Multiplicative equations over commuting matrices
(Extended Abstract)

László Babai[1], Robert Beals[2],
Jin-yi Cai[3], Gábor Ivanyos[4], Eugene M. Luks[5]

Mailing address: Robert Beals
School of Mathematics
Institute For Advanced Study
Olden Lane
Princeton, New Jersey, 08540

[1]Department of Computer Science, University of Chicago, Chicago, Illinois 60637 and Eötvös University, Budapest, Hungary H-1088
[2]DIMACS, Rutgers University, Piscataway, NJ 08855-1179 and Institute for Advanced Study, Princeton, NJ 08540
[3]Department of Computer Science, SUNY at Buffalo, Buffalo, NY 14260
[4]Computer and Automation Institute, Hungarian Academy of Sciences, P.O.Box 63, Budapest, Hungary H-1528
[5]Department of Computer and Information Science, University of Oregon, Eugene, OR 97403

Abstract

We consider the solvability of the equation

$$\prod_{i=1}^{k} A_i^{x_i} = B$$

and generalizations, where the A_i and B are given commuting matrices over an algebraic number field F. In the *semigroup membership problem*, the variables x_i are constrained to be nonnegative integers. While this problem is NP-complete for variable k, we give a polynomial time algorithm if k is fixed. In the *group membership problem*, the matrices are assumed to be invertible, and the variables x_i may take on negative values. In this case we give a polynomial time algorithm for variable k and give an explicit description of the set of all solutions (as an affine lattice).

The results generalize recent work of Cai, Lipton, and Zalcstein [CLZ] where the case $k = 2$ is solved using Jordan Normal Forms (JNF). We achieve greater clarity, simplicity, and generality by eliminating the use of JNF's and referring to elementary concepts of the structure theory of algebras instead (notably, the *radical* and the *local decomposition*).

Partial solutions are combined using algorithms for (affine) lattices. The special case of 1×1 matrices was recently solved by G. Ge [Ge1-2] and we heavily rely on his results.

1 Introduction

We describe the *constructive membership problem* for k-generated commutative matrix semigroups: An instance consists of a field F, together with $k + 1$ commuting square matrices $B, A_1, A_2, \ldots, A_k$ over F. The problem is to determine whether there exists a solution in nonnegative integers $x_1, \ldots, x_k$ to

$$\prod_{i=1}^{k} A_i^{x_i} = B, \tag{1}$$

and to exhibit such a solution if one exists. (Actually, our algorithm will find a polynomial size encoding of the set of all solutions.) In this paper, we consider the case when F is the field $\mathbf{Q}$ of rational numbers and, more generally, when F is an *algebraic number field* (finite extension of $\mathbf{Q}$), represented as $\mathbf{Q}[x]/(p(x))$, given by an irreducible polynomial p. This representation allows exact symbolic arithmetic in F.

We refer to the set $S = \{A_1, \ldots, A_k\}$ as the *generating set.*

Theorem 1.1 *For any fixed k, the constructive membership problem for k-generated commutative matrix semigroups over algebraic number fields can be solved in polynomial time.*

We represent the set of all solutions as the set of lattice points in the union of polynomially many convex cones. A solution (if one exists) can then be extracted via [Le2].

Our results imply that even for variable k, the commutative semigroup membership problem (existence of a solution) belongs to NP. Combined with [Be] this implies that the problem is NP-complete.

We also consider two related problems. Suppose that S consists of invertible matrices, and we allow the x_i to take on negative values. In this case the set of solutions to (1) is an affine lattice L, and we give a polynomial time algorithm to find a basis and an offset vector for L (cf. subsection 3.1). The set of matrices B admitting a nonempty solution is the *group* generated by S. We refer to this problem as the constructive membership problem for commutative matrix groups, or simply the *group case*. In the group case, the number k of generators will be viewed as an input variable.

Theorem 1.2 *The constructive membership problem for commutative matrix groups over algebraic number fields can be solved in polynomial time (even for variable k).*

We also show that it is possible to test membership in an *orbit* of a commutative group. Suppose S consists of commuting invertible $n \times n$ matrices, and let G be the group they generate. Let $\ell \geq 1$ and let A and B be arbitrary $n \times \ell$ matrices. We give a polynomial time algorithm for testing whether or not B belongs to the orbit GA. In fact, we find the affine lattice of solutions in integers x_i to

$$\left(\prod_{i=1}^{k} A_i{}^{x_i}\right) A = B. \tag{2}$$

As in the group case, k is variable.

