THE ORBIT PROBLEM IS DECIDABLE

Ravindran Kannan and Richard J. Lipton†

Computer Science Division
University of California, Berkeley

Introduction

The "accessibility problem" for linear sequential machines (Harrison [7]) is the problem of deciding whether there is an input x that sends such a machine from a given state q_1 to a given state q_2. Harrison [7] showed that this problem is reducible to the "orbit problem:" Given $A \varepsilon Q^{n\times n}$ does there exist $i \varepsilon \mathrm{N}$ such that $A^i\mathbf{x} = y$.* We will call this the "orbit problem" because the question can be rephrased as: Does y belong to the orbit of $\mathbf{x}$ under A where the "orbit of $\mathbf{x}$ under A" is the set $\{A^i\mathbf{x}: i = 0,1,2,\cdots\}$. ($A^0$ is the identity matrix I.) In Harrison's original problem the elements of $A, \mathbf{x}$, and y were members of an arbitrary "computable" field. In view of the lack of structure of such fields, we study only the rationals. Shank [13] proves that the orbit problem is decidable for the rational case when $n = 2$. The current paper establishes that for the general rational case, the problem is decidable - and in fact polynomial-time decidable.

We wish to give a brief idea of our approach to the problem. This requires the following definitions which should make the paper self-contained. These definitions may be found in any basic algebra text (e.g., Birkoff and MacLane [2]). An *algebraic number* is the root of a polynomial in $Q[x]$. An algebraic number is said to be an *algebraic integer* if it is the root of a monic polynomial with integer coefficients. For a matrix A (algebraic number α), the minimal polynomial of A (of α) denoted $f_A(x)$ $(f_\alpha(x))$ is the least degree monic polynomial in $Q[x]$ such that $f_A(A) = 0$ $(f_\alpha(\alpha) = 0)$. For algebraic numbers $\alpha_1,\alpha_2,\cdots,\alpha_n$, $Q(\alpha_1,\alpha_2,\cdots,\alpha_n)$ denotes the extension of the rationals by $\alpha_1,\alpha_2,\cdots,\alpha_n$. $(Q(\alpha_1,\alpha_2,\cdots,\alpha_n)$ can be thought of as the set of all expressions in $\alpha_1,\alpha_2,\cdots,\alpha_n$ with rational coefficients.) Such a field is called a *number field.*

Let I be the set of all algebraic integers. Then it is known that I is a ring. Thus for any number field F, $F\cap I$ is a ring. An ideal S of $F\cap I$ is a set satisfying the following conditions: S is a subgroup under addition and $\alpha \varepsilon S$, $\beta \varepsilon F\cap I \Rightarrow \alpha\beta \varepsilon S$. For any $\alpha \varepsilon F\cap I$, we define (α), *the ideal generated by* α to be the smalled ideal of $F\cap I$ that contains α. Whereas the unique factorization theorem does not hold for all number rings, it holds for ideals of number rings. To be more precise, an ideal S of $F\cap I$ is said to be a *prime* ideal if for $\alpha,\beta \varepsilon F\cap I, \alpha\beta \varepsilon S \Rightarrow \alpha \varepsilon S$ or $\beta \varepsilon S$. For two ideals S_1 and S_2 in $F\cap I$, we define the product of S_1 and S_2, S_1S_2, to be the smallest ideal containing all products of the form $\alpha\beta$ where $\alpha \varepsilon S_1$, $\beta \varepsilon S_2$. Then we have the *fundamental theorem of ideal theory* (unique

† This research was supported in part by National Science Foundation grants MCS77-09906-A02 and MCS79-20409.

* See a list of notation at the end of the paper.

factorization theorem for ideals of a number ring): In the domain of algebraic integers of a number field, every ideal can be expressed uniquely, except for order, as the product of prime ideals.

Let A be in $F^{n\times n}$ where F is any field. Then A is said to be *similar* over F to $B \varepsilon F^{n\times n}$ if there exists an S in $F^{n\times n}$, S invertible in $F^{n\times n}$ such that $B = SAS^{-1}$.

Let us now examine a plausible approach that attempts to show that some quantity associated with $A^i x$ grows with i and hence we can derive an upper bound on i such that $A^i x = y$. Suppose for the moment that the roots of $f_A(x)$ are all distinct. Then it is known (Birkoff and MacLane [2]) that A is diagonalizable, i.e., there is an $S \varepsilon (Q(\alpha_1,\alpha_2,\cdots,\alpha_n))^{n\times n}$ where $\alpha_1,\alpha_2,\cdots,\alpha_n$ are the roots of $f_A(x)$ such that SAS^{-1} = a diagonal matrix D in $Q(\alpha_1,\alpha_2,\cdots,\alpha_n)^{n\times n}$. Hence we have $A^i x = y \Longleftrightarrow S^{-1}(SAS^{-1})^i Sx = y \Longleftrightarrow S^{-1}D^i Sx = y \Longleftrightarrow D^i(Sx) = Sy$. Let $x' = Sx$ and $y' = Sy$. Then $A^i x = y \Longleftrightarrow D^i x' = y' \Longleftrightarrow (D_{jj})^i x'_j = y'_j$ for $j = 1,2,\cdots,n$ (since D is diagonal). Hence the problem is reduced to several problems of the form $\alpha^i = \beta$ where α and β are algebraic numbers. Now, if $|\alpha| > 1$, then clearly $|\alpha|^i$ monotonically increases and we can bound i. Similàr reasoning holds when $|\alpha| < 1$. If $|\alpha| = 1$ and α is a root of unity, then $\alpha^j = 1$ for some j and hence the only values of i to be checked are $i = 1,2,\cdots,j$. The real "problem case" is when $|\alpha| = 1$ and α is not a root of unity as well as the case when $f_A(x)$ has repeated roots (whence A need not be diagonalizable).

