop are only with words of length $\mathrm{O}(n)$. The loop is passed at most $\alpha(V, U)$ times and the cost for one pass is $\mathrm{O}(l(mn^2 + mn^2 + \alpha(V, U)n)) = \mathrm{O}(l^2mn^3)$. The whole cost is then the bound given in the statement of the theorem. □

Notice, if U, V are fixed and we want only to decide whether $Hx \cap yK \neq \emptyset$, then we have a linear time algorithm in the length of x and y.

3.4. Theorem. *The problems*

$$\textsc{Icos}(x, y, U, V) \Leftrightarrow Hx \cap yK \neq \emptyset,$$

$$\textsc{Ircos}(x, y, U, V) \Leftrightarrow Hx \cap Ky \neq \emptyset,$$

$$\textsc{Ilcos}(x, y, U, V) \Leftrightarrow xH \cap yK \neq \emptyset,$$

$$\textsc{Isubg}(U, V) \Leftrightarrow H \cap K \neq \langle e \rangle$$

are solvable in polynomial time with time bound as in Lemma 3.3. Furthermore, in the positive case we can compute an element of the respective intersection within the same time bound.

Proof. For Icos (intersection of cosets) we refer to Lemma 3.3. The problems Ircos and Ilcos (intersection of right and left cosets, respectively) are subproblems of Icos: for example, $Hx \cap Ky \neq \emptyset$ iff $Hx\bar{y}^1 \cap eK \neq \emptyset$. For Isubg (intersection of subgroups) we start in Algorithm Intersect with input $x \equiv y \equiv e$ and ignore the trivial solution $h \equiv e$. □

4. Computing generators for $H \cap K$

A group is said to have the Howson property if the intersection of any two finitely generated subgroups is again finitely generated. It is known that free groups have

the Howson property. If $H=\langle U\rangle$ and $K=\langle V\rangle$ are subgroups of $F=\langle S;\emptyset\rangle$ with cardinalities $\|V\|=m$ and $\|U\|=l$, respectively, then $G=H\cap K$ is generated by a set W with cardinality $\|W\|\leq 2\cdot(l-1)(m-1)+1$. There are different proofs of this fact [3, 4, 5] but no explicit algorithm for computing a set of generators is given there. We will modify Algorithm INTERSECT to get a polynomial time algorithm for computing from U, V a set W of generators for $G=H\cap K$.

From Lemma 3.1 we can deduce a bound on the U-length of the $w\in W$. This gives a new—combinatorial—proof for the fact that free groups have the Howson property.

4.1. Lemma. *Let U, V be N-reduced.*

(a) *There is a set $W\subset \underline{S}^*$ such that $\langle W\rangle = H\cap K$ and $|w|_U<2\alpha(V, U)$ for all $w\in W$.*

(b) *Free groups have the Howson property.*

Proof. Since (a) implies (b) we have only to prove (a). If $x\in H\cap K$, then there is a $w\in \underline{U}^*$ freely reduced in $\underline{U}$ such that $x=w$ in F and $w\in K$. By Lemma 3.1 with $u\equiv v\equiv e$, if $|w|_U\geq\alpha(V, U)$, then w is a product $w=w'w''$ in F with w', $w''\in \underline{U}^*$ and $w''\in K$, so w', $w''\in H\cap K$. Furthermore, we have $|w'|_U<2\alpha(V, U)$ and $|w''|_U<|w|_U$. Repeating this argument we get that w is a product $w=w_1\ldots w_q$ in F with $w_i\in H\cap K$, $w_i\in \underline{U}^*$ and $|w_i|_U<2\cdot\alpha(V, U)$. This proves (a). □

To compute a set W of generators for $G=H\cap K$ we organize the set $M_0=\{w\in \underline{U}^*\mid w$ freely reduced in $\underline{U}$, $|w|_U<2\alpha(V, U)\}$ in a tree T_0 as in Section 3. To traverse the whole tree T_0 and collect all nodes w with $w\in K$ costs too much time. So we have to develop a search strategy that avoids to visit all nodes but still leads to a set W such that $\langle W\rangle=G$.

Suppose we traverse T_0 breadth first and actually visit node w.