Theorem 1.3 *The constructive membership problem for orbits of commutative matrix groups over algebraic number fields can be solved in polynomial time (for variable k).*

We mention that our techniques extend to the following *orbit intersection problem.* Given commuting $n \times n$ matrices $A_1, \ldots, A_h, B_1, \ldots, B_k$, and $n \times \ell$ matrices A and B, determine whether or not there exist solutions in nonnegative integers x_i and y_j to

$$\left(\prod_{i=1}^{h} A_i{}^{x_i}\right) A = \left(\prod_{j=1}^{k} B_j{}^{y_j}\right) B,$$

and exhibit a solution if one exists.

Theorem 1.4 *For fixed k, one can solve the orbit intersection problem for commutative matrix semigroups over algebraic number fields in polynomial time.*

2 History of the problem and comparison with previous work

The case $k = 1$ of the semigroup membership problem ("is B a power of A?") was known as the "orbit problem" and was solved in polynomial time in a celebrated paper by Kannan and Lipton in 1980 [KL]. The case $k = 2$ (the "A-B-C problem"), formulated in [KL], was solved in [CLZ] (1994). In this paper we extend these results to the greatest generality permitted by NP-hardness obstacles (arbitrary fixed k for the semigroup problem, variable k for the group problem).

We note that the most natural generalization of the "orbit problem" (membership in cyclic semigroups of matrices) would be the membership problem for matrix semigroups, given by a list of generators. However, this problem is undecidable even for 3×3 integral matrices (Paterson [Pa]), and even the group membership problem is undecidable for 4×4 integral matrices (Mihaĭlova [Mi]). Therefore we restrict our attention to the *commutative* case, still quite challenging, as its history demonstrates. A possible future extension of the present work would examine the complexity of membership in nilpotent or solvable groups; these cases are known to be decidable (Kopytov [Ko]).

The commutative semigroup membership problem is known to be NP-hard (its special case of finite transformation semigroups is NP-complete, Beaudry [Be]). A non-trivial by-product of our main results is that this problem belongs to NP and is therefore NP-complete (for variable k). We do not know the complexity status of this problem for variable k but bounded dimension.

Finite matrix groups in characteristic zero are well understood [BB], [BBR]. The case of matrix groups over finite fields is of different nature [Lu], [BB]. While undecidability cannot occur, other obstacles do; the 1×1 case is identical with the discrete log problem.

The introduction of [CLZ] provides additional history and further explanation of the number theoretic difficulties in characteristic zero (our case).

Here we wish to add that one of the sources of difficulty encountered by the algorithms in [CLZ] stems from its use of the Jordan Normal Form (JNF). The difficulties are of combinatorial as well as of algebraic nature. The underlying combinatorial structure can be held responsible for the impossibility of simultaneous JNF's of a pair of commuting matrices. The algebraic difficulties arise from the fact that the splitting field of the characteristic polynomial may have exponentially large degree. Indeed, [CLZ] relegates the details of JNF manipulation to another paper [C].

We avoid the use of JNF's and instead refer to the basic structure of matrix algebras. The key concept is the *radical*. In the case of a commutative algebra $\mathcal{A}$, the radical is simply the subalgebra consisting of all *nilpotent* matrices in $\mathcal{A}$.

This concept, which is much simpler (although less well known) than the JNF, turns out to be precisely the right tool for these problems. JNF-manipulations are replaced by a simple algorithm, essentially due to Friedl and Rónyai [FR] (cf. [IRSz]) to split a commutative algebra into its "local" components. (See Section 3.2.)

Through the use of the radical, the proofs gain in elegance and generality. We note that this Extended Abstract contains essentially complete proofs of all the results stated (modulo known results).

We comment on the tools.

The case of large k requires the theory of systems of linear diophantine equations, applied to lattice intersection algorithms (cf. Sec.3.1).

A major source of difficulty was recently removed by G. Ge [Ge1-2]. The problem is to solve the 1×1 case of the group membership problem over an arbitrary algebraic number field. This problem arises even if we are interested in integral or rational matrices only.

The Lovász lattice reduction is implicitly used in several ways, both through the factoring algorithms for polynomials over algebraic number fields [LLL,Le1,La,GC1-2] required for the algebra decomposition algorithm and through the direct manipulation of the lattices of solutions in Ge's work.

