Word Problems Solvable in Logspace

RICHARD J. LIPTON

Yale University, New Haven, Connecticut

AND

YECHEZKEL ZALCSTEIN

State University of New York at Stony Brook, Stony Brook, New York

ABSTRACT Extending a result of Rabin, it is shown that the word problem for linear groups (groups of matrices) over a field of characteristic 0 is solvable in (deterministic) logspace As an application of this result, it follows that the word problem for free groups and hence the membership problem for the two-sided Dyck language are solvable in logspace

KEY WORDS AND PHRASES. word problems, linear groups, logspace

CR CATEGORIES 5 25

1. *Introduction*

Ritchie and Springsteel [13] 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 space complexity log(n). Surprisingly, as pointed out by Albert Meyer and communicated to us by Nancy Lynch, 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 one allows nondeterminism.

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 of characteristic zero (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 or not a product of group elements is equal to the identity element. It is a well-known theorem, proved independently by Novikov and Boone (see the exposition in [14, Ch. 12]), that the word problem for finitely presented groups is recursively unsolvable and in fact, as has been shown by Boone and Clapham, can have any preassigned recursively enumerable degree. However, Rabin [11, Th. 5] has stated without proof that the word problem is solvable for groups of matrices over a field. Rabin's unpublished proof actually shows that this word problem is solvable in polynomial time [12]. Our main result is a strong refinement of Rabin's theorem stating that the word problem for groups and even

Part of this work was performed while the first author was a visitor at the IBM Thomas J Watson Research Center at Yorktown Heights, N Y 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

Authors' present addresses R J Lipton, Department of Computer Science, Yale University, New Haven, Connecticut 06520, Y Zalcstein, Department of Mathematics, University of Southern California, Los Angeles, California 90007

semigroups of matrices over a field of characteristic zero is solvable in logspace. As a corollary, we obtain Rabin's result for fields of characteristic 0.

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 [3] and Cannonito and Gatterdam [4], 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 or not there exist $w \in G$ such that $u = w^{-1}vw$ in G. The word problem is the special case of the conjugacy problem where $v = 1$. Miller [10] 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 $\mathscr{E}^0_*$-solvable but the conjugacy problem is unsolvable. This is related to a problem posed by Boone [2].

As a final application we exhibit a large class of context-free languages of logspace complexity

2. *Preliminaries*

Definition. A *presentation* of a finitely generated group G is an ordered pair (X, D) where $X = \{x_1, \dots, x_m\}$ is a finite set of generators and D is a set of words over $X \cup \{x_1^{-1}, \dots, x_m^{-1}\}$ 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 $X \cup \{x_1^{-1}, \dots, x_m^{-1}\}$ reduces to the identity element of G In particular, the *word problem for the free group is*:

Given a word w over $X \cup \{x_1^{-1}, \dots, x_m^{-1}\}$, *find* whether or not w can be reduced to the empty word by applications of the following rules ($i = 1, \dots, m$): (1) $x_i x_i^{-1}$ can be replaced by $\wedge$, (2) $x_i^{-1}x_i$ can be replaced by $\wedge$, where b is the empty word.

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 6, 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 5

Definition. $\mu(n) = \Pi p, p \leq n$, p a prime (i.e. the product of all primes is less than or equal to n)

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

PROOF. In Hardy and Wright [6, p 341] it is shown 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 $p \leq n$, $x = 0 \bmod p$*

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

Definition. For any $m \times m$ matrix, $A = (a_{ij})$, $1 \leq i, j \leq m$, $|A| = \sum_{i,j=1}^{m} |a_{ij}|$.