- If $g_V(w)\notin \mathrm{SP}(V, U)$, then no descendant of w is an element of K by Lemma 3.2 with $u\equiv v\equiv e$. So the subtree with root w is cancelled.
- If $g_V(w)\equiv e$, then $w\in K$ and we put w into W. We are looking for a small set W of generators for G. If a descendant $w_0\equiv ww'$ of w is in K, then w, w' are of shorter U-length than w_0 and both are in K. If w, $w'\in W$, we have $w_0\in\langle W\rangle$. So we cancel the subtree with root w in this case.
- If $g_V(w)\in \mathrm{SP}(V, U)-\{e\}$, then we distinguish whether a node v with $g_V(v)\equiv g_V(w)$ has been visited earlier or not. If so, we have $w\bar{v}^1\in K$, put $w\bar{v}^1$ into W and cancel the subtree with root w. Otherwise the search in this subtree must go on.

Notice that this strategy guarantees $\langle W\rangle\leq G$; it remains to prove $G\leq\langle W\rangle$.

The exact algorithm is given below. As in Section 3 we do not build up the whole tree T_0. Instead we maintain a list L with entries $(w, g_V(w))$ for any node w that is or has to be visited. Again, the pth element of L is $L_p=(L_p', L_p'')$, i points to the actual list element and j points to the currently last list element. The search stops if $i>j$, i.e., if there are no more nodes to be visited.

Algorithm GENERATORS
Input: U, V N-reduced.
Output: $W \subset \underline{U}^*$ a set of generators for G.
Method:

```
(1)  L_1 ⇐ (e, e); W ⇐ ∅;
(2)  i ⇐ 1; j ⇐ 1;
(3)  while i ≤ j do
(4)    begin for all z ∈ U with L_i' does not end with z̄^1 do
(5)      begin x ⇐ L_i' z; y ⇐ g_V(L_i'' z);
(6)        if y ∈ SP(V, U) then
(7)        if y ≡ e then W ⇐ W ∪ {x}
(8)                 else if ∃k ≤ j: L_k'' ≡ y
(9)                      then W ⇐ W ∪ {x L_k'^{-1}}
(10)                     else j ⇐ j + 1; L_j ⇐ (x, y)
(11)     end;
(12)     i ⇐ i + 1
(13)   end
```

We prove that the algorithm always stops and gives a set of generators for G as output.

4.2. Theorem. *Let* $U = \{u_1, \ldots, u_l\}$, $V = \{v_1, \ldots, v_m\}$ *be N-reduced,* $|u_i|, |v_i| \leq n$ *and* $H = \langle U \rangle$, $V = \langle K \rangle$. *Algorithm* GENERATORS *computes a set* W *of generators for* $G = H \cap K$ *in time* $O(l^3 m^2 n^5)$.

Proof. We first prove the time bound. If v, w are in the list L and $v \neq w$, then $g_V(v) \neq g_V(w)$ and $g_V(v), g_V(w) \in \mathrm{SP}(V, U)$. So L cannot become longer than $\alpha(V, U)$ and hence the **while**-loop is executed at most $\alpha(V, U)$ times. In line (4) there are at most $2 \cdot l$ z's to be considered. Line (5) costs $O(mn^2)$, line (6) costs $O(n \cdot \alpha(V, U))$ and line (8) costs $O(n \cdot \alpha(V, U))$. So one pass through the **while**-loop costs $O(l \cdot (mn^2 + \alpha(V, U)n))$. Since $\alpha(V, U) \leq (ln + 1) \cdot (mn + 1) = O(lmn^2)$, the total cost is $O(l^3 m^2 n^5)$. W has at most $l \cdot \alpha(V, U) = O(l^2 mn^2)$ elements and these have U-length less than $2\alpha(V, U)$.