To handle all these cases and circumvent the use of cumbersome similarity transformations and canonical forms, we use a natural relation between matrices and algebraic numbers (Theorem 3.1). We first outline here our method of attack. In Section 1, the orbit problem is reduced to the following problem: Given an n by n matrix A of rationals and a polynomial $q(x)$ with rational coefficients, does there exist a natural number i such that $A^i = q(A)$? If now, α is a root of the minimal polynomial of A then, $A^i = q(A)$ implies $\alpha^i = q(\alpha)$ (Theorem 3.1). We use this fact to solve our problem. The key ideas are as follows:

The minimal polynomial of A has a root α which is not an algebraic integer. In this case, by the unique factorization theorem for ideals of a number field, there is a prime ideal that divides the ideals generated by the numerator and denominator of
fact that the norm of any prime ideal is at least 2 can be used to derive a bound on i.

The minimal polynomial of A has a root which is an algebraic integer but not a root of unity. We use a theorem of Blanksby and Montgomery that asserts: If an algebraic integer of degree n is not a root of unity, then it has a conjugate of magnitude at least $1 + (1/30\, n^2 \log n)$. Thus since the magnitude of $q(\alpha)$ can be bounded, we again have a bound on i. The remaining case is

All the roots of the minimal polynomial of A are roots of unity. In this case, we can determine exactly what the roots are. If there are no repeated roots, i can be found by solving a system of simultaneous congruences. If there are repeated roots, then we use the fact that $A^i = q(A)$ if and only if $B^i = q(B)$ whenever B has the same minimal polynomial as A. We replace A by a matrix B which is a direct sum of Jordan blocks with elements from the splitting field of the minimal polynomial of A. The structure of B then enables us to solve the problem. Of course this entails doing computations on algebraic numbers which is easily accomplished by treating them as formal polynomials.

Section 1

In this section, we prove that the orbit problem, restated for convenience as problem (1.1), is polynomially reducible to problem (1.2).

(1.1) Given $A \varepsilon Q^{n\times n}$, $x, y \varepsilon Q^n$, does there exist a nonnegative integer i such that $A^i x = y$?

(1.2) Given $A, D \varepsilon Q^{n\times n}$, does there exist a nonnegative integer i such that $A^i = D$?

Define $\nu = \max \ell : \{x, A^1x, A^2x, \cdots, A^\ell x\}$ are linearly independent. Let $C = [x \mid Ax \mid \ldots \mid A^\nu x]$ be the $(\nu+1) \times n$ matrix of rank $\nu+1$. Note that since matrix multiplication and rank finding can be done in polynomial-time ν and C can be computed in polynomial-time given A and x.

Case 1: $\nu = n-1$. Then C is an $n \times n$ invertible matrix and therefore $A^i x = y \Leftrightarrow A^i C = [y \mid Ay \mid \ldots \mid A^\nu y] \Leftrightarrow A^i = [y \mid Ay \mid \ldots \mid A^\nu y] C^{-1} = D$. Since D can be computed in polynomial-time, we have completed the reduction in this case.

Case 2: $\nu \leq n-2$. In this case we reduce the problem (1.1) to a problem of the same form, but in $\nu+1$ dimensions. Note that $\nu+1 \leq n-1$. (Intuitively, it is reasonable that this can be done. As is explained later, the column space of C (called the cyclic space generated by x under A) is where all $A^i x$ lie and thus, one should expect to be able to shift the entire scenario to this space which is of dimension $\nu+1$. This is precisely what happens here.) After at most $n-1$ such reductions, we either end up with a problem of the form (1.2) or a problem of the form (1.1) in 1 dimension in which case the solution is trivial.

By the definition of ν, there are rational numbers $a_\nu^{(\nu+1)}, a_{\nu-1}^{(\nu+1)}, \cdots, a_0^{(\nu+1)}$ such that

$$(1.3) \quad A^{\nu+1}x = \sum_{j=0}^{\nu} a_j^{(\nu+1)} A^j x \quad \text{where } A^0 = I.$$

Further from (1.3),

$$A^{\nu+2}x = \sum_{j=0}^{\nu} a_j^{(\nu+1)} A^{j+1}x = a_\nu^{(\nu+1)} A^{\nu+1}x + \sum_{j=0}^{\nu-1} a_j^{(\nu+1)} A^{j+1}x = a_\nu^{(\nu+1)} \left(\sum_{j=0}^{\nu} a_j^{(\nu+1)} A^j x \right) + \sum_{j=0}^{\nu-1} a_j^{(\nu+1)} A^{j+1} x$$

(by (1.3)). Thus $A^{\nu+1}x, A^{\nu+2}x \cdots$ are all expressible as combinations of $x, Ax, \cdots, A^\nu x$. The lemma below gives the explicit expressions of these combinations.