3 Background

3.1 Linear diophantine equations

A *lattice* is a subgroup of $\mathbf{R}^n$ which is generated by linearly independent vectors. Such a set of linearly independent vectors is called a $\mathbf{Z}$-*basis* (or simply basis) for the lattice. Any subgroup of $\mathbf{Z}^n$ is a lattice, as is any finitely generated subgroup of $\mathbf{Q}^n$. We denote the lattice generated by $x_1, \ldots, x_m$ by $L(x_1, \ldots, x_m)$. An *affine lattice* is either the empty set, or a set of vectors of the form $x_0 + L = \{x_0 + x \mid x \in L\}$, where L is a lattice. The vector x_0 is called an *offset vector*. For basic facts on lattices and algorithms for manipulating them, we refer to [Schr, Part II]. We summarize a few essentials facts:

Lemma 3.1 *Let $x_1, \ldots, x_m$ and x be vectors in $\mathbf{Z}^n$. The following can be done in polynomial time:*

1. *Calculate a $\mathbf{Z}$-basis $b_1, \ldots, b_k$ for $L = L(x_1, \ldots, x_m)$.*
2. *Determine whether $x \in L$, and if so calculate integers $\lambda_1, \ldots, \lambda_m$ such that $x = \sum_{i=1}^{m} \lambda_i x_i$.*$\square$

We assume that algorithms which take lattices as input or produce them as output represent them by a basis. Likewise, we assume that affine lattices are represented by an offset vector together with a lattice basis.

We require the following theorem of Von zur Gathen and Sieveking and Votyakov and Frumkin (cf. [Schr, Corollary 5.3c], see also [Col] and [Ka]):

Theorem 3.2 *Given a rational matrix A and a rational vector b, we can in polynomial time calculate the affine lattice of integer solutions x to the system of equations $Ax = b$.*$\square$

Corollary 3.3 *Let $L_1, \ldots, L_k$ be affine lattices in $\mathbf{Z}^n$. We can in polynomial time calculate their intersection.*

Proof: For $1 \leq i \leq k$, let the columns of B_i be an offset vector for L_i followed by a $\mathbf{Z}$-basis for the lattice. Let n_i be the number of columns of B_i. We introduce integer variables y_{ij}, for $1 \leq i \leq k$ and $1 \leq j \leq n_i$. By y^i we denote the subvector of y with entries $y_{i1}, \ldots, y_{in_i}$. Note that $L_i = \{B_i y^i \mid y_{i1} = 1\}$. By Theorem 3.2 we may calculate the affine lattice L' of integer solutions to: For all $1 \leq i \leq k$,

$$y_{i1} = 1.$$

For all $2 \leq i \leq k$,

$$B_i y^i = B_1 y^1.$$

The affine lattice we desire is simply $L = \{B_1 y^1 \mid y \in L'\}$, so we can calculate an offset vector x_0 and a generating set $x_1, \ldots, x_m$ for L by multiplying B_1 by the y^1 subvectors of the offset vector and basis for L'. This generating set may not consist of linearly independent vectors, however, note that by Lemma 3.1, the generating set $x_1, \ldots, x_m$ may be replaced by a $\mathbf{Z}$-basis in polynomial time. $\square$

3.2 Algebra decomposition

We use algorithms from computational algebra to reduce the semigroup membership problem to simpler problems.

An *algebra* $\mathcal{A}$ over the field F is simultaneously a ring and a vector space over F, satisfying the natural associativity identities. A *matrix algebra* $\mathcal{A}$ over the field F is a nonempty set of $n \times n$ matrices over F, closed under multiplication and F-linear combination. Every finite dimensional algebra is representable as a matrix algebra.

The algebra *generated* by a set $S \subset \mathcal{A}$ is the closure of S under multiplication and linear combination. For computational purposes, our algebras will always be given by a set of generators.

The *radical* $\mathrm{Rad}(\mathcal{A})$ is the largest nilpotent ideal of $\mathcal{A}$. The quotient $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ is *semisimple*, i.e. its radical is 0.

If $\mathcal{A}$ is commutative (as is the case throughout this paper) then $\mathrm{Rad}(\mathcal{A})$ consists simply of the nilpotent elements of $\mathcal{A}$. (An element $A \in \mathcal{A}$ is *nilpotent* if $A^\ell = 0$ for some ℓ.) The commutative algebra $\mathcal{A}$ is a *local* algebra if the quotient algebra $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ is an extension field of F.

Let $\mathcal{A}$ be the commutative F-algebra generated by I (the identity element) and the commuting matrices $A_1, \ldots, A_k$. $\mathcal{A}$ can be decomposed into the direct sum

$$\mathcal{A} = \mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_m,$$

of local algebras. The decomposition can be implemented in polynomial time, combining the methods of [FR] and [IRSz]. This is accomplished in two phases. First we use the Friedl-Rónyai algorithm [FR] to decompose the semisimple algebra $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ as a direct sum of fields (cf. [Eb,GMT,Ro]). Then, the primitive idempotents $f_1, \ldots, f_m$ of $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ (the identity elements of those fields) are lifted to idempotents in $\mathcal{A}$ by the iteration of the $f \mapsto f^2(3-2f)$ map, which will approximate the idempotents of $\mathcal{A}$ modulo exponentially growing powers of $\mathrm{Rad}(\mathcal{A})$ [IRSz]. The fast convergence ensures that the bit-length of the numbers involved grow by a polynomial factor only.