LEMMA 3. *For any $m \times m$ matrices A and B, $|A \cdot B| \leq m^2 |A|\,|B|$ (where $\cdot$ denotes matrix product).*

PROOF The absolute value of each element of AB is bounded from above by $|A|\,|B|$. Actually it can be shown that $|AB| \leq |A|\,|B|$, but we do not need this sharper estimate □

LEMMA 4 *For any $m \times m$ matrices $A_1, \dots, A_n$,*

$$|A_1 \cdot A_2 \cdots A_n| \leq m^{2(n-1)} |A_1| \cdots |A_n| \,.$$

PROOF By induction on n, applying Lemma 3 □

3. *Main Results*

Let F be a field of characteristic zero. A group is a *linear group* over F (or an *F-linear* group) provided it is isomorphic to a group of $k \times k$ invertible matrices over F, for some positive integer k.

THEOREM 5. *The word problem for a finitely generated linear group over a field of characteristic zero is solvable in logspace.*

Before proving the theorem, we present the important application:

COROLLARY 6. *The word problem for finitely generated free groups is solvable in logspace.*

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

$$x_1 \rightarrow \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad x_2 \rightarrow \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

Furthermore, any finitely generated free group is isomorphic to a subgroup of the free group on two generators [14, p. 262]. □

PROOF OF THEOREM 5. The first reduction of the problem is of course replacing the word problem by the following problem:

Given: A product $A_1 \cdot A_2 \cdots A_n$ of matrices over F.

Determine: If $A_1 \cdot A_2 \cdots A_n = I$ where I is the identity matrix.

We first solve the problem when the matrices are over the ring Z of integers.

LEMMA 7. *Suppose we consider the following problem*:

Given: *A sequence of $k \times k$ matrices $A_1, \ldots, A_n$ over Z with entries bounded by d.*

Determine: *If $A_1 \cdot A_2 \cdots A_n = I$, where k is fixed and $d = O(2^n)$.*

Then this problem can be done in logspace.

PROOF. The algorithm is:

For each integer $q \leq c_3 n^2$ do the following (c_3 is defined later) Compute the product $A_1 \cdot A_2 \cdots A_n \bmod q$ and test whether or not $A_1 \cdot A_2 \cdots A_n - I \equiv 0 \bmod q$. If it is equal to 0 for all q, then accept the input; otherwise, reject the input.

This algorithm operates in space bounded by $k^2(2 \log n + \log c_3)$. Also, this algorithm operates correctly: If $A_1 \cdot A_2 \cdots A_n - I = 0$, then it clearly accepts On the other hand, if it accepts, then for all primes $p \leq c_3 n^2$, $A_1 \cdot A_2 \cdots A_n - I \equiv 0 \bmod p$. Let $B = A_1 \cdot A_2 \cdots A_n - I$. Then $|B| \leq |A_1 \cdot \cdots \cdot A_n| + |I| = |A_1 \cdot \cdots \cdot A_n| + n$ and thus, by Lemma 4, $|B| \leq k^{2(n-1)}(k^2 d)^n + n \leq (kc_2)^{4n} 2^{n^2}$ for some constant c_2. But by Lemmas 1 and 2, $B = 0$ provided that $(kc_2)^{4n} 2^{n^2} < 2^{c_1 c_3 n^2}$, which is clearly true for a sufficiently large c_3. □

We now extend this lemma to the case where the matrices A_i can have elements from $Z[x_1, \ldots, x_m]$, the ring of polynomials in the indeterminates $x_1, \ldots, x_m$ having integer coefficients.

Let $f(x_1, \ldots, x_m)$ be a polynomial in $Z\{x_1, \ldots, x_m\}$. f is a sum of monomials $x_1^{i_1} \cdots x_m^{i_m}$ with integer coefficients. Define the degree of $x_1^{i_1} \cdots x_m^{i_m}$ 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 nonzero coefficients.

LEMMA 8. *Consider the following problem*:

Given: *A sequence of $k \times k$ matrices $A_1, \ldots, A_n$ over $Z[x_1, \ldots, x_m]$ such that all entries have degree at most g and have all coefficients bounded in absolute value by b.*

Determine: *If $A_1 \cdot A_2 \cdots A_n = I$, where m, k, g, and b are fixed.*

Then this problem can be solved in logspace.

