SIAM J. COMPUT.
Vol. 29, No. 6, pp. 1878–1888

THE COMPLEXITY OF THE *A B C* PROBLEM*

JIN-YI CAI†, RICHARD J. LIPTON‡, AND YECHEZKEL ZALCSTEIN§

Abstract. We present a deterministic polynomial-time algorithm for the $A\,B\,C$ problem, which is the membership problem for 2-generated commutative linear semigroups over an algebraic number field. We also obtain a polynomial-time algorithm for the (easier) membership problem for 2-generated abelian linear groups. Furthermore, we provide a polynomial-sized encoding for the set of all solutions.

Key words. polynomial-time algorithm, membership problem, semigroup, commutative, lattice

AMS subject classifications. 20M99, 68Q25, 68W40

PII. S0097539794276853

1. Introduction.

Most algorithmic questions about infinite groups and semigroups given by presentations (generators and relations) are known to be undecidable [11], [38], [1], [40]. However, the most useful and interesting representation of groups is by matrices over a field. Most groups occurring in physics and many finite simple groups arise as groups of matrices. Nonetheless, it should be noted that many interesting groups do not have faithful matrix representations. An interesting class of groups that cannot be represented by matrices is the uncountable class of infinite Burnside groups introduced by Grigorchuk [20] and whose computational properties were studied in [16]. Rabin has stated without proof in [41] that if the groups are represented by matrices over a field then the word problem is decidable. This result was improved to log space complexity by Lipton and Zalcstein [33] for fields of characteristic zero and by Simon [42] for fields of positive characteristic.

The word problem is a "checking" problem. The corresponding "search" problem is the membership problem: Precisely, given a finite number of elements $a_1, \ldots, a_k$ (given as matrices or permutations) of a group G and a target element g, does g belong to the group generated by $a_1, \ldots, a_k$?

In this generality the problem is undecidable [37], even for groups of 4-by-4 matrices. Thus work on this problem has focused on *finite* groups. Babai and Szemeredi [5] have shown that, for finite groups of matrices over a finite field the problem is in NP. This problem has also motivated the introduction of the complexity class AM [2]. Since, as has been observed in [5], the membership problem for finite matrix groups over finite fields is closely related in complexity to that of the discrete logarithm problem, further progress seems unlikely and most research has concentrated

*Received by the editors November 8, 1994; accepted for publication (in revised form) July 13, 1998; published electronically April 4, 2000. A preliminary version of this paper, "Complexity of the membership problem for 2-generated communatative semigroups of rational matrices," was presented at the 1994 Annual Symposium on Foundations of Computer Science (FOCS), pp. 135–142.

http://www.siam.org/journals/sicomp/29-6/27685.html

†Department of Computer Science, SUNY at Buffalo, Buffalo, NY 14260 (cai@cs.buffalo.edu). Research supported in part by NSF grants CCR 9057486 and CCR 9319093 and an Alfred P. Sloan Fellowship.

‡Department of Computer Science, Princeton University, Princeton, NJ 08544 (rjl@cs.princeton.edu). Research supported in part by NSF grant CCR-9304718

§Division of Computer and Computation Research, National Science Foundation, 4201 Wilson Boulevard, Arlington, VA 22230 (zzalcste@nsf.gov). The statements contributed by this author to the paper represent his personal opinions and are not necessarily those of the National Science Foundation.

on groups represented by *permutations* rather than matrices. Over the years, this research has culminated in efficient sequential and parallel algorithms [3, 4, 15, 22]. Progress on the matrix representation case is very recent. Luks [35] has presented a polynomial-time membership test for solvable matrix groups over "good" finite fields (where the discrete logarithm problem can be bypassed). Beals and Babai [6] have given a polynomial-time *Las Vegas* membership test for arbitrary finite matrix groups over an algebraic number field. For semigroups the problem is even harder. It is known to be undecidable even if the target element g is the zero matrix and the matrices are 3 by 3 [39] (for a related unsolvable problem for semigroups of triangular 3-by-3 matrices see [23]). For finite semigroups the problem is PSPACE-hard [25], even if the semigroups are inverse (this follows from [9, Theorem 5.4]) and it is NP-hard for finite *commutative* semigroups [8].

In this paper, we extend previous algorithmic results in two directions. First, we allow infinite systems, where even decidability is not clear, and second, we consider as semigroups as well. On the other hand, since the general problem is undecidable, some restrictions are needed. In 1980, Kannan and Lipton [28] solved the following *orbit problem*, which is the membership problem for a *cyclic* semigroup, by giving a polynomial-time algorithm:

> Given two commuting matrices A and B over the rational numbers,
> does there exist a nonnegative integer i, such that $A^i = B$?

The following *generalized orbit problem*, or *the A B C problem*, has remained open since 1980:

> Given commuting matrices A, B, and C over the rational numbers,
> does there exist nonnegative integers i and j, such that $A^iB^j = C$?