The only thing which remains to be proved is that $G \leq \langle W \rangle$. Let $x \in \underline{U}^* \cap K$, we prove that $x \in \langle W \rangle$. Suppose this is not the case and let $x \in \underline{U}^* \cap K$ be minimal according to our order $<$ with $x \notin \langle W \rangle$. Then $x \neq e$ and $x \equiv z_1 \ldots z_p$, $z_i \in \underline{U}^*$, $z_i \neq z_{i+1}^{-1}$. Let $x_q \in \underline{U}^*$ be a maximal prefix of x which is in the list and $x \equiv x_q z u$, $z \in \underline{U}$, $u \in \underline{U}^*$. Then $0 \leq |x_q|_U < p$ and $g_V(x_q z) \in \mathrm{SP}(V, U)$ but $x_q z$ is not added to the list. This leads to two possible cases:

(i) $x_q z \in K$ and so $x_q z \in W$, or

(ii) $\exists x_i \in \underline{U}^*$ in the list with $x_i < x_q z$ and $x_q z \bar{x}_i^{-1} \in K$ so that $x_q z \bar{x}_i^{-1} \in W$.

In case (i), $x = x_q z u \in K$ and $x_q z \in K$ so $u \in K$. But $|u|_U < p$ and the minimality of x leads to $u \in \langle W \rangle$ which means $x \in \langle W \rangle$. In case (ii), $x = x_q z x_i^{-1} x_i u \in K$ and $x_q z x_i^{-1} \in K$

so $x_i u \in K$. But $x_i u < x$, which means $x_i u \in \langle W \rangle$. Together with $x_q z x_i^{-1} \in W$ this again gives $x \in \langle W \rangle$. In both cases we have a contradiction to $x \notin \langle W \rangle$ and so $G = \langle W \rangle$. □

One can prove a type of minimality condition for W: If $x \in \underline{U}^* \cap K$ is freely reduced, then x is a product of elements $w \in W$ with $|w|_U \leq |x|_U$. So the generators in W are of minimal U-length.

By Theorem 4.2 we can compute a presentation for the intersection of two subgroups. This immediately leads to an algorithm to compute a representation for the intersection of cosets.

4.3. Corollary. *There is a polynomial time algorithm to compute a representation for $Hx \cap yK$ if $U, V \subset \underline{S}^*$ with $H = \langle U \rangle$, $K = \langle V \rangle$ are given.*

Proof. With Algorithm INTERSECTION we can decide whether there is a $w \in Hx \cap yK$ and in the positive case determine such a w. If such a w does not exist, then $Hx \cap yK = \emptyset$. If $w \in Hx \cap yK$, then $Hx = Hw$ and $yK = wK$, so $Hx \cap yK = Hw \cap wK = (H \cap wK\bar{w}^1)w$. With Algorithm GENERATORS we can compute a finite set of generators for $H \cap \bar{w}^1 Kw$. □

5. Conjugacy problems

In Section 3 we studied the intersection problem for cosets, i.e., whether $Hx \cap yK \neq \emptyset$, and in Section 4 we gave an algorithm to compute a representation for $Hx \cap yK$. Now we are interested in the equality problem for cosets, i.e., whether $Hx = yK$. Furthermore, we want to characterize for fixed H and K the set of solutions (x, y) such that $Hx = yK$. Since $Hx = yK \Leftrightarrow \bar{x}^1 Hx = K \wedge y \in Hx$, the equation $Hx = yK$ is solvable iff $\bar{x}^1 Hx = K$ is solvable. So, we are led to the conjugacy problem for subgroups

$$\text{CONJUG}(U, V) \Leftrightarrow \exists x \in \underline{S}^*: \bar{x}^1 Hx = K.$$

There is a well-known algorithm of Moldavanskii [7, 5] for this problem, but it runs in exponential time. Here we refine the arguments of Moldavanskii to get polynomial time bounds. It so happens that all considerations that lead to a test whether $\exists x: \bar{x}^1 Hx = K$ also lead to a test whether $\exists x: \bar{x}^1 Hx \leq K$. So we first study the problem

$$\text{CONJUG}^+(U, V) \Leftrightarrow \exists x \in \underline{S}^*: \bar{x}^1 Hx \leq K.$$

We want first to characterize the 'short' solutions w of $\bar{w}^1 Hw \leq K$ and then characterize all solutions in terms of the 'short' ones.

