Word Problems Solvable in Logspace

Richard J. Lipton and Yechezkel Zalcstein

Research Report #60

January 1976

Part of this work was performed while Lipton was a visitor at the IBM Watson Research Center at Yorktown Heights. The research was also supported in part by the National Science Foundation under Grant DCR-75-01998 and by the Office of Naval Research under Grant N00014-75-C-0752.

1. Introduction

Ritchie and Springsteel [14] have proved that the one-sided Dyck language (the set of all well-formed expressions over two pairs of matching left and right parentheses) has deterministic logspace complexity. Surprisingly, the argument, based on a "level trick," does not easily generalize to the two-sided Dyck language (where parentheses may balance on either side), even when nondeterminism is allowed.

In this paper we show that the two-sided Dyck language does indeed have deterministic logspace complexity. We actually prove a general theorem that the word problem for a group of matrices over a field (i.e. a linear group) is solvable in logspace. The result follows since the membership problem for the Dyck language is equivalent to the word problem for free groups, and free groups are representable as groups of matrices over a field of characteristic zero.

The *word problem* for a group is the problem of deciding whether a product of group elements is equal to the identity element. It is a well-known theorem; Novikov and Boone proved independently that the word problem for finitely presented groups is recursively unsolvable, and Boone and Clapham showed that it can have any preassigned recursively enumerable degree. (See the exposition in Rotman [15a].) But Rabin [13] has stated without proof that the word problem is solvable for groups of matrices over a field. To our knowledge, no proof of this theorem has been published. Our main result is a strong refinement of Rabin's theorem stating that the word problem for groups and even semigroups of matrices over a field is solvable in logspace. As a corollary, we obtain Rabin's result.

Since several classes of groups such as free groups and polycyclic groups have representations by matrices over the integers, we obtain as an immediate corollary that the word problem for these groups is solvable in logspace. This extends and sharpens results of Cannonito's and Gatterdam's [4,5], where these word problems were shown to be elementary recursive.

The *conjugacy problem* for a group G is the problem of deciding for an arbitrary pair of words u,v in G whether there exists $w \in G$ such that $u = w^{-1}vw$ in G. The word problem is the special case of the conjugacy problem where v = 1. Miller [11] has shown that the conjugacy problem is unsolvable for finitely generated linear groups. Thus the class of linear groups has the property that the word problem is ε_*^0-solvable but the conjugacy problem is unsolvable. This is related to a problem posed by Boone [4].

Another application is the construction of context-free languages of logspace complexity. Finally, we show that Schützenberger F-recognizable languages [17] have logspace complexity.

2. Preliminaries

Definition: A *presentation* of a finitely generated group G is an ordered pair (X,D) where $X = \{x_1,\ldots,x_m\}$ is a finite set of generators and D is a set of words over $X \cup \{x_1^{-1},\ldots,x_m^{-1}\}$ such that G is isomorphic to the quotient group formed by the free group on X modulo the normal subgroup generated by the words in D.

Let (X,D) be a presentation of a group G. The *word problem* for (X,D) is the problem of deciding whether an arbitrary word w over the alphabet $X \cup \{x_1^{-1},\ldots,x_m^{-1}\}$ reduces to the identity element of G. In particular, the word problem for the free group is: Given a word w over $X \cup \{x_1^{-1},\ldots,x_m^{-1}\}$, find whether w can be reduced to the empty word by applications of the rules

1) $x_i x_i^{-1}$ can be replaced by $\wedge$, the empty word $(i = 1,\ldots,m)$
2) $x_i^{-1} x_i$ can be replaced by $\wedge$.

The word problem for (X,D) is solvable in logspace provided that it can be solved by a deterministic Turing machine with a two-way read-only input tape and a working tape

bounded in length by log n where n is the length of the input. Our main result, Corollary 1, is that the word problem for a free group is solvable in logspace.

The following results from number theory are needed in the proof of Theorem 1.

Definition: $\mu(n) = \prod_{p \le n} p$, p a prime.

Lemma 1: There is a constant $c_1 > 0$ such that $\mu(n) > 2^{c_1 n}$.

Proof: Hardy and Wright [7] show that $\log \mu(n) > An$. The result then follows. □

Lemma 2: Let x be an integer such that $|x| < \mu(n)$. Then $x = 0$ if and only if, for all primes $p \le n$, $x \equiv 0 \bmod p$.