Lemma 1.1: $\forall \ell \geq \nu+2$, the rational numbers $a_0^{(\ell)}, a_1^{(\ell)}, a_2^{(\ell)}, \cdots, a_\nu^{(\ell)}$ defined recursively by (1.4) satisfy (1.5).

$$(1.4) \quad \begin{pmatrix} a_0^{(\ell)} \\ a_1^{(\ell)} \\ \cdot \\ \cdot \\ \cdot \\ a_\nu^{(\ell)} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0^{(\nu+1)} \\ 1 & 0 & \ldots & 0 & a_1^{(\nu+1)} \\ 0 & 1 & 0 & 0 & a_2^{(\nu+1)} \\ & \cdot & \cdot & & \cdot \\ 0 & \ldots & \ldots & 1 & a_\nu^{(\nu+1)} \end{pmatrix} \begin{pmatrix} a_0^{(\ell-1)} \\ a_1^{(\ell-1)} \\ \cdot \\ \cdot \\ \cdot \\ a_\nu^{(\ell-1)} \end{pmatrix}$$

$$(1.5) \quad A^\ell x = \sum_{j=0}^{\nu} a_j^{(\ell)} (A^j x) = C\, a^{(\ell)} \quad (\text{where } a^{(\ell)} \text{ denotes the column vector on the left of (1.4)}).$$

Proof: Suppose $A^\ell x = \sum_{j=0}^{\nu} a_j^{(\ell)} A^j x$ and $\ell \geq \nu+2$. Then $A^{\ell+1}x = \sum_{j=0}^{\nu} a_j^{(\ell)} A^{j+1} x = \sum_{j=0}^{\nu} \left\{ a_{j-1}^{(\ell)} + a_\nu^{(\ell)} a_j^{(\nu+1)} \right\} A^j x$ where $a_{-1}^{(\ell)} = 0$. Hence the lemma. □

Letting A' denote the $(\nu+1) \times (\nu+1)$ coefficient matrix in (1.4), we get by applying (1.4) repeatedly,

$$(1.6) \quad a^{(\ell)} = (A')^{\ell-(\nu+1)}\, a^{(\nu+1)} \quad (\ell \geq \nu+2).$$

We now reduce the problem (1.1) to a problem of the same form, but with A' rather than A as the coefficient matrix. Note that since $\nu+1 \le n-1$, this will be a lower dimensional problem. Consider the system of equations:

(1.7) $Cs = y$ where $s \in Q^{\nu+1}$ are the unknowns.

Lemma 1.2: The system (1.7) has at most one solution s. If (1.7) has no solution, then $A^i x \neq y$ for any i.

Proof: The first assertion follows from the fact that the columns of C are linearly independent. Now suppose that $A^i x = y$ for some i. If $i \le \nu$, then $s = e_i$, the i^{th} unit vector is a solution to $Cs = y$. If $i \ge \nu+1$, then by (1.5), $A^i x = Ca^{(i)} = y \Rightarrow s = a^{(i)}$ is a solution to (1.7). □

Now our strategy is as follows: we first find in polynomial-time the unique s_0 satisfying $Cs_0 = y$. (If none exists, lemma 1.2 assures us that we can quit.) If s_0 is a unit vector or if $s_0 = a^{(\nu+1)}$, then we know that problem (1.1) is answered in the affirmative. If not, $A^i x = y \Rightarrow i \ge \nu+2$. Since s_0 gives the unique way in which the columns of C may be combined to give y, if $A^i x = y$, then $A^i x$ must equal the same combination of the columns of C. More precisely, $A^i x = y$ for $i \ge \nu+2 \Leftrightarrow Ca^{(i)} = y$ (by (1.5)) $\Leftrightarrow C\left[(A')^{i-(\nu+1)}\right]a^{(\nu+1)} = y$ (by (1.6)) $\Leftrightarrow (A')^{i-(\nu+1)}a^{(\nu+1)} = s_0$ (by lemma (1.2)). Thus the problem is of finding a j such that $(A')^j a^{(\nu+1)} = s_0$. This is a problem of the same form where A', s_0 and $a^{(\nu+1)}$ are polynomial time computable from $A, x,$ and y. ($a^{(\nu+1)}$ may be obtained as the unique solution to the system of simultaneous equations (1.3) and A' is easily obtained from $a^{(\nu+1)}$ by the way it is defined (see (1.4)).

It appears that at this stage, we have finished the reduction: at most $n-1$ iterations of the above process leads either to a problem of the form (1.2) or a trivially solved problem and as shown in the discussion above, each iteration can be done in *polynomially many arithmetic operations*. So one is tempted to conclude that the entire process can be carried out in *polynomial-time*. However, note that in obtaining A' from A, we had to solve a system of simultaneous equations. Thus in the worst case, we could have $\|A'\| > \|A\|^2$. Thus after $\frac{n}{2}$ iterations the length of the binary representation of the numbers involved may themselves be as large as $2^{n/2}\cdot$(length of the numbers in the original output). Hence we do not have a proof that such an algorithm is polynomial-time bounded.