5.1. Lemma. *Let $H = \langle U \rangle$ and $K = \langle V \rangle$, where V is N-reduced and $u_1 \in H$, $u_1 \neq \varepsilon$ in F. If $w_1^{-1} H w_1 \leq K$, then there exist a $k \in K$ and a $w_0 \equiv uz$ where u is a prefix of u_1 or u_1^{-1} with $|u| \leq \frac{1}{2}|u_1|$ and $\bar{z}^1 \in \text{SPREF}(V)$ such that $w_1^{-1} H w_1 = (w_0 k)^{-1} H (w_0 k)$ and hence $w_0^{-1} H w_0 \leq K$.*

Proof. For $x \in K$ let $\varphi(x)$ be the minimal V-length of any $y \in \underline{V}^*$ such that $x = y$ in F. From $w_1^{-1} H w_1 \leq K$ we have $w_1^{-1} u_1 w_1 \in K$ and $w_1 \in H w_1 K$. We restrict the set of all solutions w of $\bar{w}^{-1} H w \leq K$ by defining

$$M_1 = \{w \in \underline{S}^* \mid \bar{w}^{-1} H w \leq K,\ w \in H w_1 K\},$$

$$M_2 = \{w \in M_1 \mid \varphi(\bar{w}^{-1} u_1 w) \leq \varphi(\bar{v}^{-1} u_1 v) \text{ for all } v \in M_1\},$$

$$M_3 = \{w \in M_2 \mid |w| \leq |v| \text{ for all } v \in M_2\}.$$

Clearly, $M_3 \subset M_2 \subset M_1$ and $M_3 \neq \emptyset$ since $w_1 \in M_1 \neq \emptyset$. Let $w_0 \in M_3$, so w_0 is freely reduced. Since $w_0 \in M_1$, there are $h \in H$, $k \in K$ with $w_0 k = h w_1$ in F. This gives $\bar{w}_1^{-1} H w_1 = (h w_1)^{-1} H (h w_1) = (w_0 k)^{-1} H (w_0 k)$.

Let $w_0 \equiv uz$, where u is the maximal common prefix of w_0 and u_1 or u_1^{-1}. We assume that u is a prefix of u_1; the other case is similar. We prove the lemma by showing that $|u| \leq \frac{1}{2}|u_1|$ and $\bar{z}^{-1} \in \text{SPREF}(V)$.

Suppose $|u| > \frac{1}{2}|u_1|$. Then $u_1 \equiv uy$ with $|y| < |u|$. Let $\hat{w} \equiv \bar{y}^{-1} z$, so $\hat{w} = \bar{u}_1^{-1} w_0$ in F. Since $w_0 \in M_1$ we have $w_0^{-1} H w_0 \leq K$ and $w_0 \in H w_1 K$. This gives $\hat{w}^{-1} H \hat{w} \leq K$ and $\hat{w} \in H w_1 K$ so $\hat{w} \in M_1$. Since $\hat{w}^{-1} u_1 \hat{w} = w_0^{-1} u_1 w_0$ in F we also have $\hat{w} \in M_2$. But $|\hat{w}| < |w_0|$ and this contradicts $w_0 \in M_3$. So $|u| > \frac{1}{2}|u_1|$ is impossible.

We have $w_0^{-1} u_1 w_0 \equiv \bar{z}^{-1} \bar{u}^{-1} u_1 u z$. Since $|u| \leq \frac{1}{2}|u_1|$, the free reduction ρ gives $\rho(w_0^{-1} u_1 w_0) \equiv \bar{z}^{-1} x z$, where $x \equiv \rho(\bar{u}^{-1} u_1 u) \neq e$. Since $w_0^{-1} u_1 w_0 \in K$, there are $z_1, \ldots, z_p \in \underline{V}$ such that $\bar{z}^{-1} x z = z_1 \ldots z_p$ in F and $z_1 \ldots z_p$ is freely reduced in $\underline{V}$. This implies that an isolated prefix of z_1 is a prefix of $\bar{z}^{-1} x z$. If $|z| > \frac{1}{2}|z_1|$, then this isolated prefix is a prefix of $\bar{z}^{-1}$ and so also a prefix of z_p^{-1}, which means $z_1 \equiv z_p^{-1}$. Let $\hat{w} \equiv w_0 z_1$; then $\hat{w}^{-1} H \hat{w} = z_1^{-1} w_0^{-1} H w_0 z_1 \leq z_1^{-1} K z_1 = K$ and $\hat{w} \equiv w_0 z_1 \in H w_1 K z_1 = H w_1 K$, hence $\hat{w} \in M_1$. Now $\hat{w}^{-1} u_1 \hat{w} = z_2 \ldots z_{p-1}$ in F and so $\varphi(\hat{w}^{-1} u_1 \hat{w}) = p - 2 < p = \varphi(w_0^{-1} u_1 w_0)$, which contradicts $w_0 \in M_2$. So $|z| > \frac{1}{2}|z_1|$ is impossible, hence $|z| \leq \frac{1}{2}|z_1|$ and $\bar{z}^{-1}$ is a prefix of z_1, so $\bar{z}^{-1} \in \text{SPREF}(V)$. □