In this paper, we resolve the *A B C* problem by giving a polynomial-time algorithm which not only decides the solvability of a given instance A, B and C, but also finds all solutions by showing that the set of solutions is a (possibly empty) "affine lattice" and producing a polynomial-sized basis for that lattice.

We also obtain the corresponding result for the group case. We would like to point out that the semigroup problem is harder, even when the generating matrices are invertible, since we do not allow the use of the inverse operation. The results are new, even in the group case. Prior to this work, the best result for the problem in the group case was that it is decidable, a result by Kopytov [24]. The proof in [24], which constructs "yes" and "no" lists, does not give any complexity bounds. Nothing was previously known for the semigroup case.

The techniques presented here can be generalized and modified to solve the membership problem for the case of $k > 2$ generators, where k is fixed [7]. However, we should point out that, for semigroups, the number of generators must be fixed; otherwise, as noted above, the problem is already NP-hard in the finite case.

We will explain briefly why the problem is challenging. Let us assume first (this is seemingly the easiest case) that the matrices A, B, and C are all diagonalizable. Since they commute they must be simultaneously diagonalizable. In this case the problem is reduced to n instances of the following problem (n is the size of the matrices): Given algebraic numbers α, β, and γ, are there nonnegative integers i, j such that $\alpha^i\beta^j = \gamma$? Or more generally, for a fixed k, given algebraic numbers $\alpha_1, \ldots, \alpha_k$, and η, are there nonnegative integers $i_1, \ldots, i_k$ such that

$$\alpha_1^{i_1} \ldots \alpha_k^{i_k} = \eta \tag{1}$$

holds? In case some of the α's are not units, one can use Kummer's unique factorization of ideals and apply an argument based on the exponential growth of the

norms $[\mathbf{N}(\alpha_i)]^i$. However, the hard case is when all the α's are units. The theorem of Blanksby and Montgomery [10] used in [28] is inadequate for the case $k \geq 2$. Another natural attempt is to use Dirichlet's unit theorem to decompose the α's in terms of fundamental units. However, the complexity of computing such decompositions has not, to our knowledge, been analyzed and it may not be computationally tractable. Furthermore, Dirichlet's theorem handles only the group case. Finally, in reducing the general case to the diagonalizable case, Dirichlet's theorem is not enough. We need a description of all solutions of (1). Such a description, for the special case that $\eta = 1$, has been obtained only recently by Masser [36]. A more recent result, by Ge [19] gives a polynomial-time algorithm for computing a basis for all solutions of (1), for $\eta = 1$.

The proof builds upon Ge's result and the observation that if a matrix A is given in Jordan normal form (JNF), then there are closed form formulas for the powers of A. A recent result [12], developed simultaneously with this paper, gives a polynomial-time algorithm for computing JNF. This observation, together with Theorem 3.2 which handles the scalar case, provides a quick proof of the Kannan–Lipton theorem. It should be pointed out that [12] uses the L^3 algorithm [31], which had not yet been discovered at the time that [28] was written. Generalizing to the case of two generators, if both generators are diagonalizable, the problem is reduced to the scalar case. If at least one of the generator matrices is not diagonalizable, it is tempting to believe that, since the matrices commute, they can be brought simultaneously to JNF. If this were true, an extension of the argument in the diagonalizable case could possibly be constructed. However, this is not true. To overcome this difficulty, we introduce a technique which we call *successive restriction*.

Our results are as follows.

THEOREM 1.1. *There is a polynomial-time algorithm for the following problem: Given $k+1$ algebraic numbers $\alpha_1, \ldots, \alpha_k$ and η, are there nonnegative integers $i_1, \ldots, i_k$ such that* (1) *holds? If so, find all solutions (in a polynomial-sized encoding).*

THEOREM 1.2. *There is a polynomial-time algorithm to decide the solvability of the A B C problem; namely, given commuting matrices A, B, and C over an algebraic number field, do there exist nonnegative integers i and j such that $A^i B^j = C$? Further, if there is a solution, the algorithm finds all solutions (in a polynomial-sized encoding).*

THEOREM 1.3. *There is a polynomial-time algorithm to solve the A B C problem in the group case, i.e., where the exponents are allowed to be arbitrary integers.*

It is possible to generalize Theorem 1.3 as follows. A group G satisfies the *permutation* (or *rewriting*) property P_3 iff for any three elements a_1, a_2, a_3 in G, the product $a_1 a_2 a_3$ equals a product which is a nontrivial permutation of a_1, a_2, a_3. Any abelian group satisfies the property P_3. It is known [14] (see also [17]) that a group satisfies P_3 iff it has at most one nontrivial commutator. Thus in a group satisfying P_3, any product of powers of the generators equals the product $a_1^{i_1} \ldots a_k^{i_k}$, possibly post-multiplied by the unique commutator. Thus membership testing is reduced to the abelian case. Unfortunately, the P_3 semigroups have not been characterized completely (for some partial results see [17]) and the complexity of the membership problem for P_3 semigroups is not known.