We shall see that this decomposition is a useful divide-and-conquer tool, and that our problems can be solved by considering each $\mathcal{A}_j$ separately.

3.3 Multiplicative representations of algebraic numbers

In this section we consider the group case for 1×1 matrices; i.e. the algebra is the field F itself, and the exponents are arbitrary integers. This case was solved by G. Ge in [Ge1]. We review his results here.

Theorem 3.4 (Ge) *Given an algebraic number field F and nonzero elements $\alpha_1, \ldots, \alpha_k \in F$, one can in polynomial time calculate the lattices L_1 and L_2 given by*

$$L_1 = \left\{ x \in \mathbf{Z}^k \mid \prod_{i=1}^{k} {\alpha_i}^{x_i} \in O^* \right\} \qquad \textit{and} \qquad L_2 = \left\{ x \in \mathbf{Z}^k \mid \prod_{i=1}^{k} {\alpha_i}^{x_i} = 1 \right\}$$

where O^* denotes the group of units of the ring of algebraic integers of F. □

Corollary 3.5 *Given an algebraic number field F and nonzero elements $\alpha_1, \ldots, \alpha_k, \beta \in F$, one can in polynomial time calculate the affine lattice L given by*

$$L = \left\{ x \in \mathbf{Z}^k \mid \prod_{i=1}^{k} {\alpha_i}^{x_i} = \beta \right\}$$

Proof: First we apply Theorem 3.4 to the $k+1$ numbers $\alpha_1, \ldots, \alpha_k, \beta$. The affine lattice L that we seek consists exactly of those elements of L_2 with first coordinate -1, which can be found by Cor. 3.3. $\square$

A few remarks on the proof of Ge's Theorem are in order. At first it may seem easy to find the lattice L_2 by taking the (complex) logarithms of the α_i and solving linear equations. In fact, an algorithm of Hastad, Helfrich, Lagarias and Schnorr finds integer relations among real numbers [HHLS]. A difficulty with this approach is that the number of bits of precision required by the [HHLS] algorithm may be exponentially large (for recent estimates in this area, see [BW]). Ge avoids these difficulties by first calculating the lattice L_1, and by proving that for logarithms of units, polynomial precision suffices. Given L_1, Ge calculates L_2 using Lovász's basis-reduction algorithm [LLL]. An alternative approach to finding L_2 for the case $L_1 = \mathbf{Z}^k$ was found independently by G. Ostheimer [Os].

The lattice L_1 is calculated using a generalization of factor refinement (cf. [BDS]) to the case of ideals of algebraic integers. A difficulty with this is that algorithms for working with ideals usually require a $\mathbf{Z}$-basis (see [Coh]). Merely finding a $\mathbf{Z}$-basis for the ring of algebraic integers of F seems to require factoring the discriminant of F. Ge resolves this by always working within an order O (cf. [VdW, Chap. 17.3]). If his algorithm ever needs to divide by an ideal that is not invertible in O, then O is replaced by a strictly larger order.

Note that as a consequence of Ge's results, the lattices L_1 and L_2 have bases with polynomially bounded bit length. Masser [Ma] gives tighter bounds on the bit lengths required to encode these lattices.

3.4 Unipotent elements and their logarithm

The element $u \in \mathcal{A}$ is *unipotent* if $u - 1$ is nilpotent. In a commutative algebra, the set U of unipotent elements is a group under multiplication.

For a unipotent element $u = 1 + r$, we define the logarithm $\log u$ to be the sum $\log u := \sum_{i=1}^{\infty} (-1)^{i-1} r^i / i$. (Note that this sum has only a finite number of nonzero terms.) The logarithm transformation is invertible, its inverse is $\exp(r) := \sum_{i=0}^{\infty} r^i / i!$ for $r \in R$.

Let u_1 and u_2 be commuting unipotent elements of an algebra $\mathcal{A}$. Then $\log(u_1 u_2) = \log u_1 + \log u_2$ and $\log(u_1/u_2) = \log u_1 - \log u_2$. It follows that:

Proposition 3.6 *Let G be a finitely generated subgroup of the (multiplicative) group of unipotent elements of a commutative algebra $\mathcal{A}$ over $\mathbf{Q}$. Then the logarithm is an isomorphism of G to a lattice contained* $\mathrm{Rad}(\mathcal{A})$.

