THE RATIONAL CASE OF A MATRIX PROBLEM
OF HARRISON

H.S. SHANK
Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario

Received 7 August 1975
Revised 26 March 1979

Given a $2 \times 2$ matrix $A$ and two column vectors $x$ and $y$, with all entries rational, the question
of whether there is a positive integer $n$ for which $A^n x = y$ is shown to be decidable.

1. Introduction

Let $A$ be a $2 \times 2$ matrix, and $x$ and $y$ two column vectors ($x \neq 0$) with all entries in
a computable field $F$. M. Harrison asked if it is decidable whether there is an $n$
for which $A^n x = y$. Subsequently it was asked by A. Meyer and then by Harrison
whether this is decidable even when $F$ consists of the rational numbers. We show
here that it is indeed decidable over the rationals, by outlining a procedure for
finding possible candidates $n$ or showing that there are none.

The problem partitions naturally into two pieces that are treated somewhat
differently, depending on whether the eigenvalues of $A$ are complex conjugates
on the unit circle. If they are not, the question can be settled largely by one or
another monotonicity argument.

When the eigenvalues are complex conjugates on the unit circle, the problem
can be restated as: given that $\cos \theta$ and $\cos \tau$ are rational, is there an $n$ for which
$\cos n\theta = \cos \tau$? Since, in general, $\{\cos n\theta | n = 1, 2, 3, \ldots\}$ is dense in the unit
interval, the monotonicity arguments that handle the other case are simply
unavailable. Indeed, this fact seems to support the plausibility that the question is
undecidable. However, some simple arguments about the growth of the
numerator of $\cos n\theta$ (which is necessarily rational), take care of this case.

Generalizations of this result might be to fields other than the rationals (the
original Harrison question) or to $m \times m$ matrices. For the latter it will be clear
that the methods shown here can be invoked to show decidability in many cases.
The outstanding case in which they can not (or, it is unclear that they can) is when
the eigenvalues of $A$ all occur on the unit circle and in multiplicities greater than
2.

Because there is probably little interest in many details of the partitioning into
subcases and carrying out some of the rather routine details of algebraic manipu-
lations, most will be skimmed over.
We assume that $A$ is already in rational canonical form so that (omitting the trivial case that $A$ is scalar) $A$ has the form

$$
\begin{pmatrix}
0 & 1 \\
b & 2a
\end{pmatrix}.
$$

We denote $\alpha$ and $\beta$ by, respectively,

$$
\begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}
\gamma \\
\delta
\end{pmatrix}.
$$

We omit the case $b = 0$. Sections 2, 3 and 5 handle all cases except $|a| < 1$ and $b = -1$. This case, which corresponds to the cosine question, is discussed in Section 4.

2. The case $|b| \neq 1$.

Define the sequence $b_{-1}, b_0, b_1, \ldots$ by $b_{-1} = \alpha$, and $b_0 = \beta$, and $b_{n+1} = 2ab_n + bb_{n-1}$, so that for $n \geq 0$ we have

$$
A^n \begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} = \begin{pmatrix}
b_{n-1} \\
b_n
\end{pmatrix}.
$$

Then we are interested in whether there is an $n$ for which $\gamma = b_{n-1}$ and $\delta = b_n$.

If the eigenvalues $\lambda_1$ and $\lambda_2$ of $A$ are distinct, $a^2 + b \neq 0$ and $b_n = c_1\lambda_1^n + c_2\lambda_2^n$ for suitable $c_1$ and $c_2$. Then (since $b_{n+1} - b_n\lambda_2 = c_1\lambda_1^n (\lambda_1 - \lambda_2)$ and $b_{n+1} - b_n\lambda_1 = c_2\lambda_2^n (\lambda_2 - \lambda_1)$) $b_n$ and $b_{n-1}$ satisfy

$$
b_n^2 - 2ab_nb_{n-1} - b_{n-1} = -c_1c_2(4a^2 + 4b)(-b)^{n-1}.
$$

Noting that

$$
c_1c_2 = \frac{b_1^2 - b_0^2(a^2 + b)}{4(a^2 + b)},
$$

we see that any solution $n$ must satisfy

$$
\delta^2 - 2a\gamma\delta - b\gamma^2 = -b_1^2 + b_0^2(a^2 + b)(-b)^{n-1}.
$$

We omit the (trivial) cases that $b$ or one of the $c_i$ is zero. It is clear that since $|b| \neq 1$ any candidate $n$ can be distinguished.