The plan for this paper is as follows. In section 2 we will deal with some preliminary issues. Proofs in section 2 are omitted. In section 3 we prove Theorem 3.2, from which Theorem 1.1 follows. In section 4, we first give an illustration of the power of

our new techniques in a simple setting by giving a transparent proof of the Kannan–Lipton theorem. Then in section 4 we use the method of successive restriction to complete the solution of the A B C problem.

2. Preliminaries. First, without loss of generality, we may assume that the matrices are over the rationals. This reduction uses the classical matrix representation of a finite algebraic extension over the ground field [21]. Let A, B, and $C \in \mathbf{Q}^{n\times n}$ be $n \times n$ rational matrices. The input size to the problem is n plus the sum of binary lengths of all entries. By an extension of a technique from [28], we may assume that C is given as a polynomial in A and B with rational coefficients. This is certainly a necessary condition, and whether C is such a polynomial can be decided in polynomial time, as it is a question of linear dependence over the rationals [26].

Thus, we are given $A, B \in \mathbf{Q}^{n\times n}$ such that A, B commute, and a polynomial p in A and B. The question is to decide if p can be expressed as a product of nonnegative powers of A and B. In [28], the computation of eigenvalues could be circumvented, using the crucial fact that the ring of polynomials in one variable over a field is principal. Since the ring of polynomials in two variables is not principal, this strategy no longer works. We will compute in various number fields, mostly symbolically; i.e., we will have an irreducible polynomial f (proven so by the L^3-algorithm), and each element in the field will be represented by a polynomial of degree $< \deg(f)$ [31, 29]. This can be done over any number fields as well, not just $\mathbf{Q}$. However, an important issue is that we cannot allow the degree of the extension over $\mathbf{Q}$ to be too large; in general, to stay within polynomial time, we cannot operate in the splitting field of an irreducible polynomial of degree say, n, since the Galois group of this extension field might be too large. It is not known how to compute in polynomial time in an extension field where the Galois group has size $n!$ and in fact it is believed to be impossible [32].

We will need to compute the JNF for either of the matrices A or B. What we will show in the paper is a technique of successive restriction which is of independent interest and is almost as good for our purposes as simultaneous JNF. But before we get to that, let's first ask if we can compute a basis change for the JNF of a matrix A in polynomial time. The difficulty is that if we use the standard textbook algorithm, we will be dealing with the splitting field of χ_A over $\mathbf{Q}$. Thus the standard algorithm will not do. However, there is a polynomial-time algorithm [12] that finds an invertible matrix T, such that $T^{-1}AT = J_A$, the JNF for A. The matrix T has entries from the splitting field of χ_A, but the trick is that in [12] we can find a T where every entry t in fact belongs to a much smaller extension field, which varies with t and can be computed in polynomial time within the smaller field. The matrix J_A is *not* computed from the *product* $T^{-1}AT$; in fact, computing T^{-1} from T, say using Gaussian elimination, involves the splitting field again. However, a different technique is used in [12] to compute J_A, and to compute T^{-1} from T, without ever going to the splitting field, all accomplished in polynomial time.

Next there is the issue of how to apply this basis transformation to another matrix M. The fact is that this cannot be done in polynomial time. The same difficulty with the splitting field gets in the way. *But it can be done for the matrices B and C*, using the fact that they commute with A. It is only in this limited sense that we have obtained this basis transformation computationally. Fortunately, this is sufficient for the solution of the A B C problem.

There is another technical issue concerning conjugates of the same irreducible polynomial. When it is necessary to distinguish one root from another, we will use a

"good enough" rational approximation, which gives a polynomial number of bits and uniquely identifies the root on the complex plane. We refer the reader to [34] for the details.

In the following we will speak freely of computing JNF, invariant subspaces, etc., all in polynomial time, without further comment. We will reduce the situation to the case where both A and B have exactly one eigenvalue each, λ and μ, respectively. We view A and B as linear transformations over the field $\mathbf{C}$ of complex numbers. Let $p(.)$ be a polynomial with complex coefficients. Consider a subspace V defined as $\ker(p(A))$ or $\mathrm{Im}(p(A))$. It is easy to see that V is an invariant subspace for both A and B

Now consider the subspace $V_\lambda = \ker(\lambda I_n - A)^{n-1}$, where λ is any eigenvalue of A, i.e., $\lambda \in Spec(A)$. Since A and B commute, V_λ is an invariant subspace for both A and B.

After some preparation, we can arrive at the following situation: we have a decomposition of $\mathbf{C}^n$ as a direct sum of subspaces $V_{\lambda,\mu}$, invariant for both A and B, where λ and μ range over $Spec(A)$ and $Spec(B)$, i.e., all eigenvalues of A and B, such that there is just one eigenvalue λ (and μ, respectively) for A (and B, respectively) on $V_{\lambda,\mu}$:

$$\mathbf{C}^n = \bigoplus_{\lambda \in Spec(A), \mu \in Spec(B)} V_{\lambda,\mu}.$$

LEMMA 2.1.
Suppose A, B commute and C is a polynomial in A and B; then for any i, j,

$$A^i B^j = C \Longleftrightarrow (A\mid_{V_{\lambda,\mu}})^i (B\mid_{V_{\lambda,\mu}})^j = C\mid_{V_{\lambda,\mu}},$$

$\forall \lambda \in Spec(A), \mu \in Spec(B)$.

