RATIONAL METHODS IN MATRIX EQUATIONS[1]

MARK H. INGRAHAM

I. **Introduction.**[2] I shall start with what I hope will not prove an overelaborate statement of the limitations of this paper in scope and treatment. I shall assume throughout a knowledge of the definitions of a field, a division algebra, of matrices and rational operations thereon. I shall also need to assume a knowledge of what is meant by the invariant factors and elementary divisors of a matrix. Little essential will be lost if the only field considered by the listeners is the rational number system and the only division algebra that of quaternions over the rational field.

Consider a field $\mathfrak{K}$ and a system of constant matrices $A_1, \cdots, A_l$, unknown matrices $X_1, \cdots, X_n$ and equations

$$\phi_i(A_1, \cdots, A_l, X_1, \cdots, X_n) = 0 \tag{1}$$

where the ϕ_i's are polynomials with coefficients in $\mathfrak{K}$. If the elements of A_i are a_{ijk} and of X_i are x_{ijk}, (1) is equivalent to a system

$$\psi_s(\cdots, x_{ijk}, \cdots) = 0 \tag{2}$$

where the ψ_s are polynomials with coefficients in $\mathfrak{K}$. (If $\mathfrak{K}$ is replaced by a division algebra $\mathfrak{d}$ over $\mathfrak{K}$, the number of equations in (2) is merely enlarged.) We have therefore "reduced" the equations (1) to those of (2). This process we shall technically designate without great exaggeration as the "worst possible algorithm," or, following modern style, W.P.A. This indicates that no "tour de force" which shows that ultimately a matrix problem can be solved in a finite time, but shows little else, is of interest. This is a topic in which the above simple proof of the existence of inelegant methods means that we need only pay attention to results that essentially use the matricial properties of matrices, only to results and methods having at least a minimum degree of elegance.

Partly as a consequence of the above, this lecture, as is often the case, is not so much a description of broad theories of the nature we desire, as a report on what special cases have been found to be seduci-

---

[1] An address delivered before the Chicago meeting of the Society, April 14, 1939, by invitation of the Program Committee; presented in part April 15, 1939, under the title *An algorithm for the solution of the unilateral matrix equation.*

[2] The author wishes to thank H. C. Trimble, C. J. Everett, and J. H. Bell for help in preparing this paper. Their aid was made possible by the Research Committee of the University of Wisconsin.

ble. As a definition of the type of result I shall describe and the literary style in which this description will be given, I will lay down, for this lecture, four canons. The first and last of these I would not defend as completely valid dicta.

1. Irrational methods will be relegated to the background. In particular, we will not assume that we can reduce every polynomial into linear factors.

2. A theorem that is valid for the field of rational numbers is ipso facto of interest. This is particularly true if it extends to the case of all division algebras with finite basis over that field. (If a "field" had been defined to have characteristic zero and others to be "semi-fields," we would, I believe, have had a more wholesome set of values than at present.)

3. Proofs that are essentially algorithmic belong to the aristocracy.

4. The language of matrices, bases, vectors, linear spaces, polynomials, greatest common divisors, and so on, will be used instead of operators, modules, ideals, lattices, and so on. This is in deference to (a) the non-algebraists, (b) the frequency with which generalizations avoided are merely formal, (c) my personal taste.

The paper when presented as a symposium address included the discussion of the equation $TA=BT+C$ and a discussion of the unilateral matrix equation. Only the latter is included here since an extended form of the former is being published elsewhere. (Ingraham [8].)

II. **The unilateral equation.** We will now pass to the consideration of the unilateral (as to position of coefficients) equation

$$\sum A_i X^i = 0. \tag{3}$$

We will endeavor to show that much more can be said of this equation than has heretofore been shown. However, at best the general treatment is not simple so that it is desirable to use when available simpler theories for special types of equations, or for yielding special types of solutions.

What follows will be divided into three parts:

1. The case where all the A_i are polynomials in a single matrix A with scalar coefficients, and solutions X are sought which are of the same type.

2. The case where (3) is of the type

$$\psi(X) = A \tag{4}$$

where the polynomial ψ has scalar coefficients.