If the eigenvalues $\lambda_1$ and $\lambda_2$ are equal, then $b = -a^2$ and $\lambda_1 = \lambda_2 = a$, so that any candidate $n$ must satisfy

$$
\delta - a\gamma = a^n(\beta - aa).
$$

From this, if $\beta \neq aa$, any solution $n$ can be found (recall we are assuming $|b| \neq 1$). We omit the (trivial) case $\beta = aa$. 
3. The case $b = -1$ and $|a| > 1$ and the case $b = 1$.

The eigenvalues $\lambda_1$ and $\lambda_2$ are real and different. Using the matrix

$$P = \begin{pmatrix} \lambda_1 & -1 \\ \lambda_2 & -1 \end{pmatrix}$$

we have

$$PAP^{-1} = D = \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$$

and the problem becomes that of finding an $n$ for which

$$D^n(P(\alpha)) = P(\gamma).$$

A straightforward monotonicity argument can now be invoked to bound any candidates for suitable $n$.

4. The case of $b = -1$ and $|a| < 1$.

In this case $|A - xI| = x^2 - 2ax + 1$ has roots $e^{i\theta}$ and $e^{-i\theta}$, with $a = \cos \theta$. Accordingly, $A^n$ has eigenvalues $e^{in\theta}$, $e^{-in\theta}$, so that

$$|A^n - xI| = x^2 - 2 \cos n\theta x + 1.$$  \hspace{1cm} (1)

Let $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $PAP^{-1} = A^{-1}$, so that

$$A^n(\alpha) = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

requires also that

$$A^n(\delta) = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}.$$  

That is,

$$A^n(\alpha) = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

will occur only when

$$A^n(\beta \gamma) = \begin{pmatrix} \gamma & \beta \\ \delta & \alpha \end{pmatrix}.$$  

Now assume that $(\alpha \beta \gamma \delta)$ is nonsingular. The parenthetical paragraph below shows
that such an assumption is not really a restriction. Accordingly,

$$A^n = \begin{pmatrix} \gamma & \beta \\ \delta & \alpha \end{pmatrix} \begin{pmatrix} \alpha & \delta \\ \beta & \gamma \end{pmatrix}^{-1} = \frac{1}{\alpha \gamma - \beta \delta} \begin{pmatrix} \gamma & \beta \\ \delta & \alpha \end{pmatrix} \begin{pmatrix} \gamma & -\delta \\ \delta & \alpha \end{pmatrix}.$$  

Comparing coefficients of $x$ in the resulting expression for $|A^n - xI|$ and in the preceding one (1), we have

$$\cos n\theta = \frac{\gamma^2 + \alpha^2 - \beta^2 - \delta^2}{2(\alpha \gamma - \beta \delta)}. $$

That is, any candidate $n$ must satisfy this. Since both $a(=\cos \theta)$ and $\cos n\theta$ are rational, we can rewrite the question as: given that $\cos \theta = r/s$, with $(r, s) = 1$, and $\cos \theta = u/v$, with $u, v = 1$, is there an $n$ for which $\cos n\theta = u/v$?

(In case $|\beta, \delta| = 0$ then, for some $c = \pm 1$, $\delta = c\alpha$ and $\gamma = c\beta$: consider instead the equivalent problem by finding $n-1$ for which

$$A^{n-1} \begin{pmatrix} \beta \\ 2a\beta - \alpha \end{pmatrix} = \pm \begin{pmatrix} \beta \\ \alpha \end{pmatrix},$$

for which the corresponding determinant is now

$$\pm \begin{vmatrix} \beta & \alpha \\ 2a\beta - \alpha & \beta \end{vmatrix} = \pm (\beta^2 + 2a\alpha\beta + \alpha^2).$$

Since $|a|<1$, this can't be 0.)

We omit the (trivial) case of $r/s = \pm \frac{1}{2}$. For the case of $u/v = 0$, which is not covered by the above formulation of the question, note that $\cos n\theta = 0$ implies $c_{2n+1} (4n+1) \theta = \cos \theta$.

$\cos n\theta$ is a polynomial in $\cos \theta$, with integer coefficients. If this is $p_n(\cos \theta) = p_n(r/s)$, then $s^n p_n(r/s)$ is an integer, say $c_n$. It is given by

$$2rc_{n+1} - s^2 c_n = c_{n+2}, \tag{2}$$

with $c_1 = r$ and $c_2 = 2r^2 - s^2$. (This recurrence comes from: let $a_n = \sin nx$, $b_n = \cos nx$, so that $a_{n+1} = a_1 b_n + b_1 a_n$, $b_{n+1} = b_1 b_n - a_1 a_n$, etc.)