To avoid this problem, we show that with some care, we need to perform this iteration at most thrice (irrespective of n) before we are in case 1.

Claim 1.1: Without loss of generality, we can assume that $a_0^{(\nu+1)} \neq 0$.

Proof: If $a_j^{(\nu+1)} = 0\ \forall j$, then $A^{(\nu+1)}x = 0$ and the problem is easily solved by checking if $A^j x = y$ for any $j \le \nu$ or if $y = 0$. Thus suppose $a_j^{(\nu+1)} \neq 0$ for some j and suppose λ is the minimum such j. Suppose $\lambda \ge 1$. We first check in polynomial-time if $A^j x = y$ for any $j \le \lambda - 1$. If there is, we can stop. If not, we have $A^i x = y \Rightarrow i \ge \lambda \Rightarrow A^{i-\lambda}(A^\lambda x) = y$. Substituting $x^* = A^\lambda x$, we have $\exists i: A^i x = y \Leftrightarrow \exists j: A^j x^* = y$. Thus a new problem has been defined with x^* replacing x and for this problem we define $\nu^*, C^*, (A')^*$ and $\left[(a^*)^{(\nu^*+1)}\right]$ corresponding to ν, C and A' and $a^{(\nu+1)}$ defined for the original problem. Then note that $\nu^* = \nu - \lambda$; $C^* = [x^*|Ax^*|\cdots|A^{\nu-\lambda}x^*]$. Further,

$A^{\nu+1}x = \sum_{j=0}^{\nu} a_j^{(\nu+1)}A^j x$ (from (1.3)) $= \sum_{j=\lambda}^{\nu} a_j^{(\nu+1)}A^j x$ (by the definition of λ) $= \sum_{j=0}^{(\nu-\lambda)} a_{j+\lambda}^{(\nu+1)}A^j x^*$ (since $x^* = A^\lambda x$). Thus $A^{\lambda^*+1}x^* = \sum_{j=0}^{\nu^*} a_{j+}^{(\nu+1)}A^j x^*$. Thus $(a^*)_0^{(\nu^*+1)} = a_\lambda^{(\nu+1)} \neq 0$. This finishes the proof of the claim. □

For ease of notation, we assume that A' has been replaced by $(A^*)'$ if necessary; i.e., we assume that $a_0^{(\nu+1)} \neq 0$, or equivalently let $a' \neq 0$. To start with A may or may not be singular. What we have so far shown is that after one iteration, we are either in case 1 or in case 2 and in the latter case, the problem is reducible to a lower dimensional problem involving a nonsingular matrix. In what follows, for simplicity, we will assume that we are dealing with the following problem: Given $A \in Q^{n\times n}$, A nonsingular, does there exist $i \in N$ such that $A^i x = y$? i.e., we will assume that if A were singular, one iteration has already been performed (in polynomial-time) to arrive at the above form. Let A', C, ν and $a^{(\nu+1)}$ be defined as before based on this nonsingular A. Let $M = [a^{(\nu+1)}|A'a^{(\nu+1)}|\ldots|(A')^{\nu}a^{(\nu+1)}]$. Then it follows $CM = A^{\nu+1}C = [A^{\nu+1}x|A^{\nu+2}x|\cdots|A^{2\nu+1}x]$.

Claim 1.2: A is nonsingular implies that M has rank $\nu+1$.

Proof: If A is nonsingular, then so is $A^{\nu+1}$. Thus for any vector v, $A^{\nu+1}CV = 0 \Rightarrow CV = 0 \Rightarrow v = 0$ since C has full column rank. Thus $A^{\nu+1}C$ has rank $\nu+1$ and so does CM (since $CM = A^{\nu+1}C$). Now suppose $v \neq 0$ and $Mv = 0$. Then $CMv = 0$ contradicting the fact that rank of $CM = \nu+1$. Thus M has rank $\nu+1$ under the hypothesis that A is nonsingular. □

Note that the column space of M is the cyclic space generated by $a^{(\nu+1)}$ under A'. Thus M has rank $\nu+1$ (full rank) implies that a further iteration performed on A' would land us in case 1. Thus we require at most three iterations - one to get a nonsingular A and two more to land us in case 1.

Finally, we wish to reduce problem (1.2) further to a problem of the form (1.8):

(1.8) Given $A \in Q^{n\times n}$ and $q(x) \in Q[x]$, does there exist $i \in N$ such that $A^i = q(A)$?

Note that we can assume without loss of generality that degree $q(x) \leq n$ (since the minimal polynomial of A has degree at most n). Thus given a problem of the form (1.2), we solve the n^2 simultaneous equations $\sum_{j=0}^{n} q_j A^j = D$ in the variables $q_0,\cdots,q_n$. If there is no solution $q \in Q^{n+1}$, then $A^i \neq D$ for any i. Otherwise the problem is reduced to a problem of the form (1.8).

Section 2

For any algebraic number α, we denote by $f_\alpha(x)$ the monic irreducible polynomial in $Q[x]$ satisfied by α and by n_α the degree of $f_\alpha(x)$. The following is central to our proof.