For what follows, we will fix any pair of eigenvalues $\lambda \in Spec(A)$ and $\mu \in Spec(B)$ and consider $A\mid_{V_{\lambda,\mu}}$ and $B\mid_{V_{\lambda,\mu}}$. We will call them A and B, respectively, when no confusion arises.

3. The affine lattice of solutions. We will need the following theorem of Masser [36].

THEOREM 3.1. *Fix any $k \geq 1$. Let $\alpha_1, \ldots, \alpha_k$ be nonzero algebraic numbers over $\mathbf{Q}$. Let $D = [\mathbf{Q}(\alpha_1, \ldots, \alpha_k) : \mathbf{Q}]$ be the degree of the algebraic extension, and let h be the maximum height [1] of $\alpha_1, \ldots, \alpha_k$ over $\mathbf{Q}$. Then, the relation group*

$$L = \{\ (e_1, \ldots, e_k) \in \mathbf{Z}^k \mid \alpha_1^{e_1} \cdots \alpha_k^{e_k} = 1\ \}$$

is a lattice with a small basis. More specifically, L has a generating set $v_1, \ldots, v_\ell \in \mathbf{Z}^k$, $1 \leq \ell \leq k$, such that the maximum entry in these vectors $\max_{1 \leq i \leq \ell}\ _{1 \leq j \leq k} |v_{i,j}|$ is at most

$$(ckh)^{k-1} D^{k-1} \frac{(\log(D+2))^{3k-3}}{(\log\log(D+2))^{3k-4}},$$

where c is some absolute constant.

In order to appreciate this remarkable theorem of Masser, let's look at its implication on the computational complexity of finding such a basis. Note that in the

[1] The height function of an algebraic number is essentially the sum of the degree and the binary length of all coefficients in the defining equation over $\mathbf{Q}$.

inequality, the left hand side refers to the *quantity* $v_{i,j}$, while the right hand side essentially refers to the binary length of the input data. (Recall that k is fixed.) Thus, an exhaustive search can be done in polynomial time to find a small basis.

We call a shift of a lattice $L + v$, for some $v \in \mathbf{Z}^k$, an *affine lattice*. We say that an affine lattice has *small description* if it is $L + v$ for some small v and L has a small basis; here small means all entries are polynomially bounded in *quantity* (not merely in binary length).

THEOREM 3.2. *Given nonzero algebraic numbers $\alpha, \beta_1, \ldots, \beta_k$, the set*

$$\{\ (j_1, \ldots, j_k) \mid \alpha\beta_1^{j_1} \cdots \beta_k^{j_k} = 1\ \}$$

is either empty or is an affine lattice with rank at most k and a small description. Moreover, it is decidable in polynomial time whether it is empty, and if not, to compute a small description in terms of an off-set vector v and a small basis. Finally, if the rank of the affine lattice is k, then all of $\alpha, \beta_1, \ldots, \beta_k$ are roots of unity.

Proof. Consider the lattice

$$L = \{\ (i, j_1, \ldots, j_k) \mid \alpha^i\beta^{j_1} \cdots \beta^{j_k} = 1\ \}.$$

By Ge's theorem [19], we get a small basis $v_1, \ldots, v_\ell$, $\ell \le k + 1$. Now we wish to intersect this lattice with the affine lattice $\{(1, j_1, \ldots, j_k) \mid j_1, \ldots, j_k \in \mathbf{Z}\}$.

Write

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\ell \end{pmatrix} = \begin{pmatrix} v_{10} & v_{11} & \ldots & v_{1k} \\ v_{20} & v_{21} & \ldots & v_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ v_{\ell 0} & v_{\ell 1} & \ldots & v_{\ell k} \end{pmatrix},$$

where $v_{ij} \in \mathbf{Z}$ and $|v_{ij}| \le n^{O(1)}$.

We can first perform a basis reduction to transform the basis to a so-called canonical basis in the sense of Hermite. This can be done in polynomial time [27]

$$\begin{pmatrix} v_{10} & v_{11} & \ldots & v_{1k} \\ 0 & v_{21} & \ldots & v_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \cdot \end{pmatrix},$$

where $0 \le v_{10}$, $0 \le v_{11} \le v_{21}$, etc. The row vectors still form a basis for L. We will still call them $v_1, \ldots, v_\ell$.

Now it is clear that this lattice intersects with $\{(1, j_1, \ldots, j_k) \mid j_1, \ldots, j_k \in \mathbf{Z}\}$ iff $v_{10} = 1$, and if so, then the intersection is $L' + v_1$, where L' is the lattice spanned by $v_2, \ldots, v_\ell$.