Thus, problems relating to such groups can often be reduced to solving systems of linear diophantine equations, to which Lemma 3.1 and Theorem 3.2 apply.

4 Reduction to the group orbit case

We assume that the algebra decomposition described in subsection 3.2 has been carried out.

For $A \in \mathcal{A}$, let $\phi_j(A)$ denote the $\mathcal{A}_j$-component of $\mathcal{A}$. Note that ϕ_j of any element of $\mathcal{A}$ is either nilpotent or invertible (in $\mathcal{A}_j$).

We consider separately the $\mathcal{A}_j$ such that $\phi_j(B) = 0$: let $T = \{j \mid \phi_j(B) = 0\}$. We divide the generating set $S = \{A_1, \ldots, A_k\}$ into three subsets:

- Let $S_1 = \{A \in S \mid \det(A) \neq 0\}$ consist of all invertible elements of S. Let $I_1 = \{i \mid A_i \in S_1\}$.
- Consider the $j \notin T$, i.e., $\phi_j(B) \neq 0$. Let $S_2 = \{A \in S \mid \exists j \notin T : \det(\phi_j(A)) = 0\}$ consist of all elements of S for which the $\mathcal{A}_j$ component is nilpotent for at least one such j. Let $I_2 = \{i \mid A_i \in S_2\}$.
- $S_3 = S \setminus (S_1 \cup S_2)$ consists of the remaining elements of S. Let $I_3 = \{i \mid A_i \in S_3\}$. The elements of S_3 are not invertible, however for $i \in S_3, 1 \leq j \leq m$, either $\phi_j(A_i)$ is invertible or $j \in T$.

Consider any solution to $\prod_{i=1}^k A_i^{x_i} = B$. Note that for $i \in I_2$, we must have $x_i < n$. Our algorithm simply cycles through all $n^{|S_2|}$ possibilities for the x_i for $i \in I_2$. Once these x_i have been assigned, let

$$A = \prod_{i \in I_2} A_i^{x_i}.$$

Now consider the elements of S_3. We introduce auxiliary variables y_i for $i \in I_3$. Let y denote the vector $(y_i)_{i \in I_3}$. By exhaustive search (of a space of order $n^{|S_3|}$), we find the set Y of all minimal solutions to

$$\forall j \in T : \left(\prod_{i \in I_3} \phi_j(A_i)^{y_i} \right) \phi_j(A) = 0$$

subject to $0 \leq y_i < n$.

Now we are ready to reduce the constructive membership problem for commutative semigroups to the group orbit case. For each assignment to the variables x_i with $i \in I_2$, we do the following: For $1 \leq j \leq m, j \notin T$, we calculate the affine lattice L_j of solutions to

$$\left(\prod_{i \in I_1 \cup I_3} \phi_j(A_i)^{x_i} \right) \phi_j(A) = \phi_j(B).$$

(Note that this is an instance of the group orbit case in which the algebra is local, and A commutes with the A_i.) Let L be the intersection of the L_j (L can be found in polynomial time by Corollary 3.3). For each $y \in Y$, we solve the following system of linear diophantine inequalities in the variables $x_i : i \in (I_1 \cup I_3)$.

- For all $i \in (I_1 \cup I_3)$, $x_i \geq 0$.
- For all $i \in I_3$, $x_i \geq y_i$.

Note that by Lenstra's algorithm [Le2], this step is in polynomial time if the dimension of L is fixed (which is certainly true if k is fixed, since $L \subseteq \mathbf{Z}^k$). Thus, we have reduced Theorem 1.1 to Theorem 1.3.

5 Algorithms for the group orbit case

Recall that the input consists of a set $S = \{A_1, \ldots, A_k\}$ of commuting matrices, together with matrices A and B. We seek the affine lattice of solutions to (2). Let G denote the group generated by the A_i, and let V denote the vector space F^n on which these matrices act.

5.1 The case when A is square and commutes with the A_i

In this case we reduce the group orbit problem to the group case of the membership problem. (This subcase is the one encountered in the previous subsection in the reduction of the semigroup membership problem to the group orbit case.)