We notice two facts about Lemma 5.1 and its proof. The first fact is that $w_1^{-1} H w_1 \leq K$ iff $w_0^{-1} H w_0 \leq K$. So $\bar{w}^{-1} H w \leq K$ has a solution w iff there is a w_0 of the given form with $w_0^{-1} H w_0 \leq K$. The second fact is that all arguments go through if we consider the equation $\bar{w}^{-1} H w = K$ instead of $\bar{w}^{-1} H w \leq K$. This gives the following lemma.

5.2. Lemma. *Let $H = \langle U \rangle$, $K = \langle V \rangle$, where V is N-reduced and $u_1 \in H$, $u_1 \neq e$ in F and let*

$$M = \{uz \mid u \text{ a prefix of } u_1 \text{ or } \bar{u}_1^{-1} \text{ with } |u| \leq \tfrac{1}{2}|u_1|,\ \bar{z}^{-1} \in \text{SPREF}(V)\}.$$

Then

$$\exists w \in \underline{S}^*: \bar{w}^{-1} H w \leq K \quad \textit{iff} \quad \exists w \in M: \bar{w}^{-1} H w \leq K,$$

$$\exists w \in \underline{S}^*: \bar{w}^{-1} H w = K \quad \textit{iff} \quad \exists w \in M: \bar{w}^{-1} H w = K.$$

Now we can prove the main result of this section

5.3. Theorem. *The following problems are solvable in polynomial time*:

$$\text{EQCOS}(x, y, U, V) \Leftrightarrow Hx = yK,$$

$$\text{EQRCOS}(x, y, U, V) \Leftrightarrow Hx = Ky,$$

$$\text{EQCOS}^*(U, V) \Leftrightarrow \exists x, y: Hx = yK,$$

$$\text{EQRCOS}^*(U, V) \Leftrightarrow \exists x, y: Hx = Ky,$$

$$\text{CONJUG}(U, V) \Leftrightarrow \exists x: \bar{x}^{-1}Hx = K,$$

$$\text{CONJUG}^+(U, V) \Leftrightarrow \exists x: \bar{x}^{-1}Hx \leq K.$$

Proof. It is easy to see that, for any $x, y \in \underline{S}^*$,

$$Hx = yK \Leftrightarrow \bar{x}^{-1}Hx = K \wedge y\bar{x}^{-1} \in H,$$

$$Hx = Ky \Leftrightarrow H = K \wedge y\bar{x}^{-1} \in H.$$

In [2] it was shown that the generalized word problem ($x \in \langle U \rangle$?), the equality problem ($\langle U \rangle = \langle V \rangle$?), and the subgroup problem ($\langle U \rangle \leq \langle V \rangle$?) are solvable in polynomial time. This proves that EQCOS and EQRCOS are solvable in polynomial time. For the problems CONJUG and CONJUG$^+$ we refer to Lemma 5.2 and the fact that the cardinality of M is polynomial in the length of U, V. The problems EQCOS* and EQRCOS* are solvable in polynomial time since we have EQCOS*$(U, V) \Leftrightarrow$ CONJUG(U, V) and EQRCOS*$(U, V) \Leftrightarrow H = K$. □

By Theorem 5.3 it is decidable in polynomial time whether $\exists w: \bar{w}^{-1}Hw = K$ and whether $\exists w: \bar{w}^{-1}Hw \leq K$. We want to compute a representation for the solutions w. To do this we recall the definition of the normalizer $N(H)$ of H in the free group F

$$N(H) = \{w \mid \bar{w}^{-1}Hw = H\}.$$

It is easy to see that $N(H)$ is a subgroup of F containing H. Now, if $w_1^{-1}Hw_1 = K$ and $w_2^{-1}Hw_2 = K$, then $w_1^{-1}Hw_1 = w_2^{-1}Hw_2$ and so $w_1w_2^{-1} \in N(H)$. Hence, if $w_0^{-1}Hw_0 = K$, then for any $w \in \underline{S}^*$ we have $\bar{w}^{-1}Hw = K$ iff $w \in N(H)w_0$. This characterizes the solutions w of $\bar{w}^{-1}Hw = K$.