If the rank of the affine lattice is k, then $\ell = k + 1$. The basis matrix is a square matrix and all diagonal entries are nonzero. In particular, $v_{kk} \neq 0$, and $\beta_k^{v_{kk}} = 1$. Thus, β_k is a root of unity. Continuing, we have $v_{k-1,k-1} \neq 0$, and $\beta_{k-1}^{v_{k-1,k-1}} = \beta_k^{-v_{k-1,k}}$, which is a root of unity. Thus, β_{k-1} is also a root of unity. The proof is completed by an easy induction. ∎

If any of the algebraic numbers $\alpha, \beta_1, \ldots, \beta_k$ are 0, we will adopt the convention that $0^0 = 1$ and $0^i = 0$ for $i > 0$. Under this convention, the statement in Theorem 3.2 can be easily adapted to allow 0's. Now to prove Theorem 1.1, note that the set

of k-tuples of nonnegative integers $(i_1, \ldots, i_k)$ such that (1) holds is obtained by intersecting the affine lattice L of Theorem 3.2 with the set of k-tuples of nonnegative integers. By Lenstra [30], membership in the intersection can be decided in polynomial time.

4. The proof. We will first illustrate the new technique, in a simple setting, by demonstrating how swiftly the Kannan–Lipton Theorem [28] can be proved using this technique.

4.1. The Kannan–Lipton theorem.

THEOREM 4.1. *There is a polynomial-time algorithm for the following problem: Given two rational matrices A, B, is there a nonnegative integer i such that $A^i = B$?*

Proof. Put A in JNF. Restrict to a subspace V_λ, where the only eigenvalue for A on V_λ is λ.

- Case 1. $\lambda = 0$. Then $A|_{V_\lambda}$ is nilpotent, $(A|_{V_\lambda})^n = 0$. Thus we need only check the cases $(A|_{V_\lambda})^i = (B|_{V_\lambda})$, for $0 \le i \le n$.
- Case 2. $\lambda \neq 0$. Consider the solutions to $\lambda^i = c$, which is obtained by looking at any diagonal entry in $(A|_{V_\lambda})^i = B|_{V_\lambda}$. If the solution set is empty, we are finished. Suppose the solution set is an affine lattice of rank 0, i.e., there is a unique solution i and since $i \le n^{O(1)}$ we can directly check if $A^i = B$. The only nontrivial case is rank 1. Then by Theorem 3.2, λ is a root of unity. So must be c, hence $c \neq 0$. The order of λ must be polynomially bounded, since $\chi_A(\lambda) = 0$.
  1. $A|_{V_\lambda}$ is diagonal. Then it is completely determined by Theorem 3.2.
  2. $A|_{V_\lambda}$ is not diagonal. Then some Jordan block has size ≥ 2. We can symbolically compute the powers of $A|_{V_\lambda}$, up to $(A|_{V_\lambda})^i$, for $i \le 2^{n^{O(1)}}$. This uses the fact that λ is a root of unity, and we know the closed form formula for powers of JNF. Thus, on the diagonal we get equation $\lambda^i = c$, and on the off-diagonal we get an equation $\binom{i}{1}\lambda^{i-1} = c'$. This gives the necessary condition that $i = \lambda c'/c$. If $\lambda c'/c$ is not a nonnegative integer, then there is no solution. Otherwise, we simply check directly if $\lambda^i = c$.

The Kannan–Lipton Theorem is proved. ∎

4.2. The method of successive restriction. Now the setting is $V_{\lambda,\mu}$. We will write A for $A|_{V_{\lambda,\mu}}$ and do the same for B. There will be four cases, depending on whether $\lambda = 0$ and/or $\mu = 0$. The cases when at least one of the eigenvalues is 0 are in fact simpler, since then the matrix is nilpotent, so that we need only check powers up to n. (Recall that on $V_{\lambda,\mu}$, each matrix has exactly one eigenvalue.) We will omit the details on these three cases and assume $\lambda \neq 0$ and $\mu \neq 0$. If both A and B are diagonal matrices $\lambda I$and μI, then this case is completely determined by Theorem 3.2. Suppose A is not diagonal. Put A in its JNF. Since $A \neq \lambda I$, at least one block is of dimension > 1.

Let

$$V' = \ker(\lambda I - A)$$

and

$$V'' = \ker(\lambda I - A)^2.$$

Since A and B commute, both V' and V'' are invariant subspaces of B as well as A. In terms of the Jordan form of A, V' corresponds to the first rows and columns

of each λ-block. And V'' corresponds to the first and the second rows and columns (whenever a second row and column exists) of each λ-block. Since at least one block is of dimension > 1, $V' \neq V''$.

Let $n_1 = \dim V'$ and $n_1 + n_2 = \dim V''$; then $n_1 \geq n_2 \geq 1$.