In our case, if (2) has any solutions then B commutes with the A_i and A and B have the same image and kernel (these conditions are easily verified). Let $v_1, \ldots, v_n$ be a basis for V such that $v_{t+1}, \ldots, v_n$ is a basis for the kernel of A. Let W be the image of A. Note that W is a G-invariant subspace. Let $\rho : G \to GL(W)$ be the restriction of G to W. By construction, $Av_1, \ldots, Av_t$ and $Bv_1, \ldots, Bv_t$ are bases for W. Let $C \in GL(W)$ be the change of basis matrix defined by $C(Bv_i) = Av_i$ for $1 \leq i \leq t$. Then $x_1, \ldots, x_k$ is a solution to (2) iff $\prod_{i=1}^k \rho(A_i)^{x_i} = C$, so we have reduced Theorem 1.1 to Theorem 1.2.

5.2 Reduction of the group orbit case to the unipotent case

Now we consider the general group orbit case, where A and B are $(n \times \ell)$ matrices. We may work separately with the ℓ columns of A. The affine lattice of solutions to (2) is the intersection of the ℓ affine lattices obtained from working with each column. Thus, by Corollary 3.3, it is enough to find the affine lattice of solutions in x_i to

$$\left(\prod_{i=1}^{k} A_i^{x_i}\right) v = w \tag{3}$$

for given column vectors v and w.

Let $V = V_1 \oplus \ldots \oplus V_m$ be the decomposition of V corresponding to the decomposition of $\mathcal{A}$, i.e. $V_j = \mathcal{A}_j V$. For $1 \leq j \leq m$, let v^j denote the projection of v onto V_j. Then $(x_1, \ldots, x_k)$ is a solution to (3) iff for all $1 \leq j \leq m$ we have:

$$\left(\prod_{i=1}^{k} \phi_j(A_i)^{x_i}\right) v^j = w^j.$$

Therefore, again by Corollary 3.3, it suffices to work separately in each V_j, and take the intersection of the m affine lattices obtained.

We may therefore assume that $m = 1$, i.e., $\mathcal{A}$ is a local algebra. Set $R = \mathrm{Rad}(\mathcal{A})$ $K := \mathcal{A}/\mathrm{Rad}(\mathcal{A})$; K is a field. By extending the domain of scalars we may assume $K = F$. Now the elements of $\mathcal{A}$ have the form $\lambda I + N$ where $\lambda \in K$ and $N \in R$. It is easy to find a basis $e_1, \ldots, e_n$ for V such that R consists of strictly upper triangular matrices (zeros in the diagonal). (Note that this does not require JNF's.) With respect to this basis, let $(v_1, \ldots, v_n)^T = v$ and $(w_1, \ldots, w_n)^T = w$. Let s be the largest index such that v_s is nonzero (if $v = 0$ then the problem is trivial). Then, for any $g \in G$ with eigenvalue $\lambda \in F$, we have $(gv)_s = \lambda v_s$ and $(gv)_j = 0$ for $j > s$. Therefore, if solutions to (3) exists, we must have that s is the largest index such that w_s is nonzero. For $1 \leq i \leq k$, let $\alpha_k \in F$ be the eigenvalue of A_k. Let $\alpha = w_s/v_s$. Note that any solution to (3) is a solution to

$$\prod_{i=1}^{k} {\alpha_i}^{x_i} = \alpha. \tag{4}$$

By Ge's algorithm (cf. Corollary 3.5), the affine lattice of solutions to (4) can be found in polynomial time. If this affine lattice is nonempty, let it be generated by the basis $b_1, \ldots, b_r$ and the offset vector b_0. The $b_1, \ldots, b_r$ correspond to generators for the unipotent subgroup H of G, and the offset vector b_0 corresponds to an element of G with eigenvalue α. To be precise, the subgroup H of unipotent elements of G is generated by the elements h_i for $1 \leq i \leq r$, where

$$h_i = \prod_{j=1}^{k} {A_j}^{b_{ij}}.$$

The element $g_0 = \prod_{j=1}^{k} {A_j}^{b_{0j}}$ has eigenvalue α. To calculate g_0 and the h_i, we write the elements A_i as $\alpha_i u_i$, where u_i is unipotent. Then computing g_0 and the h_i reduces to evaluating expressions of the form

$$\prod_{i=1}^{k} {u_i}^{x_i} = \exp(\sum_{i=1}^{k} x_i \log u_i).$$

Both the exp and log functions are computable in polynomial time, so we are able in this way to compute g_0 and the h_i. Let $v' = g_0 v$. In order to solve (3), it suffices to solve

$$\left(\prod_{i=1}^{r} {h_i}^{y_i}\right) v' = w,$$

which is simply an instance of (3) with a unipotent group.

5.3 Two algorithms for the unipotent group case

We give two algorithms for the unipotent case of the group orbit problem. One of the algorithms is Monte Carlo, the other deterministic. By the reductions in the preceding subsection, we consider the problem of finding the affine lattice of solutions to (3) where the A_i are commuting unipotent matrices.