Theorem 2.1: There exists a polynomial $P(\cdot,\cdot,\cdot)$ such that for any algebraic number α and for any $q(x) \in Q[x]$, if α is not a root of unity then $\alpha^i = q(\alpha) \Rightarrow i \leq P(n_\alpha, \log\|q\|, \log\|f_\alpha\|)$. Further, if α is a s^{th} root of unity then either $I_s = \{i : \alpha^i = q(\alpha)\}$ is empty or $I_s = \{i_0 + zs \mid z \text{ in } Z\}$ where i_0 is a fixed integer satisfying $0 \leq i_0 \leq s-1$.

Proof: The second case is quite obvious. So suppose that α is not a root of unity. If α is an algebraic integer, there is a conjugate θ of α such that $|\theta| > 1 + \dfrac{1}{(30n^2\log_e 6n_\alpha)}$ (Blanksby and Montgomery [4]). Since θ is a conjugate of α we have $\alpha^i = q(\alpha) \Longleftrightarrow \theta^i = q(\theta) \Rightarrow i \leq \dfrac{\log|q(\theta)|}{\log|\theta|}$. $\log|q(\theta)| \leq \log[(n+1)\,|\theta|^n\,\|q\|] = \log(n+1) + n\cdot\log|\theta| + \log\|q\|$ because $|\theta| > 1$. Thus $\alpha^i = q(\alpha) \Rightarrow i \leq \dfrac{\log(n+1) + \log\|q\|}{\log|\theta|} + n \leq (30n^2\log_e 6n)\log(n+1) + \log\|q\| + n = p(n,\log\|q\|,\log\|f_\alpha\|)$ (say) where p is certainly a polynomial.

We now consider the case when α is not an algebraic integer. (In particular, of course, it is not a root of unity.) Let $\alpha_1,\alpha_2,\beta_1,\beta_2$ be algebraic integers such that $\alpha = \alpha_1/\alpha_2$ and $q(\alpha) = \beta = \beta_1/\beta_2$. Then $\alpha^i = q(\alpha) = \beta \Longleftrightarrow \alpha_1^i\beta_2 = \alpha_2^i\beta_1$. Since α is not an algebraic integer the ideals (α_1) and (α_2)

generated by α_1 and α_2 respectively are not equal. $(\alpha_1) \neq (\alpha_2) \Rightarrow \exists$ a prime ideal P such that $P^{\ell_1} \| (\alpha_1)$ and $P^{\ell_2} \| (\alpha_2)$ and $\ell_1 \neq \ell_2$. (Here $P^{\ell} \| (\alpha)$ means that P^{ℓ} divides (α) and $P^{\ell+1}$ does not.) Also let $P^{\ell_3} \| (\beta_1)$ and $P^{\ell_4} \| (\beta_2)$. Then $\alpha_1^i \beta_2 = \alpha_2^i \beta_1$ can hold only if P divides the ideals generated by both sides an equal number of times, i.e., only if $i\ell_1 + \ell_4 = i\ell_2 + \ell_3$. (The key fact used here is that the unique factorization theorem holds for ideals of any algebraic number ring.)

Assume without loss of generality that $\ell_1 > \ell_2$. Then since $\ell_4 \geq 0$, it follows that $i = \frac{\ell_3 - \ell_4}{\ell_1 - \ell_2} \leq \frac{\ell_3}{\ell_1 - \ell_2} \leq \ell_3$. We only need to show that ℓ_3 is "small." Since P^{ℓ_3} divides (β_2), it follows that $N((P)^{\ell_3}) \mid N((\beta_2))$ where now this is the norm on ideals not algebraic integers. But $N((P)) \geq 2$, thus $\ell_3 \leq \log_2 N((\beta_2))$. $B\alpha$ is an algebraic integer for some positive rational integer B with $B \leq \|f_\alpha\|$ (Marcus [10]). Thus, we can choose $\alpha_2 = B$ and $\beta_2 = B^n$ and apply the above argument. We then have $\alpha^i = q(\alpha) \Rightarrow i \leq n \log_2 \|f_\alpha\|$. Taking $P(\cdot,\cdot,\cdot)$ to be the maximum of the polynomials in the two cases, we have theorem 2.1. □

Remark: The proof of theorem 2.1 is as short as it is only because the remarkable result of Blanksby and Montgomery [4] is available to us. This result is a substantial strengthening of a theorem of Kronecker's [9] which showed that if an algebraic integer is not a root of unity, then at least one of its conjugates has absolute value greater than one. It was first improved on by Ore [11]. Schinzel and Zaasenhaus [12] showed that if α is an algebraic integer of degree n over Q and is not a root of unity, then $|\overline{\alpha}| = \max\limits_{\substack{\theta \text{ conjugate} \\ \text{of } \alpha}} |\theta| > 1 + \frac{c}{2^n}$; c a constant. Subsequent strengthening by Blanksby [3] increased the right hand side to $1 + \frac{c}{(2^{\frac{1}{2}} + \varepsilon)^n}$.