Let $v_{11}, \ldots, v_{1k_1}, v_{21}, \ldots, v_{2k_2}, \ldots, v_{\ell 1}, \ldots, v_{\ell k_\ell}$ be the basis vectors for which A has its Jordan form, where $v_{i1}, \ldots, v_{ik_i}$ is the basis vectors corresponding to the ith block. We also assume that the blocks are ordered so that $k_1 \geq \cdots \geq k_\ell$. Then $v_{11}, \ldots, v_{\ell 1}$ spans the eigenspace $V' = \ker(\lambda I - A)$, and consequently $\ell = n_1$. By assumption $k_1 \geq 2$, and let $\ell' = \max\{i \mid k_i \geq 2\}$; then $v_{11}, \ldots, v_{\ell,1}, v_{12}, \ldots, v_{\ell' 2}$ spans V'' and $\ell' = n_2$.

Consider $A\,|_{V''}$ and $B\,|_{V''}$. If we order the basis vectors as $v_{11}, \ldots, v_{\ell,1}, v_{12}, \ldots, v_{\ell' 2}$, then A has the form

$$A = \begin{pmatrix} \lambda I_{n_2} & 0 & I_{n_2} \\ 0 & \lambda I_{n_1 - n_2} & 0 \\ 0 & 0 & \lambda I_{n_2} \end{pmatrix}.$$

By decomposing B in blocks of the same dimensions, one can easily verify that

$$A \text{ and } B \text{ commute} \iff B \text{ is of the following block upper triangular form:}$$

$$B = \begin{pmatrix} X & Y & Z \\ 0 & U & V \\ r0 & 0 & X \end{pmatrix},$$

where X, Y, Z, U, V are of the appropriate dimensions.

(If $n_1 = n_2$, then the middle blocks $\lambda I_{n_1 - n_2}$ in A, and Y, U, and V in B are understood not to appear.)

4.2.1. Restriction to V'. Choose a basis transformation of V' such that $B\,|_{V'}$ is in its Jordan form. Note that on V', $A\,|_{V'}$ is the scalar matrix λI_{n_1} which is unchanged under all basis transformations. Thus, under this basis, $A\,|_{V'}$ is still the scalar matrix λI_{n_1}, and $B\,|_{V'}$ is a direct sum of Jordan blocks all of which have μ on its diagonal, since $Spec(B\,|_{V'}) = \{\mu\}$. By comparing eigenvalues, we get $\lambda^i \mu^j = c$. By Theorem 3.2 we get either an empty set of solutions or an affine lattice of small description. If it is empty, we are finished; or if the rank is 0, we can directly check it. If the rank is 1, then we can reduce it to Kannan–Lipton's theorem. In fact, let $i = i_0 + as$ and $j = j_0 + bs$ for small i_0, j_0, a, b; then we have to solve for s in $(A^a B^b)^s = (CA^{-i_0} B^{-j_0})$.

Now suppose the rank is 2. Then both λ and μ are roots of unity. We note that in this case we can compute high powers of A and B, up to $2^{n^{O(1)}}$, in polynomial time. This is accomplished separately for A and B by first putting the target matrix in JNF, then taking its power, and finally reverting back.

Suppose $B\,|_{V'}$ is not a scalar matrix μI. Then some μ-block of $B\,|_{V'}$ has dimension > 1. Then consider

$$U' = \ker(\mu I - B\,|_{V'})$$

and

$$U'' = \ker(\mu I - B\,|_{V'})^2.$$

As before, both U' and U'' are invariant subspaces of A as well as B. Since at least one block of $B\mid_{V'}$ is of dimension > 1, $U' \neq U''$.

Let $m_1 = \dim U'$ and $m_1 + m_2 = \dim U''$; then $m_1 \geq m_2 \geq 1$, and if we order the basis vectors appropriately, we have $A\mid_{U''} = \lambda I_{m_1+m_2}$ and

$$B\mid_{U''} = \begin{pmatrix} \mu I_{m_2} & 0 & I_{m_2} \\ 0 & \mu I_{m_1-m_2} & 0 \\ 0 & 0 & \mu I_{m_2} \end{pmatrix}.$$

(Again, if $m_1 = m_2$, then the middle blocks are understood not to appear.)

Implied by the forms of $A\mid_{U''}$ and $B\mid_{U''}$ is the fact that the first and the last m_2 basis vectors together generate an invariant subspace for both A and B. By focusing on this subspace, we get a necessary condition of $A^i B^j = C$ in the form of a pair of equations

$$\lambda^i \mu^j = c, \qquad j\lambda^i \mu^{j-1} = c'.$$

This gives us, upon substitution, $j = \mu c'/c$, which reduces the problem to the one-variable case.

4.2.2. Restriction to V''. Now we suppose on V', $B\mid_{V'} = \mu I_{n_1}$; thus on V'',

$$B\mid_{V''} = \begin{pmatrix} \mu I_{n_2} & 0 & Z \\ 0 & \mu I_{n_1-n_2} & V \\ 0 & 0 & \mu I_{n_2} \end{pmatrix}.$$

(Once again, the middle blocks disappear if $n_1 = n_2$.)