Even if we aim at a deterministic algorithm, the Monte Carlo algorithm will serve a theoretical purpose, namely its analysis is our way to guarantee that the solutions have a small (polynomial size) description; we are unable to prove this directly for the deterministic algorithm we present.

The Monte Carlo algorithm proceeds as follows. First, by considering $\mathcal{A}$ as a vector space over F and solving linear equations, we obtain a basis and an offset vector for the affine subspace $\mathcal{U} = \{X \in 1 + \mathrm{Rad}(\mathcal{A}) \mid Xv = w\}$. By the Schwartz–Zippel lemma ([Schw], [Zi]) we will with high probability find a basis and an offset vector for the affine subspace $\mathcal{L} = \{\log X \mid X \in \mathcal{U}\}$ by taking the logarithms of $O(n^2)$ random elements of X (chosen independently with coordinates uniformly selected from $\{0, \ldots, 2n\}^d$ where d is the dimension of $\mathcal{U}$). Solving (3) now is equivalent to finding the intersection of $\mathcal{L}$ with the lattice generated by the logarithms of the A_i, which can be done in polynomial time by Theorem 3.2.

Now we describe a deterministic algorithm for the unipotent case. As in the general group orbit case, we work with a basis with respect to which $\mathcal{A}$ consists of upper triangular matrices. Let V_r denote the span of the first r basis vectors. Let L_r denote the affine lattice of solutions to

$$\left(\prod_{i=1}^{k} A_i{}^{x_i}\right) v \in w + V_r.$$

Note that the above Monte Carlo algorithm can be used to find L_r in polynomial time, so in particular L_r has a basis and an offset vector with polynomially bounded bit length. Note that $L_n = \mathbf{Z}^k$. We show how to find L_{r-1} from L_r. The basis and offset vector correspond to generators $h_1, \ldots, h_\ell$ of the subgroup H which fixes $v + V_r$ and an element g_0 which maps $v + V_r$ to $w + V_r$. As in the preceding subsection, g_0 and the h_i can be calculated in polynomial time. For $h \in H$ and $u \in v + V_r$, the r coordinate of hu differs from the r coordinate of u by an amount $\sigma(h)$ that depends only on h. The function $\sigma : H \to F$ is a homomorphism to the additive group of F. Therefore, we may calculate L_{r-1} from L_r by solving linear equations. However, we need to take some care to insure that the bit lengths of the coefficients used to express L_r remain polynomially bounded. As noted above, the analysis of the Monte Carlo algorithm proves that L_r has a basis with sufficiently small coefficients. It is enough therefore to adopt the convention that all affine lattices are represented by a lattice basis in Hermite normal form, together with an offset vector which, when projected orthogonally onto the span of the lattice, is a linear combination of the basis vectors with all coefficients bounded by $1/2$ in absolute value.

This completes a proof of Theorem 1.3, which implies Theorem 1.1 (as shown above) as well as Theorem 1.2 (take A to be the identity matrix)$\Box$.

The group case has a somewhat simpler algorithm, which we present in the next subsection, giving another proof of Theorem 1.2.

5.4 The group case

Let $A_1, \ldots, A_k$ and B be commuting invertible matrices. We wish to find the affine lattice L of solutions to (1). As in Section 4, we may assume $\mathcal{A}$ is local and the field $K := \mathcal{A}/\mathrm{Rad}(\mathcal{A})$ coincides with F. – We factor each A_i as $\alpha_i u_i$ and B as βv where $\alpha_i, \beta \in K$ and u_i, v are unipotent. Let L_1 be the affine lattice of integer solutions to $\prod_{i=1}^k \alpha_i{}^{x_i} = \beta$. Let L_2 be the affine lattices of integer solutions to $\sum_{i=1}^k x_i \log u_i = \log v$. We find L_1 by Ge's algorithm (cf. Corollary 3.5), and L_2 by solving linear diophantine equations (cf. Theorem 3.2). The set of solutions to (1) is $L_1 \cap L_2$, completing the proof of Theorem 1.2.$\Box$

References

[BDS] E. Bach, J. Driscoll, J. O. Shallit: Factor refinement, *Proc 1st ACM-SIAM SODA* (1990), 201–211. *J. Algorithms*, to appear.

[BW] A. Baker, G. Wüstholz: Logarithmic forms and group varieties, *J. reine angew. Math.* **442** (1993), 19–62.

[BB] R. Beals, L. Babai: Las Vegas algorithms for matrix groups, *Proc. 34th IEEE FOCS* (1993), 427–436.