Proof: Assume that $x \equiv 0 \bmod p$ for all primes $p \le n$. Then $x \equiv 0 \bmod \mu(n)$, but since $|x| < \mu(n)$ it follows that $x = 0$. The converse is trivial. □

Definition: For any m×m matrix $A = (a_{ij})$, $1 \le i, j \le m$,

$$|A| = \sum_{i,j=1}^{m} |a_{ij}|.$$

Lemma 3: For any m×m matrices A and B, $A \cdot B \le m^2 |A||B|$ (where · denotes matrix product).

Proof: The absolute value of each element of AB is bounded from above by $|A||B|$. □

Lemma 4: For any m×m matrices $A_1, \ldots, A_n$, $|A_1 \cdot A_2 \cdot \ldots \cdot A_n| \le m^{2(n-1)} |A_1| \ldots |A_n|$.

Proof: By induction on n, applying Lemma 3. □

3. Main Result

Let F be a field.† A group is a *linear group over F* (or an F-linear group) provided it is isomorphic to a group of k×k invertible matrices over F for some positive integer k.

Theorem 1: The word problem for finitely generated linear groups over a field is solvable in logspace.

Before proving the theorem, we present the important application:

Corollary 1: The word problem for finitely generated free groups is solvable in logspace.

Proof of corollary: The free group on two generators x_1, x_2 is isomorphic to a group of 2×2 matrices over the field of rational numbers via the correspondence

$$x_1 \to \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} \qquad x_2 \to \begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix}$$

Furthermore, any finitely generated free group is isomorphic to a subgroup of the free group on two generators [15b]. □

Proof of theorem: The first reduction of the problem is, of course, replacing the word problem with the problem:

> Given a product $A_1 \cdot A_2 \cdot \ldots \cdot A_n$ of matrices over F, determine whether $A_1 \cdot A_2 \cdot \ldots \cdot A_n = I$ where I is the identity matrix.

We first solve the problem when the matrices are over the ring $\mathbb{Z}$ of integers.

Suppose that we consider the following problem:

> Given a sequence of k×k matrices $A_1, \ldots, A_n$ over $\mathbb{Z}$ with entries bounded by d, determine whether $A_1 \cdot A_2 \cdot \ldots \cdot A_n = I$ where k is fixed and $d = O(2^n)$.

---

† All fields considered here are of characteristic 0.

This problem can be done in logspace. Our algorithm (A_1) is:

> For each integer $q \leq c_3 n^2$ (c_3 is defined later), compute the product $A_1 \cdot A_2 \cdot \ldots \cdot A_n$ modulo q and test whether $A_1 \cdot A_2 \cdot \ldots \cdot A_n - I \equiv 0$ modulo q. If it is equal to 0 for all q, accept the input; otherwise, reject the input.

This algorithm operates in space bounded by $k^2(2 \log n + \log c_3)$. It also operates correctly: If $A_1 \cdot A_2 \cdot \ldots \cdot A_n - I = 0$, then it clearly accepts. On the other hand, if it accepts, then for all primes $p \leq c_3 n^2$, $A_1 \cdot A_2 \cdot \ldots \cdot A_n - I \equiv 0$ modulo p. Let $B = A_1 \cdot A_2 \cdot \ldots \cdot A_n - I$. Then by lemma 4,

$$|B| \leq k^{2(n-1)} (k^2 d)^n \leq c_2^{n^2}$$

for some constant c_2. But by lemmas 1 and 2, B = 0 provided that

$$c_2^{n^2} < 2^{c_1 c_3 n^2},$$

which is clearly true for a sufficiently large c_3.

We now extend the algorithm A_1 to the case where the matrices A_i can have elements from $\mathbb{Z}[x_1,\ldots,x_m]$ where, for a commutative ring R, $R[x_1,\ldots,x_m]$ denotes the set of polynomials in the indetermines $x_1,\ldots,x_m$ having coefficients from R.

Let $f(x_1,\ldots,x_m)$ be a polynomial in $\mathbb{Z}[x_1,\ldots,x_m]$. f is a sum of monomials $x_1,\ldots,x_m$ with integer coefficients. Define the degree of the monomial

$$x_1^{i_1} \ldots x_m^{i_m}$$

to be

$$\sum_{j=1}^{m} i_j$$

and the degree of f to be the maximum of the degrees of the monomials in f having non-zero coefficients.

Consider the following problem:

> Given a sequence of k×k matrices $A_1,\ldots,A_n$ over $\mathbb{Z}[x_1,\ldots,x_m]$ such that all entries have degree at most g and have all coefficients bounded in absolute value by b, determine whether $A_1 \cdot A_2 \cdot \ldots \cdot A_n = I$ where m, k, g, and b are fixed.