Section 3

We first collect some useful facts in the following theorem:

Theorem 3.1: Let F be any field. Suppose A in $F^{n\times n}$ has minimal polynomial $p(x)$ belonging to $F[x]$ and let $r(x)$ and $q(x)$ be elements of $F[x]$. Then,

$$(3.1) \qquad r(A) = q(A)$$

$$(3.2) \qquad \Longleftrightarrow r(x) = q(x) (\operatorname{mod} p(x)).$$

Further, if $F = Q$ and $p(x)$ is irreducible over Q and has α as a root, then (3.1) and (3.2) are equivalent to

$$(3.3) \qquad r(\alpha) = q(\alpha).$$

Proof: Clearly to any $s(x)$ in $F[x]$, there corresponds a unique polynomial $s'(x)$ in $F[x]$ satisfying $s'(x) = s(x) (\operatorname{mod} p(x))$ and degree $s'(x) <$ degree $p(x)$. Note that by the definition of $p(x)$, $r(A) = r'(A)$ and $q(A) = q'(A)$. Thus $r(x) = q(x)(\operatorname{mod} p(x)) \Longleftrightarrow (r' - q')(x) = 0 \Longleftrightarrow (r' - q')(A) = 0$ (since degree $(r' - q')(x) <$ degree $p(x)) \Longleftrightarrow r(A) = q(A)$ (since $p(A) = 0$). If $F = Q$ and $p(x)$ is irreducible over Q and has root α, then $r(x) = q(x)(\operatorname{mod} p(x)) \Rightarrow r'(x) = q'(x) \Rightarrow r'(\alpha) = q'(\alpha) \Rightarrow r(\alpha) = q(\alpha)$ (since $p(\alpha) = 0$). Conversely, $r(\alpha) = q(\alpha) \Rightarrow r'(\alpha) = q'(\alpha) \Rightarrow (r' - q')(\alpha) = 0$. But note that $r'(x) - q'(x)$ has degree less than degree p which is the irreducible polynomial satisfied by α. Thus we must have $r'(x) = q'(x)$. □

We now are ready to present a polynomial algorithm to solve the problem (1.8). It turns out that the case when all the roots of the minimal polynomial of A are roots of unity needs special attention. We must first find the minimal polynomial $f_A(x)$ of matrix A. The following obviously polynomial algorithm does the job - though not in the most efficient manner.

```
procedure MIN_POLY(A,n)
    find A^2,A^3,...,A^n
      for i = 1 step 1 until n
        do
          if the system of n^2 equations  Σ_{j=0}^{i} Y_j A^j = 0  has a solution
              Y = (Y_0,Y_1,...,Y_i)  in the rationals, with  Y_i ≠ 0
              then return  f_A(x) = Σ_{j=0}^{i} Y_j x^j
        end
end
```

Thus the procedure returns the minimum degree polynomial satisfied by A which must obviously be a scalar multiple of the minimal polynomial. Thus the minimal polynomial $f_A(x)$ is easily found. The procedure runs in polynomial-time because solution of simultaneous equations can be done in polynomial-time.

The next procedure determines whether $f_A(x)$ has only roots of unity as its roots.

```
procedure ROOTS_OF_UNITY:
    initialize: h_j(x) ← 1  for  j = 1,2,...,(degree f_A)^2; f'_A(x) ← f_A(x);
      for  j = 1 step 1 until (degree f_A(x))^2 do
        begin
             h_j(x) ← gcd(f'_A(x),(x^j - 1)^(degree f_A));
             f'_A(x) ← f'_A(x)/h_j(x);
        end
      end
end
```

Lemma 3.2: At the end of the above procedure, $f'_A(x) = 1 \Longleftrightarrow$ all roots of $f_A(x)$ are roots of unity. Further, $h_j(x) = (C_j(x))^{k_j}$ where $k_j \geq 0$ and $C_j(x)$ is the j^{th} cyclomatic polynomial (irreducible monic polynomial in $Q[x]$ with ω_j as a root).

Proof: Let degree $f_A(x) = d$. If a j^{th} primitive root of unity is also a root of $f_A(x)$, then $C_j(x)|f_A(x)$. Thus $d \geq \phi(j)$. From elementary theory (e.g., see Apostol [1]), we get the crude bound $\phi(j) \geq \sqrt{j}$. Hence if a j^{th} primitive root of unity is a root of $f_A(x)$, we must have $d \geq \sqrt{j}$. Further, the multiplicity of any root of $f_A(x)$ is at most d. Thus at the end of the procedure, $f'_A(x)$ contains no roots of unity, but contains all the roots of $f_A(x)$ that are not roots of unity. Thus the first statement in the lemma follows. The second statement follows from the fact that when the algorithm finds $h_j(x)$, the only possible complex numbers that are roots of both $f'_A(x)$ and $(x^j - 1)$ are the j^{th} roots of unity. □

At the conclusion of the last procedure, we know which of the following three cases we are in and we handle the problem accordingly.

Case 1: There is an α not a root of unity such that $f_A(\alpha) = 0$. In this case $A^i = q(A)$ implies $x^i \equiv q(x) \bmod f_A(x)$ which then implies that $x^i \equiv q(x) \bmod f_\alpha(x)$ (since $f_\alpha(x)|f_A(x)$). Then by theorem 3.1 it follows that $\alpha^i = q(\alpha)$. Finally theorem 2.1 allows us to decide this by a polynomially bounded search.