To characterize the solutions of $\bar{w}^{-1}Hw \leq K$ let $\{w_1, \ldots, w_q\} = \{w \in M \mid \bar{w}^{-1}Hw \leq K\}$, where M is as in Lemma 5.2. By Lemma 5.1 and the considerations above for any $w \in \underline{S}^*$ we have $\bar{w}^{-1}Hw \leq K$ iff $w \in N(H)w_1K \cup \cdots \cup N(H)w_qK$. So, if we can compute a set of generators for the normalizer $N(H)$ we have a representation for all solutions w of $\bar{w}^{-1}Hw = K$ and of $\bar{w}^{-1}Hw \leq K$.

Our algorithm for computing a set of generators for $N(H)$ is based on the following lemma.

5.4. Lemma. *Let $H = \langle U \rangle \neq \langle e \rangle$ where U is N-reduced and $u_1 \in U$ and let $V = \{uz \mid u$ is a small prefix of u_1 or $\bar{u}_1^{-1}$, $z^{-1} \in \text{SPREF}(U), (uz)^{-1}H(uz) = H\}$. Then $N(H) = \langle U \cup V \rangle$.*

Proof. Clearly, $\langle U \cup V\rangle \leq N(H)$. So it remains to show $N(H) \leq \langle U \cup V\rangle$. We assume this is false and repeat the arguments of the proof to Lemma 5.1 to show that this assumption leads to a contradiction.

Notice that $\bar{x}^{-1}u_1 x \in H$ for all $x \in N(H)$. For any $y \in H$ let $\varphi(y)$ be the minimal U-length of any $w \in \underline{U}^*$ such that $y = w$ in F. Let

$$M_1 = \{x \in N(H) \mid x \notin \langle U \cup V\rangle\} \neq \emptyset,$$

$$M_2 = \{x \in M_1 \mid \varphi(\bar{x}^{-1}u_1 x) \leq \varphi(\bar{y}^{-1}u_1 y) \text{ for all } y \in M_1\},$$

$$M_3 = \{x \in M_2 \mid |x| \leq |y| \text{ for all } y \in M_2\}.$$

Since $M_1 \neq \emptyset$, we have $M_3 \neq \emptyset$. Let $x \in M_3$ and $x \equiv uz$ where u is the maximal common prefix of x and u_1 or $\bar{u}_1^{-1}$. We assume u is a prefix of u_1, so $u_1 \equiv uy$. If $|y| < |u|$, then $\hat{x} \equiv \bar{y}^{-1}z$ is in M_2 and shorter than x. This contradicts $x \in M_3$ and so $|u| \leq |y|$, which means that u is a small prefix of u_1. Now $\rho(\bar{x}^{-1}u_1 x) \equiv \bar{z}^{-1}yz$ where $y \equiv \rho(\bar{u}^{-1}u_1 u) \neq e$. Since $\bar{x}^{-1}u_1 x \in H$, we have $\bar{z}^{-1}yz = z_1 \ldots z_p$ in F, where $z_1 \ldots z_p \in \underline{U}^*$ is freely reduced in $\underline{U}$. Exactly as in the proof of Lemma 5.1 we get that $\bar{z}^{-1}$ is a small prefix of z_1, so $\bar{z}^{-1} \in \text{SPREF}(U)$. Now we have proved $x \in M_3$ and $x \equiv uz \in V$. This is a contradiction, since $x \in M_3$ implies $x \in M_1$ and so $x \notin \langle U \cup V\rangle$.

The only assumption $M_1 \neq \emptyset$ has led to a contradiction, so $N(H) \leq \langle U \cup V\rangle$ is true and Lemma 5.4 is proved. □

There is only a polynomial number of words $w \equiv uz$ with u a small prefix of u_1 or $\bar{u}_1^{-1}$ and $\bar{z}^{-1} \in \text{SPREF}(U)$. For each such w the test whether $\bar{w}^{-1}Hw = H$ is polynomial. So we have the following theorem.