Suppose $n_1 > n_2$. $V^* = \operatorname{span}\{v_{n_2+1\,1}, \ldots, v_{n_1 1}\}$, the subspace corresponding to the middle blocks, is an invariant subspace for both A and B. Consequently we may consider the quotient space V''/V^* and the induced action of A and B on this quotient space, denoted by $\tilde{A}$ and $\tilde{B}$, respectively. (If $n_1 = n_2$, then $V^* = 0$ and $V''/V^* = V''$.) Under the induced basis from $\{v_{11}, \ldots, v_{n_2,1}, v_{1,2}, \ldots, v_{n_2,2}\}$ for V''/V^*,

$$\tilde{A} = \begin{pmatrix} \lambda I_{n_2} & I_{n_2} \\ 0 & \lambda I_{n_2} \end{pmatrix}$$

and

$$\tilde{B} = \begin{pmatrix} \mu I_{n_2} & Z \\ 0 & \mu I_{n_2} \end{pmatrix}.$$

If $Z = 0$ then we will get a necessary condition

$$\lambda^i \mu^j = c, \qquad i\lambda^{i-1} \mu^j = c'.$$

This gives us, upon substitution, $i = \lambda c'/c$, which reduces the problem to the one-variable case.

If $Z \neq 0$ then we will get a necessary condition

$$\lambda^i \mu^j = c, \qquad j\lambda^i \mu^{j-1} z + i\lambda^{i-1} \mu^j = c',$$

for some known algebraic numbers c, c' and $z \neq 0$. Upon substitution, we get

$$\frac{i}{\lambda} + z\frac{j}{\mu} = \frac{c'}{c}.$$

Solving i in terms of j,

$$i = \frac{\lambda c'}{c} - \frac{z\lambda}{\mu} j.$$

If $\frac{z\lambda}{\mu}$ is not rational, then we will have at most one pair of integral solution (i, j), and we can easily find it and test it. If $\frac{z\lambda}{\mu}$ is rational, then unless $\lambda c'/c$ is rational, there is no solution, and if $\lambda c'/c$ is rational, then there is an integral relationship between i and j,

$$ui + vj = w.$$

We can solve this equation in general form, $i = i_0 + v_1 t$ and $j = j_0 - u_1 t$, where $u_1 = u/\gcd(u, v)$ and $v_1 = v/\gcd(u, v)$. Substituting back in $A^i B^j = C$, we get $(A^{i_0} B^{j_0})(A^{v_1} B^{-u_1})^t = C$, which reduces it to the case with one variable t. This proves Theorem 1.2. Theorem 1.3 is proved by removing the restriction to nonnegative exponents at the appropriate places in the proof. Alternatively, as suggested by the referee, apply Theorem 1.2 four times with the respective generator pairs A, B; A, B^{-1}; A^{-1}, B; and A^{-1}, B^{-1}.

Acknowledgments. This paper would not have been possible without the contribution of M. L. Robinson, who has pointed us to transcendental number theory and in particular to Masser's theorem. We thank him for this and for many helpful discussions. We would also like to acknowledge helpful discussions with Katalin Friedl, Ravi Kannan, Susan Landau, Laci Lovász, Andrew Odlyzko, Lajos Ronyai, and William Velez. Zeke Zalcstein would also like to thank Kamal Abdali for TEX nical assistance.

REFERENCES

[1] S. I. Adyan, *Algorithmic unsolvability of problems of recognition of certain properties of groups*, Dokalady Akad. Nauk SSSR, 103 (1955), pp. 533–535 (in Russian).

[2] L. Babai, *Trading group theory for randomness*, in Proceedings of the 17th Symposium on the Theory of Computing, Providence, RI, 1985, pp. 421–429.

[3] L. Babai, E. Luks, and A. Seress, *Permutation groups in NC*, in Proceedings of the 19th Symposium on the Theory of Computing, New York, 1987, pp. 272–282.

[4] L. Babai, G. Cooperman, L. Finkelstein, E. Luks, and A. Seress, *Fast Monte Carlo algorithms for permutation groups*, in Proceedings of the 23rd Symposium on the Theory of Computing, New Orleans, 1991, pp. 90–100.

[5] L. Babai and E. Szemeredi, *On the complexity of matrix group problems* I, in Proceedings of the 25th Symposium on the Foundation of Computer Science, Singer Island, FL, 1984, pp. 229–240.

[6] R. Beals and L. Babai, *Las Vegas algorithms for matrix groups*, in Proceedings of the 33rd Symposium on the Foundation of Computer Science, Palo Alto, CA, 1993, pp. 427–436.

[7] L. Babai, R. Beals, J. Cai, G. Ivanos, and E. Luks, *Multiplicative equations over commuting matrices*, in Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), Atlanta, GA, 1996, pp. 498–507.

[8] M. Beaudry, *Membership testing in commutative transformation semigroups*, Inform. and Comput., 79 (1988), pp. 84–93.

[9] J.-C. Birget, S. Margolis, J. Meakin, and P. Weil, *PSPACE-completeness of certain algorithmic problems on the subgroups of free groups*, in Proceedings International Comput. Algorithms Lang. Programming, 1994, pp. 274–285.

[10] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith., 18 (1971), pp. 355–369.