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

For each m-tuple $v = (v_1, \ldots, v_m)$ with $0 \leq v_j \leq gn$, decide if $\langle A_1 \rangle_v \cdot \langle A_2 \rangle_v \cdots \langle A_n \rangle_v = I$ by the algorithm of Lemma 7. If this algorithm accepts for all $(gn + 1)^m$ m-tuples, then accept; otherwise, reject the input

The algorithm requires only logspace; we need only check that the algorithm of Lemma 7 uses only $O(\log n)$ space This follows since d of Lemma 7 is bounded by $b(gn + 1)^m$.

The correctness of the algorithm relies on the following elementary result (Lipton [9, Lemma 4]):

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

For any two matrices A, B over $Z[x_1, \ldots, x_m]$ it follows that $\langle A \cdot B\rangle_v = \langle A\rangle_v \cdot \langle B\rangle_v$; hence, if $A_1 \cdot A_2 \cdots A_n - I = 0$, then the algorithm accepts. Conversely, assume that the algorithm accepts. Let $B = A_1 \cdot A_2 \cdots A_n - I$. Then the algorithm proves that

$$\langle B\rangle_v = 0 \text{ for all } v = (v_1, \ldots, v_m) \text{ with } 0 \leq v_i \leq gn.$$

Now the maximum degree of an entry of B is gn. Thus, by the above result, $B = 0$. □

We can now complete the proof of the theorem. Let G be generated by the finite set $A_1, \ldots, A_l$ of $k \times k$ matrices over F. Then the elements of G are matrices over the field E generated by all the entries of the A_i. Since E is generated by a finite set, E is a finitely generated extension of the field Q of rational numbers. By field theory (Jacobson [8, p. 156]), E is a finite algebraic extension of a transcendental extension $Q(x_1, \ldots, x_m)$ of Q (where the x_i are indeterminates). But, since E is a finite-dimensional algebra over $Q(x_1, \ldots, x_m)$, it is isomorphic, via the regular representation R (Jacobson [8, Theorem 7.4]) to an algebra of (say $t \times t$) matrices over $Q(x_1, \ldots, x_m)$. Furthermore, since E is a field, each of the matrices in the representation is invertible and they commute. Thus replacing each entry in each A_i by a $t \times t$ matrix over $Q(x_1, \ldots, x_m)$ and identifying the resulting block matrices with $kt \times kt$ matrices over $Q(x_1, \ldots, x_m)$, we see that G is isomorphic to a group of $kt \times kt$ matrices over $Q(x_1, \ldots, x_m)$. Furthermore, by the formula for the determinant of a block matrix [8, p. 407], the matrices are invertible.

Finally, 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 which are matrices over $Z[x_1, \ldots, x_m]$ and the result follows by Lemma 8. □

Remark The argument used in the proof of the theorem, with slight modifications, shows more generally that the word problem is solvable in logspace for any *semigroup* of matrices over a field of characteristic zero.

Cannonito [3] and Cannonito and Gatterdam [4] have investigated the computability level of the word problem for various classes of groups with respect to the Grzegorczyk hierarchy ($\mathscr{E}^n_*$) [5]. Our theorem yields sharper results.

COROLLARY 9. *The word problem for polycyclic groups is solvable in logspace.*

PROOF. By a result of Auslander and Swan (see [16, Ch. 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 $\mathscr{E}^0_*$ of Grzegorczyk, Corollary 9 improves Cannonito and Gatterdam's result that the word problem for polycyclic groups is $\mathscr{E}^3_*$-solvable.

Cannonito [3, p. 391] has raised the question of finding the smallest index k such that the word problem for finitely generated free groups is $\mathscr{E}^k_*$-solvable. It follows immediately from Theorem 5 and the preceding paragraph that $k = 0$.