[BBR] L. Babai, R. Beals, D. Rockmore: Deciding finiteness of matrix groups in deterministic polynomial time, *Israel J. Math.*, to appear.

[Be] M. Beaudry: Membership testing in commutative transformation semigroups, *Information and Computation* **79** (1988), 84-93.

[CLZ] J-y. Cai, R. J. Lipton, Y. Zalcstein: The complexity of the membership problem for 2-generated commutative semigroups of rational matrices, *Proc 35th IEEE FOCS* (1994), 135–142.

[Coh] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math. **138**, Springer-Verlag, Berlin, 1993.

[Col] G. E. Collins, Subresultants and reduced polynomial remainder sequences, *J. ACM* (1967), 128–142.

[Eb] W. M. Eberly: Decomposition of algebras over finite fields and number fields, *Computational Complexity* **1** (1991), 179-206.

[FR] K. Friedl, L. Rónyai: Polynomial time solutions of some problems in abstract algebra, *Proc 17th ACM STOC* (1985), 153–162.

[Ge1] Guoqiang Ge, Algorithms related to multiplicative representations of algebraic numbers, PhD thesis, Math Dept, U. C. Berkeley, 1993.

[Ge2] G. Ge, Testing equalities of multiplicative representations in polynomial time, *Proc 34th IEEE FOCS* (1993), 422–426.

[GMT] P. Gianni, V. Miller, B. Trager: Decomposition of algebras, *Lecture Notes in Computer Science* **358**, Springer-Verlag 1988, 300-308.

[GC1] D.Yu. Grigoryev, A.L. Chistov: Polynomial–time factoring of the multivariable polynomials over a global field. Preprint, LOMI E-5-82, 1982, 39 pp.

[GC2] D.Yu. Grigoryev, A.L. Chistov: Fast decomposition of polynomials into irreducible ones and the solution of systems of algebraic equations, *Soviet Math. Dokl.* **29** (1984), 380–383.

[HHLS] J. Hastad, B. Helfrich, J. Lagarias, C. P. Schnorr: Polynomial time algorithms for finding integer relations among real numbers, *Proc 3rd STACS* (1986), 105–118.

[IRSz] G. Ivanyos, L. Rónyai, Á. Szántó: Decomposition of algebras over $F_q(X_1, \ldots, X_m)$, *Applicable Algebra in Engineering, Communication and Computing* **5** (1994), 71-90.

[Ka] R. Kannan: The size of numbers in the analysis of certain algorithms, Ph.D. Thesis, Operations Research Dept., Cornell University, Ithaca, NY 1980.

[KL] R. Kannan, R. Lipton: Polynomial-time algorithms for the orbit problem, *J. ACM* **33**, No. 4 (1986), 808–821.

[La] S. Landau: Factoring polynomials over algebraic number fields, *SIAM J. Comput.* **14** (1985), 184–195; Erratum in *SIAM J. Comput.* **20** (1991).

[Le1] A. K. Lenstra: Factoring polynomials over algebraic number fields, *Proc. EURO-CAL'83*, Springer L.N.C.S. Vol. 162, 1983, pp. 245–254.

[Le2] H. W. Lenstra: Integer programming with a fixed number of variables, *Mathematics of Operations Research* **8** (1983), 538–548.

[LLL] A. K. Lenstra, H. W. Lenstra, L. Lovász: Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.

[Lu] E. M. Luks: Computing in solvable matrix groups, *Proc. 33rd IEEE FOCS* (1992), 111–120.

[Ma] D. W. Masser, Linear relations on algebraic groups, in *New Advances in Transcendence Theory*, A. Baker, ed, Cambridge University Press, 1988, 248–262.

[Mi] K. A. Mihaĭlova: The occurrence problem for a direct product of groups (in Russian), *Dokl. Akad. Nauk* **119** (1958), 1103–1105.

[Os] G. Ostheimer, private communication.

[Pa] M. S. Paterson: Undecidability in 3 by 3 matrices, *J. of Math. and Physics* **49** (1970), 105-107.

[Ro] L. Rónyai: Computing the structure of finite algebras, *Journal of Symbolic Computation* **9**, (1990), 355-373.

[Schr] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, New York, 1986.

[Schw] J. T. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, *J. ACM* **27** (1980), 701–717.

[VdW] B. L. van der Waerden, *Algebra*, Vol. II., Springer-Verlag 1991.

[Zi] R. E. Zippel: Probabilistic algorithms for sparse polynomials, *Proc. EUROSAM 79*, L.N.C.S. 72 (1979), Springer-Verlag, pp. 216–226.