Case 2: $f_A(x) = \prod_{j=0}^{n} (C_j(x))^{k_j}$ where each k_j is 0 or 1. In this case we argue as follows: $A^i = q(A) \Leftrightarrow x^i \equiv q(x) \bmod f_A(x) \Leftrightarrow x^i \equiv q(x) \bmod C_j(x)$ for all j such that $k_j = 1$ (Chinese Remainder Theorem) $\Leftrightarrow \omega_j^i = q(\omega_j)$ for all j such that ω_j is a root of $f_A(x)$. The last step follows by theorem 3.1. Now by theorem 2.1 it follows that i must satisfy a set of congruences of the form $i \equiv a_j \bmod j$ for a certain set of j's. Clearly it is possible in polynomial-time to determine whether or not such a system is solvable. If it is then i exists; otherwise it does not.

Case 3: $f_A(x) = \prod_{j=1}^{n} (C_j(x))^{k_j}$ where $k_j \geq 0$ and at least one k_j is 2 or more. The proof that this last case can be handled in polynomial-time is the subject of the rest of this section.

Theorem 3.3: Let f_A be as above. Then,

$$(3.4) \quad A^i = q(A) \Leftrightarrow \binom{i}{s-r} \omega_j^{(i-(s-r))} = (q(B_j))_{r,s}$$

for all j with $k_j \geq 1$ and for all s,r with $k_j \geq s \geq r \geq 1$

where $B_j \in (Q(\omega_j))^{k_j \times k_j}$ is the $k_j \times k_j$ Jordan block with eigenvalue ω_j defined in (3.6). (As will be pointed out later, the right-hand side of (3.4) is polynomial-time checkable.)

Proof: $A^i = q(A) \Leftrightarrow x^i = q(x)(\bmod f_A(x))$ (Theorem 3.1) $\Leftrightarrow x^i = q(x)(\bmod (C_j(x))^{k_j})$ $\forall j$ (Chinese remainder Theorem). Considering x^i and $q(x)$ as polynomials in $(Q(\omega_j))[x]$, we have $x^i = q(x)(\bmod (C_j(x))^{k_j}) \Rightarrow x^i = q(x)(\bmod (x-\omega_j)^{k_j}$. Conversely, $(x-\omega_j)^{k_j} | (x^i - q(x))$ in $(Q(\omega_j))[x] \Rightarrow p(x) | (x^i - q(x))$ in $Q[x]$ where $p(x)$ is the polynomial of least degree in $Q[x]$ such that $(x-\omega_j)^{k_j} | p(x)$. Since $p(x) = (C_j(x))^{k_j}$ we have,

$$(3.5) \quad x^i = q(x)(\bmod (C_j(x))^{k_j}) \Leftrightarrow x^i = q(x)(\bmod (x-\omega_j)^{k_j}) .$$

Now, we wish to apply Theorem 3.1 with $F = Q(\omega_j)$. It is easily checked that the matrix B_j belonging to $(Q(\omega_j))^{k_j \times k_j}$ has minimal polynomial $(x-\omega_j)^{k_j}$

$$(3.6) \quad B_j = \begin{pmatrix} \omega_j & 1 & 0 & \cdot & \cdot & 0 \\ & \cdot & & & & \cdot \\ & & \cdot & & & \cdot \\ & & & \cdot & & 0 \\ & \text{\Huge 0} & & & \cdot & 1 \\ & & & & & \cdot \\ & & & & & \omega_j \end{pmatrix} = \omega_j I + M \quad \text{(say)}$$

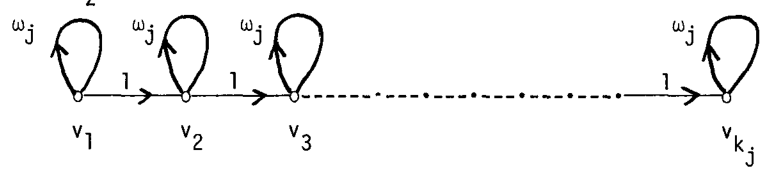
(To see this, we check that $(B_j - \omega_j I)^{k_j} = 0$. Thus $f_{B_j}(x) | (x-\omega_j)^{k_j}$. Suppose $f_B(x) = (x-\omega_j)^g$. Then $M^g = 0$. Thus we must have $g \geq k_j$. Hence $f_{B_j}(x) = (x-\omega_j)^{k_j}$.) Now by Theorem 3.1, (3.5) is equivalent to $B_j^i = q(B_j) \Leftrightarrow x^i = q(x)(\bmod (C_j(x))^{k_j})$. To sum up, we have so far proved

$$(3.7) \quad A^i = q(A) \Leftrightarrow B_j^i = q(B_j) \quad \text{for } j = 1,2,\cdots,n .$$

The lemma below explicitly calculates the entries of B_j^i and completes the proof of this theorem.

Lemma 3.4: For $k_j \geq s \geq r \geq 1$, we have $(B_j^i)_{r,s} = \binom{i}{s-r} \omega_j^{i-(s-r)}$. The entries below the diagonal in B_j^i are all zero.