5.5. Theorem. *Let $H = \langle U\rangle$. There is a polynomial time algorithm to compute a set of generators for the normalizer $N(H)$ of H in F.*

We also have the following theorem.

5.6. Theorem. *Let $H = \langle U\rangle$, $K = \langle V\rangle$ and $H \neq \langle e\rangle$.*

$A = \{\bar{w}^{-1} \in \underline{S}^* \mid \bar{w}^{-1}Hw = K\}$ is either empty or a coset $N(H)w_0$.

$B = \{\bar{w}^{-1} \in \underline{S}^* \mid \bar{w}^{-1}Hw \leq K\}$ is either empty or a finite union of double cosets $N(H)w_i K$, $i = 1, \ldots, q$.

There are polynomial time algorithms to compute a representation for A and for B.

Proof. We may assume that U and V are N-reduced. Let M be as in Lemma 5.2.

(a) We can test in polynomial time whether there is a $w_0 \in M$ such that $w_0^{-1}Hw_0 = K$ and in the positive case find such a w_0. In the negative case we have $A = \{w \mid \bar{w}^{-1}Hw = K\} = \emptyset$ by Lemma 5.2. In the positive case, if $w \in A$, then $\bar{w}^{-1}Hw = K = w_0^{-1}Hw_0$, so $ww_0^{-1} \in N(H)$ and $w \in N(H)w_0$. On the other hand, if $w \in N(H)w_0$, then $w = zw_0$ in F with $z \in N(H)$ and so $\bar{w}^{-1}Hw = \bar{w}_0^{-1}\bar{z}^{-1}Hzw_0 = \bar{w}_0^{-1}Hw_0 = K$, so $w \in A$. This proves $A = N(H)w_0$. By Theorem 5.5 we can compute a set of generators for $N(H)$ in polynomial time.

(b) We can compute in polynomial time the set $M' = \{w \in M \mid \bar{w}^1 Hw \leq K\}$. If $M' = \emptyset$, then $\{w \in \underline{S}^* \mid \bar{w}^1 Hw \leq K\} = \emptyset$. Assume $M' = \{w_1, \ldots, w_q\} \neq \emptyset$. We claim $\{w \in \underline{S}^* \mid \bar{w}^1 Hw \leq K\} = N(H)w_1 K \cup \cdots \cup N(H)w_q K$. If $\bar{w}^1 Hw \leq K$, then by Lemma 5.1 there is a $1 \leq i \leq q$ and a $k \in K$ such that $\bar{w}^1 Hw = (w_i k)^{-1} H(w_i k)$, so $w(w_i k)^{-1} \in N(H)$ and hence $w \in N(H)w_i K$. If $w \in N(H)w_i K$ for some i, then $w = zw_i k$ in F for some $z \in N(H)$, $k \in K$. This gives $\bar{w}^1 Hw = \bar{k}^1 w_i^{-1} \bar{z}^1 Hzw_i k = \bar{k}^1 \bar{w}_i^1 Hw_i k \leq \bar{k}^1 Kk = K$. So the claim is proved. Since we can compute a set of generators for $N(H)$ in polynomial time we have a representation for $\{w \mid \bar{w}^1 Hw \leq K\}$. □

6. P-complete problems

All the decision problems considered in the previous sections turned out to be in P, the class of problems solvable in polynomial time on a TM. So an upper bound for the complexity of these problems is known. Since the word problem ($x = e$ in F?) is in LogSpace [6], the class of problems solvable on logarithmic space on a TM, and since LogSpace $\subset$ P, the question comes up whether some of our problems are in LogSpace. We will prove that any of our problems is P-complete under log-space reducibility and so is in LogSpace only if P = LogSpace.

We use a construction from [2] that allows one to reduce any problem in P to a subgroup problem in a free group.

6.1. Fact. *Let Z be a polynomial time bounded* TM. *There is a free group $F = \langle S; \emptyset \rangle$ such that for any input y to Z a letter $s(y) \in S$ and a finite set $U(y) \subset \underline{S}^*$ are log-space computable with*

$$Z \text{ accepts } y \Leftrightarrow s(y) \in \langle U(y) \rangle,$$

$$Z \text{ rejects } y \Leftrightarrow U(y) \cup \{s(y)\} \text{ is independent.}$$

Now we can prove the following theorem.