[11] W. W. Boone, *The word problem*, Ann. of Math., 70 (1952), pp. 207–265.

[12] J. Cai, *Computing Jordan normal forms exactly for commuting matrices in polynomial time*, Internat. J. Foundations Comput. Sci., 5 (1994), pp. 293–302.

[13] J. Cai, R. Lipton, and Y. Zalcstein, *Complexity of the membership problem for* 2*-generated commutative semigroups of rational matrices*, in Proceedings Foundation of Computer Science, Santa Fe, NM, 1994, pp. 135–142.
[14] M. Curzio, P. Longobardi, and M. Mai, *Su di un problema combinatorio in teoria dei gruppi*, Atti Lincei VIII 74, (1983), pp. 136–142.
[15] M. Furst, J. Hopcroft, and E. Luks, *Polynomial time algorithms for permutation groups*, in Proceedings Foundation of Computer Science, 1980, pp. 60–78.
[16] M. Garzon and Y. Zalcstein, *Complexity of Grigorchuk groups with application to cryptography*, Theoret. Comput. Sci., 88 (1991), pp. 83–98.
[17] M. Garzon and Y. Zalcstein, *On permutation properties in groups and semigroups*, Semigroup Forum, 35 (1987), pp. 337–351.
[18] G. Ge, *Testing equalities of multiplicative representations in polynomial time*, in Proceedings Foundation of Computer Science, 1993, pp. 422–426.
[19] G. Ge, *Algorithms Related to the Multiplicative Representations of Algebraic Numbers*, Ph.D. dissertation, Department of Mathematics, University of California at Berkeley, Berkeley, CA, 1993.
[20] R. I. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Math. USSR Izvestiya, 25 (1985), pp. 259–300.
[21] I. Kaplansky, *Fields and Rings*, 2nd ed., University of Chicago Press, Chicago, IL, 1972.
[22] D. E. Knuth, *Notes on Efficient Representation of Permutation Groups*, manuscript, 1981.
[23] M. Krom, *An unsolvable problem with products of matrices*, Math. Systems Theory, 14 (1981), pp. 335–337.
[24] L. Kopytov, *Solvability of the occurrence problem in finitely generated soluble groups of matrices over the field of algebraic numbers*, Algebra and Logic, 7 (1968), pp. 388–393.
[25] D. Kozen, *Lower bounds for natural proof systems*, in Proceedings Foundation of Computer Science, Providence, RI, 1977, pp. 254–266.
[26] R. Kannan, *The Size of Numbers in the Analysis of Certain Algorithms*, Ph.D. dissertation, Operations Research Dept., Cornell University, Ithaca, NY, 1980.
[27] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Comput., 8 (1979), pp. 499–507.
[28] R. Kannan and R. Lipton, *The orbit problem is decidable*, in Proceedings of the 12th Symposium on the Theory of Computing, Los Angeles, CA, 1980, pp. 252–261. See also *Polynomial-time algorithms for the orbit problem*, JACM, 33 (1986), pp. 808–821.
[29] R. Kannan, A. K. Lenstra, and L. Lovász, *Polynomial factorization and non-randomness of bits of algebraic numbers and certain transcendental numbers*, Math. Comp., 50 (1988), pp. 235–250.
[30] H. W. Lenstra, *Integer programming with a fixed number of variables*, Math. Oper. Res., 8 (1983), pp. 538–548.
[31] A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515–534.
[32] S. Landau, *personal communication*, University of Massachusetts, Amherst, MA, 1994.
[33] R. Lipton and Y. Zalcstein, *Word problems solvable in logspace*, JACM, 24 (1977), pp. 522–526.
[34] L. Lovasz, *An Algorithmic Theory of Numbers, Graphs and Convexity*, SIAM, Philadelphia, 1986.
[35] E. Luks, *Computing in solvable matrix groups*, in Proceedings Foundation of Computer Science, Pittsburgh, PA, 1992, pp. 111–120.
[36] D. W. Masser, *Linear relations on algebraic groups*, in New Advances in Transcendence Theory, A. Baker, ed., Cambridge University Press, Cambridge, UK, 1988, pp. 248–262.
[37] K. A. Mihailova, *The occurrence problem for a direct product of groups*, Dokl. Akad. Nauk, 119 (1958), pp. 1103–1105.
[38] P. S. Novikov, *On the algorithmic unsolvability of the problem of equality of words in group theory*, Trudy Mat. Inst. Akad. Nauk SSSR, 44 (1955), pp. 1–144 (in Russian).
[39] M. S. Paterson, *Undecidability in* 3 *by* 3 *matrices*, J. Math. Phys., 49 (1970), pp. 105–107.
[40] M. Rabin, *Recursive unsolvability of group theoretic problems*, Ann. Math., 67 (1958), pp. 172–194.
[41] M. Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc., 95 (1960), pp. 341–360.
[42] H. U. Simon, *Word problems for groups and context-free languages*, in Foundations of Computation Theory, Lecture Notes in Comput. Sci., Springer-Verlag, New York, 1979, pp. 417–422.