Proof: B_j can be considered to be the incidence matrix of a weighted direct graph G on k_j vertices where $(B_j)_{r,s}$ = the weight on the edge from vertex r to vertex s of G. G with the weights on the edges is pictured below (v_z is the z^{th} vertex):



Then from basic graph theory (Bondy and Murty [5]):

$$(B_j^i)_{r,s} = \sum_{\substack{P:P \text{ is a} \\ \text{path of length} \\ i \text{ from } v_r \text{ to } v_s}} \{\text{product of the weights of edges of } P\}$$

For $s \geq r$, any path P of length i from v_r to v_s must consist of $(s-r)$ edges of weight ω_j. The position of the $(s-r)$ edges of weight 1 on the path uniquely determines the path. Thus there are $\binom{i}{s-r}$ such paths each with product of weights equal to $\omega_j^{i-(s-r)}$. Hence the lemma. □

Now our strategy in this case is clear. First, some k_j, say k_ℓ, is 2 or more. Then we compute $q(B_\ell)$. This can obviously be done in polynomial-time. (Note: we keep the entries of $q(B_\ell)$ as polynomials in ω_j with rational coefficients. Further, the degrees of these polynomials can of course be kept to at most n.) Then with $s = 2$ and $r = 1$ we have $A^i = q(A) \Rightarrow i\omega_\ell^{i-1} = (q(B_\ell))_{1,2}$. We thus check that $(q(B_\ell))_{1,2}$ is an integer multiple of a power of ω_ℓ. Then the ratio between $(q(B_\ell))_{1,2}$ and this unique power of ω_ℓ yields the only candidate i that can satisfy (3.7). We then use theorem 3.3 to check that $A^i = q(A)$ by checking in polynomial-time that (3.4) is indeed satisfied.

A Word of Caution: In the last case after finding i, the only possible candidate, one might try to find A^i by repeated squaring - in at most $O((\log i)\cdot n^3)$ arithmetic operations (certainly a polynomial number of operations) and check whether it equals $q(A)$. The problem with this method is that we could have $||A^{(i)/2}|| \geq ||A||^{(i)/2}$ and thus $A^{(i/2)}$ may take $\frac{i}{2}\log||A||$ bits to write down - which is an exponential number of bits since the magnitude of i is not bounded by a polynomial in the length of the input. Hence the need for the arguments in this case.

This completes the proof that the orbit problem is decidable.

Notation Used

$\mathbf{Q}$: set of rationals

$\mathbf{Z}$: set of integers

$\mathbf{N}$: set of nonnegative integers

ω_j: j^{th} primitive root of unity

$\mathbf{Q}[x]$: ring of polynomials with coefficients in $\mathbf{Q}$

$\mathbf{Z}[x]$: ring of polynomials with coeeficients in $\mathbf{Z}$

For a field F, $F^{n\times n}$ = set of $n\times n$ matrices with entries from F

For $A \in \mathbf{Q}^{n\times n}$, $||A||$ = maximum absolute value of the product of the numerator and denominator of any entry of A

For $q(x) \in \mathbf{Q}[x]$, $||q(x)||$ = maximum absolute value of the product of the numerator and denominator of any coefficient of $q(x)$

gcd ≡ greatest common divisor

For $j \in \mathbf{N}$, $\phi(j) = |\{i \mid 1 \leq i \leq j \text{ with } \gcd(i,j) = 1\}|$

For $A \in F^{n\times n}$, $A_{r,s}$ is the entry in the r^{th} row and s^{th} column of A

Acknowledgements

We are pleased to thank Mike Harrison for both telling us his question and for his kind and generous encouragement. We would also like to thank Dick Karp for his support of many kinds.

References

[1] T.M. Apostol, Introduction to analytic number theory, Springer-Verlag, Berlin (1976).

[2] G. Birkhoff and S. MacLane, A brief survey of modern algebra, 2nd ed., New York: The MacMillan Co.(1965).

[3] P.E. Blanksby, "A note on algebraic integers," *J. Number Theory 1* (1969), pp. 155-160.

[4] P.E. Blanksby and H.L. Montgomery, "Algebraic integers near the unit circle," *Acta Arithmetica* (1971), pp. 355-369.

[5] J.A. Bondy and U.S.R. Murty, Graph theory with applications, North-Holland, New York (1976).

[6] H. Cohn, A classical invitation to algebraic numbers and class fields, Springer-Verlag (1978).

[7] M. Harrison, Lectures on sequential machines, Academic Press (1969).

[8] G.T. Herman and S.D. Isard, "Computability over arbitrary fields," *J. London Math. Soc.(2),* 2(1970), pp. 73-79.

[9] L. Kronecker, "Zwei sätze über gleichungen mit ganzzahligen coeffizienten," *J. Reine unde Angewandte Mathematik,* 53 (1875), pp. 173-175.

[10] D.A. Marcus, Number fields, Springer-Verlag, Berlin (1977).

[11] O. Ore, Les corps algébriques et la théorie des idéaux, Paris, 1934.

[12] A. Schinzel and H. Zassenhaus, "A refinement of two theorems of Kronecker," *Michigan Math. J.,* 12 (1965), pp. 81-84.

[13] H.S. Shank, "The rational case of a matrix problem of Harrison," *Discrete Mathematics,* 28 (1979), pp. 207-212.