For the case that $s$ is not a power of 2, let $s = 2^a b$, with $b$ odd and $>1$. We are interested in $n$ for which

$$\frac{c_n}{2^{a^n} b^n} = \frac{u}{2^{n+1} b_1} ;$$

the following argument shows that $(c_n, b^n) = 1$, so that a necessary condition for a candidate $n$ is that $b_1 = b^n$. If some odd $d$ has $d \mid s$ and also $d \mid c_n$, then, recalling that $(r, s) = 1$, and using, consecutively, (2),

$$d \mid c_{n-1}, d \mid c_{n-2}, \ldots, d \mid c_2,$$

so that $d \mid r^2$, whence $d = 1.$
For the case that \( s \) is a power of 2, say \( s = 2^k \), \( k > 1 \) (recall, we have assumed \( r/s \neq \pm \frac{1}{2} \)) it is convenient to express \( c_n \) as \( c_n = 2^kn_n \), where \( n_n \) is odd. Accordingly, the recurrence (2) becomes:

\[
2^{n_n+1} - 2^{n_k+n_n} = 2^{n_n+2}v_{n+2}.
\]

First, we show that for some \( n \), \( \lambda_{n+1} < 2k + \lambda_{n-1} \); if not, then, always, \( \lambda_{n+1} \geq 2k + \lambda_{n-1} \), so that \( \lambda_{n+1} \geq 2(n-1)k + \lambda_1 \); since \( |\cos n\theta| < 1 \), we have \( kn \geq \lambda_n \), so that \( kn \geq 2(n-1)k + \lambda_1 - 1 \) holds for all \( n \). Clearly this is impossible.

Accordingly, let \( n_0 \) be least with \( \lambda_{n_0+1} < 2k + \lambda_{n_0} \). Then

\[
\lambda_{n_0+2} = \lambda_{n_0+1} + 1, \lambda_{n_0+2} + 1 = \lambda_{n_0+1} + 2 < \lambda_{n_0+1} + 2k.
\]

so that for each integer \( h \geq 0 \), \( \lambda_{n_0+2+h} = \lambda_{n_0+1+h} + 1 \). We have then, for each positive \( h \), \( \lambda_{n_0+h} = \lambda_{n_0} + h \).

Now return to the question of whether for some \( n \), \( \cos n\theta = u/v \). For \( \cos \theta \) having denominator \( 2^k \) then \( v \) must be a power of 2. Suppose \( v = 2^m \). It may happen that there is a solution for \( n \leq n_0 \). For \( n > n_0 \), a solution \( n = n_0 + h \) will have

\[
\cos (n_0 + h)\theta = \frac{v_{n_0+h}2^{n_0+h}}{2^{k(n_0+h)}} = \frac{u}{2^m},
\]

so that

\[
k(n_0 + h) - \lambda_{n_0} - h = m, \quad \text{or} \quad h = \frac{m + \lambda_{n_0} - kn_0}{k - 1}.
\]

That is, the only candidate solution \( n \) exceeding \( n_0 \) is

\[
n_0 + \frac{m + \lambda_{n_0} - kn_0}{k - 1}
\]

provided it is an integer.

5. The case \( b = -1 \) and \( |a| = 1 \).

Recall (from the parenthetical remark of Section 4) that a solution to

\[
A^n(\begin{array}{c}
\alpha \\
\beta
\end{array}) = (\begin{array}{c}
\gamma \\
\delta
\end{array})
\]

requires that \( \delta = ca \), \( \gamma = c\beta \) for \( c = \pm 1 \).

For \( a = 1 \), the Jordan canonical form \( J \) of \( A \) is given by \( J = PAP^{-1} \), with

\[
J = \begin{pmatrix}
1 & 1 \\
0 & 1
\end{pmatrix}, \quad P = \begin{pmatrix}
-2 & 1 \\
1 & -1
\end{pmatrix}.
\]
Using this, the problem is to find \( n \) for which
\[
J^n \begin{pmatrix} \beta - 2\alpha \\ \alpha - \beta \end{pmatrix} = \begin{pmatrix} \alpha - 2\beta \\ \beta - \alpha \end{pmatrix}.
\]

If \( \alpha = \beta \), note that \( \begin{pmatrix} 1 \\ 0 \end{pmatrix} \) is an eigenvector of \( A \). Otherwise, since \( J^n = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \), we are interested only in \( n = (\alpha + \beta)/(\alpha - \beta) \) in case this is integral. Similarly, if \( \alpha = -1 \), use
\[
J = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad P = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.
\]

Note that \( \begin{pmatrix} 1 \\ 1 \end{pmatrix} \) is an eigenvector of \( A^2 \) (for the case \( \alpha = -\beta \)), and that if \( \alpha \neq -\beta \) the only candidate \( n \) is \( \pm (\beta - \alpha)/(\alpha + \beta) \).

**Acknowledgements**

The author wishes to acknowledge stimulating conversations on this subject with M. Harrison, A. Manaster, A. Meyer, and I. Munro.