This problem can be done in logspace. For each m-tuple $v = (v_1,\ldots,v_m)$ in $\mathbb{Z}^m$ and each matrix A with entries from $\mathbb{Z}[x_1,\ldots,x_m]$, let $\langle A\rangle_v$ be the integer matrix obtained from A by replacing each entry in A with its value (as a polynomial function) at the point v. Our algorithm (A_2) is then:

> For each m-tuple $v = (v_1,\ldots,v_m)$ with $0 \le v_j \le gn$, decide whether $\langle A_1\rangle_v \cdot \langle A_2\rangle_v \cdot \ldots \cdot \langle A_n\rangle_v = I$ by the algorithm A_1. If this algorithm accepts for all $(gn+1)^m$ m-tuples, accept the input; otherwise, reject it.

This algorithm requires only logspace. We need only check that the algorithm A_2 uses no more than O(log n) space. This follows since d is bounded by $b(gn+1)^m$. The correctness of the algorithm relies on the following elementary result from Lipton [10]:

> Suppose that $f(x_1,\ldots,x_m)$ is a polynomial of degree at most h. Then $f(x_1,\ldots,x_m) = 0$ for all integers $0 \le x_i \le h$ implies that $f(x_1,\ldots,x_m)$ is identically zero.

For any two matrices A,B over $\mathbb{Z}[x_1,\ldots,x_m]$ it follows that $\langle A\cdot B\rangle_v = \langle A\rangle_v \cdot \langle B\rangle_v$. Hence, if $A_1 \cdot A_2 \cdot \ldots \cdot A_n - I = 0$, then the algorithm accepts. Conversely, assume that the algorithm accepts. Let $B = A_1 \cdot A_2 \cdot \ldots \cdot A_n - I$. Then the algorithm proves that $\langle B\rangle_v = 0$ for all $v = (v_1,\ldots,v_m)$ with $0 \le v_i \le gn$. Now the maximum degree of an entry of B is gn. Thus, by Lipton's result, B = 0.

We can now complete the proof of the theorem. Let G be generated by the finite set $A_1,\ldots,A_\ell$ of k×k matrices over F. Then the elements of G are matrices over the field E generated by all the entries of the A_i's. Since E is generated by a finite set, E is a finitely generated extension of the prime subfield P of F. By field theory (Jacobson [9]), E is a finite algebraic extension of a transcendental extension $P[x_1,\ldots,x_m]$ of P (where the x_i's are indetermines). But since E is a finite dimensional algebra over $P[x_1,\ldots,x_m]$, it is isomorphic via the regular representation R (Jacobson [8a]) to an algebra of, say, t×t matrices over $P[x_1,\ldots,x_m]$. Furthermore, since E is a field, each of the matrices in the representation is invertible and they all commute. Thus by replacing each entry in each A_i by a t×t matrix over $P[x_1,\ldots,x_m]$ and identifying the resulting block matrices with kt×kt matrices over $P[x_1,\ldots,x_m]$, we see that G is isomorphic to a group of kt×kt matrices over $P[x_1,\ldots,x_m]$. Furthermore, by the formula for the determinant of a block matrix [8b], the matrices are invertible.

Since F has characteristic 0, P = $\mathbb{Q}$, the field of rational numbers. Let a be the least common multiple of the denominators of the coefficients of all the entries in the (finitely many) generating matrices. Multiplying all generators by a, we obtain a new set of generators that are matrices over $\mathbb{Z}[x_1,\ldots,x_m]$, and the result follows by using algorithm A_2. □

Remark: The argument used in the proof of this theorem with slight modifications shows more generally that the word problem is solvable in logspace for any *semigroup* of matrices over a field. Cannonito and Gatterdam [4,5] have investigated the computability level of the word problem for various classes of groups with respect to the Grzegorczyk hierarchy (ε_*^n) [6]. Our theorem yields sharper results.

Corollary 2: The word problem for polycyclic groups is solvable in logspace.

Proof: By a result of Auslander and Swan's [2], any polycyclic group is a linear group

over Z. □

Since as is well known the logspace-solvable predicates are a subset of the class ε_*^0 of Grzegorczyk's, Corollary 2 improves Cannonito and Gatterdam's desult that the word problem for polycyclic groups is ε_*^3-solvable.

It should be pointed out that our notion of ε_*^n-solvability is not equivalent to Cannonito's notion of ε_*^n-decidability, which is defined in relation to a *fixed* Gödel numbering of the free group on X ("standard indexing"), X being elementary recursive but of space complexity higher than logspace. Thus, strictly speaking, our results do not solve Cannonito's open problems on minimizing the degree of computability within the Grzegorczyk hierarchy, although they do solve modified versions of these problems.