Cannonito [3, p. 391] has raised the further question of finding the smallest k such that a finitely generated free group is $\mathscr{E}^k_*$-decidable in the sense defined in his paper. The Gödel numbering he defines (Lemma 4.1) is in $\mathscr{E}^3$ but not in logspace. However, the simple Godel numbering that takes a finite alphabet $X = \{x_1, \ldots, x_m\}$ and maps each word over $X \cup \{x_1^{-1}, \ldots, x_m^{-1}\}$ to the corresponding base $2m$ number is a Gödel numbering which is in logspace and thus in $\mathscr{E}^0_*$. Combined with the observation in the preceding paragraph, this fact implies $k = 0$

Boone [2] has raised the question of whether there exist finitely generated groups with word problem $\mathscr{E}^\alpha_*$-decidable and conjugacy problem $\mathscr{E}^\beta_*$-decidable with $\beta > \alpha$. Since by our theorem the word problem for finitely generated subgroups of Z-linear groups is $\mathscr{E}^0_*$-solvable and by a result of Miller [10] the conjugacy problem for finitely generated subgroups of Z-linear groups is unsolvable, the disparity between the word and conjugacy problem can be even greater than anticipated in the question.

Let I be an index set and let G_i, $i \in I$, be groups with presentation (X_i, D_i); then the *free product* $\Pi_i^* G_i$ of the G_i is the group with presentation $(\bigcup_i X_i, \bigcup_i D_i)$. If I is finite, the free product is denoted by $G_1 * \cdots * G_n$.

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* iff 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 on $X_1 \cup X_2$ onto $G_1 * G_2$.

PROPOSITION 10 *The class of context-free languages that are group kernels of Z-linear groups is closed under finite free products.*

PROOF. By a theorem of Nisnevic [16, Ch 2], 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 [1], the class of context-free group kernels is closed under finite free products. □

Proposition 10 and Theorem 5 can be used to construct a large number of examples of context-free languages that are recognizable in logspaces. 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 (J. Sakarovitch [15]).

REFERENCES

(Note Reference [8] is not cited in the text)

1 ANISIMOV, A V Group languages *Kibernetika 4* (1971), 18–24, English translation in *Cybernetics 4* (1973), 594–601

2 BOONE, W W Cited in Cannonito, F B Hierarchies of computable groups and the word problem *J Symbolic Logic 31* (1966), 376–392

3 CANNONITO, F.B Hierarchies of computable groups and the word problem *J Symbolic Logic 31* (1966), 376–392

4 CANNONITO, F B , AND GATTERDAM, R W The word problem for polycyclic groups is elementary *Compositio Mathematica 27* (1973), 39–45

5 GRZEGORCZYK, A *Some Classes of Recursive Functions* Rozprawy Matematyczne 4, Instytut Matematyczne Polskey, Akademia Nauk, Warsaw, Poland, 1953, pp 1–45

6 HARDY, G H , AND WRIGHT, E M *An Introduction to the Theory of Numbers* Oxford U Press, London, fourth ed , 1959

7 JACOBSON, N. *Lectures in Abstract Algebra, Vol. III* Van Nostrand, Princeton, N J 1964

8 JACOBSON, N *Basic Algebra* W H Freeman, San Francisco, 1974.

9 LIPTON, R J Polynomials with 0-1 coefficients that are hard to evaluate Conf Rec 16th Ann IEEE Symp on Foundations of Computer Sci , 1975, pp 6–10

10 MILLER, C F III On group-theoretic decision problems and their classification *Annals of Mathematics Studies, No. 68,* Princeton U Press, Princeton, N J , 1971

11 RABIN, M O Computable algebra, general theory and theory of computable fields *Trans Amer Math Soc 95* (1960), 341–360

12 RABIN, M O Private commmnication

13 RITCHIE, R W , AND SPRINGSTEEL, F N Language recognition by marking automata *Inform and Control 20* (1972), 313–330

14 ROTMAN, J *The Theory of Groups An Introduction* Allyn and Bacon, Boston, second ed , 1973

15 SAKAROVITCH, J Private communication.

16 WEHRFRITZ, B A F *Infinte Linear Groups.* Springer-Verlag, New York, 1973

RECEIVED JANUARY 1976, REVISED AUGUST 1976