6.2. Theorem. *The problems* Icos, Ircos, Isubg, Eqcos, Eqrcos, Eqcos*, Eqrcos*, Conjug *and* Conjug$^+$ *are* P*-complete under log-space reducibility.*

Proof. Since all the problems are in P, it is enough to show that any polynomial time recognizable language L can be reduced to each of our problems. Let L be such a language and Z a polynomial time TM which recognizes L. By Fact 6.1 we have

$$\begin{aligned} y \in L &\Leftrightarrow \text{Icos}(s(y), e, U(y), U(y)) \\ &\Leftrightarrow \text{Ircos}(s(y), e, U(y), U(y)) \\ &\Leftrightarrow \text{Isubg}(U(y), \{s(y)\}) \end{aligned}$$

$$\Leftrightarrow \text{EQCOS}(s(y), e, U(y), U(y))$$

$$\Leftrightarrow \text{EQRCOS}(s(y), e, U(y), U(y))$$

$$\Leftrightarrow \text{EQCOS}^*(U(y), U(y) \cup \{s(y)\})$$

$$\Leftrightarrow \text{EQRCOS}^*(U(y), U(y) \cup \{s(y)\})$$

$$\Leftrightarrow \text{CONJUG}(U(y), U(y) \cup \{s(y)\})$$

$$\Leftrightarrow \text{CONJUG}^+(U(y) \cup \{s(y)\}, U(y)).$$

So L is log-space reducible to each of our problems and hence the problems are P-complete. □

7. Conclusion

Combinatorial arguments are strong enough to prove interesting results in free groups. They have the advantage of being constructive in the sense that they lead to efficient algorithm for deciding problems and to compute a representation for all solutions of certain equations.

In this paper we studied the solvability of

$$\exists h \in H, k \in K: hx = yk \text{ in } F, \qquad \exists w \in F: \bar{w}^1 Hw = K,$$

where H and K are subgroups of a free group F. The first problem is related to the question whether the intersection $Hx \cap yK$ is empty or equivalently whether the double cosets HxK and HyK are equal. We developed a polynomial time algorithm to compute a set of generators for $H \cap K$ and used it to compute a representation (coset) for $Hx \cap yK$. As by-product a new proof is given that the free groups have the Howson property.

The second problem is the conjugacy problem of Moldavanskii. We developed a polynomial time decision algorithm and used it to decide whether two cosets Hx and yK are equal. We also gave a polynomial time algorithm for computing a generating set for the normalizer $N(H)$ of a subgroup H and used it to compute a representation for all solutions w of $\bar{w}^1 Hw = K$ and of $\bar{w}^1 Hw \leq K$.

All the decision problems are solvable in polynomial time. To get a lower bound for the complexity of the problems, we could show that all the problems are P-complete under log-space reducibility. So they are solvable on logarithmic space only if P = LOGSPACE.

References

[1] J. Avenhaus and K. Madlener, How to compute generators for the intersection of subgroups in free groups, *CAAP 1981*, Lecture Notes in Comput. Sci. **112** (Springer, Berlin, 1981) pp. 88–100.

[2] J. Avenhaus and K. Madlener, The Nielsen reduction and P-complete problems in free groups, *Theoret. Comput. Sci.* **32** (1, 2) (1984) 61–76.
[3] A.G. Howson, On the intersection of finitely generated free groups, *J. London Math. Soc.* **29** (1954) 428–434.
[4] W. Imrich, On finitely generated subgroups of free groups, *Arch. Math.* **28** (1977) 21–24.
[5] R.C. Lyndon and P.E. Schupp, *Combinatorial Group Theory* (Springer, Berlin, 1977).
[6] R.J. Lipton and Y. Zalcstein, Word problems solvable in logspace, *J. ACM* **24** (1977) 522–526.
[7] D.J. Moldavanskii, Conjugacy of subgroups of a free group, *Algebra i Logika* **8** (1969) 394–395.
[8] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory* (Dover Publications, New York, 1976).