Boone [3] has raised the question whether there exist finitely generated groups with word problem ε_*^α-decidable and conjugacy problem ε_*^β-decidable with $\beta > \alpha$. Since by our theorem the word problem for finitely generated subgroups of Z-linear groups is ε_*^0-solvable and by a result of Miller's [11] the conjugacy problem for finitely generated subgroups of Z-linear groups is unsolvable, the disparity between the word problem can be even greater than expected.

Let I be an index set and let G_i be groups with presentations (X_i,D_i), $i \in I$. Then the *free product* $\overset{*}{\Pi}_i G_i$ of the G_i's is the group with presentation

$$(\cup_i X_i, \cup_i D_i).$$

If I is finite, the free product is denoted by $G_i * \ldots * G_n$.

Definition: Let L be a language over an alphabet $\{x_1,x_1^{-1},\ldots,x_n,x_n^{-1}\}$. L is a *group kernel* if and only if there exists a presentation (X,D), $X = \{x_1,\ldots,x_n\}$ of a group G such that L is the normal subgroup generated by the words in D. Let L_1,L_2 be group kernels of G_1,G_2 respectively. The *free product* $L_1 * L_2$ will be the kernel of the homomorphism from

the free group $X_1 \cup X_2$ onto $G_1 * G_2$.

Theorem 2: The class of context-free languages that are group kernals of Z-linear groups is closed under finite free products.

Proof: By a theorem of Nixnevic's [12], the class of F-linear groups, for a fixed field F of characteristic zero, is closed under finite free products. Furthermore, by a theorem of Anisimov's [1], the class of context-free group kernels is closed under finite free products.

Theorems 1 and 2 can be used to construct a large number of examples of context-free languages that are recognizable in logspace. For example, the free product of any finite number of Dyck languages and regular group languages will be such a language. As a matter of fact, all known context-free languages that are group kernels are of this form, according to J. Sakarovitch [16].

In a final application, we observe that Schützenberger F-recognizable languages [17] have logspace complexity. The proof of our theorem can be adapted trivially to yield a logspace algorithm for determining membership in such a language.

Acknowledgements

We wish to thank Albert Meyer for posing the problem; Nancy Lynch for communicating it to us; Celia Wrathall for a number of helpful comments on the structure of the Grzegorczyk hierarchy; and Mary-Claire van Leunen for assistance in preparing the manuscript.

References

1] A. V. Anisimov.
Group languages.
Kibernetika 4:18-24, 1971.
Translated from the Russian in
Cybernetics 4:594-601, 1973.

2] Auslander and Swan.
Cited in Wehrfritz [18].

3] Boone.
Cited in Cannonito [4a].

4] F. B. Cannonito.
Hierarchies of computable groups and
and word problem.
Journal of Symbolic Logic 31:376-392,
1966.
[4a] page 391

5] F. B. Cannonito and R. W. Gatterdam.
The word problem for polycyclic
groups is elementary.
Compositio Mathematica 27:39-45,
1973.

6] A. Grzegorczyk.
Some classes of recursive functions.
Rozprawy Matematyczne 4:1-45.
Instytut Matematyczne, Akademia
Nauk, Warsaw, Poland, 1953.

7] G. H. Hardy and E. M. Wright.
*An Introduction to the Theory of
Numbers*, page 341.
Oxford University Press, fourth
edition, 1959.

8] N. Jacobson.
Basic Algebra.
W. H. Freeman, 1974.
[8a] Theorem 7.4
[8] page 407

9] N. Jacobson.
Lectures in Abstract Algebra, Volume
III, page 156.

10] R. J. Lipton.
Polynomials with 0-1 coefficients
that are hard to evaluate,
Lemma 4.
Conference Record of the 16th Annual
IEEE Symposium on Foundations of
Computer Science, 6-10, 1975.

11] C. F. Miller III
On group-theoretic division problems and
their classification.
Annals of Mathematics Studies #68,
Princeton University Press, 1971.

12] Nisnevic.
Cited in Wehrfritz [18].

13] M. O. Rabin.
Computable algebra, general theory and
theory of computable fields,
Theorem 5.
*Transactions of the American Mathematical
Society* 95:341-360, 1960.

14] R. W. Ritchie and F. N. Springsteel.
Language recognition by marking automata.
Information and Control.

15] J. Rotman.
The Theory of Groups: An Introduction.
Allyn and Bacon, second edition, 1973.
[15a] Chapter 12
[15b] page 262

16] J. Sakarovitch.
Private communication.

17] M. P. Schützenberger.
On the definition of a family of
automata.
Information and Control 4:245-270, 1961.

18] B. A. F. Wehrfritz.
Infinite Linear Groups, Chapter 2.
Springer, New York, 1973.