3. The general unilateral equation.

The solution of case 1 was first given by Szücs[3] and though his methods are not rational, the rewriting in rational form, as here done, is not difficult. This type of solution had been given, however, for (4) by Roth,[4] and later by a method similar to that of Szücs by Franklin.[5]

Consider

$$\phi(A, X) = 0 \tag{5}$$

and consider only such solutions X as are polynomials in A. We will also assume that the field $\mathfrak{R}$ has characteristic zero. Let $X(\lambda)$ be a polynomial such that $X(A)$ is a solution of (5). Hence $\phi(A, X(A)) = 0$. A necessary and sufficient condition that this be true is that $\phi(\lambda, X(\lambda))$ be divisible by the first invariant factor of A, that is, the minimal polynomial h such that $h(A) = 0$. Let g^k be the highest power of an irreducible polynomial g contained in h as a factor. Hence if $\phi(A, X(A)) = 0$, g^k must divide $\phi(\lambda, X(\lambda))$. Since $\mathfrak{R}$ has characteristic zero this is equivalent to g dividing $\phi, \phi', \phi'', \cdots, \phi^{(k-1)}$. (In case the characteristic is not zero the condition of divisibility is still workable but not as neat.)

Let $X(\lambda) = X_0(\lambda) + X_1(\lambda)g + X_2(\lambda)g^2 + \cdots$ where the X_i are reduced mod g.

Hence

$$\phi(\lambda, X_0) \equiv 0 \bmod g,$$

or in other words, $\phi(\lambda, X)$ has a zero in the field $\mathfrak{R}[\lambda]/\{g(\lambda)\}$ for every irreducible factor g of h.

Consider

$$\begin{aligned}\phi'(\lambda, X) &= \phi_\lambda(\lambda, X) + \phi_X(\lambda, X)X' \\ &\equiv \phi_\lambda(\lambda, X_0) + \phi_X(\lambda, X_0)(X_0' + X_1 g') \\ &\equiv (X_1 g')\phi_X(\lambda, X_0) + \psi_1 \bmod g\end{aligned}$$

where ψ_1 is fixed by the determination of X_0 and, in general,

$$\phi^{(s)}(\lambda, X) \equiv s! X_s (g')^s \phi_X(\lambda, X_0) + \psi_s \bmod g$$

where ψ_s is determined in terms of $X_0, \cdots, X_{s-1}$.

Note that since g is irreducible, g' is prime to g.

It is therefore necessary if $k > 1$ that either

$$\phi_X(\lambda, X_0) \not\equiv 0 \bmod g \tag{6}$$

[3] Szücs [7].

[4] Roth [6].

[5] Franklin [1].

or that

$$\psi_i \equiv 0 \bmod g, \qquad i = 1, \cdots, k-1. \tag{7}$$

If for every irreducible factor g these conditions are satisfied, then we have for each g_i an X_{g_i} such that X is a solution of $\phi(A, X) = 0$ if and only if

$$X \equiv X_{g_i} \bmod g_i^{k_i}.$$

That such an X exists follows from the Chinese Remainder Theorem for polynomials. Hence

THEOREM 1. *If $\mathfrak{R}$ has characteristic* 0, *the equation $\phi(A, X) = 0$ has a solution which is a polynomial in A if and only if for every irreducible factor g of the minimal polynomial of A there exist in $\mathfrak{R}[\lambda]$ solutions of $\phi(\lambda, X) \equiv 0 \bmod g$ which, in case g is a multiple factor of the minimal polynomial of A, satisfy* (6), *or* (7).

If the equation considered is of the form $\theta(X) = A$ where θ has scalar coefficients, then $\phi'(\lambda, X_0) = -1$ and (6) above becomes necessary so that we can state

THEOREM 2. *If $\mathfrak{R}$ has characteristic* 0, *the equation $\theta(X) = A$ has a solution which is a polynomial in A if and only if $\theta(X) \equiv \lambda \bmod g_i$ has a solution in $\mathfrak{R}[\lambda]$, for every irreducible factor g_i of the minimum function of A which, in case g_i is a multiple factor of the minimal function of A, does not satisfy $\theta'(X) \equiv 0 \bmod g_i$.*

As a corollary of this,

THEOREM 3. *If $\mathfrak{R}$ is algebraically closed and has characteristic* 0, *the equation $X^n = A$ has a solution $X(A)$, a polynomial in A, if and only if* 0 *is not a multiple root of the minimum function of A.*

It is not difficult to compute the number of such functions.

For certain cases the existence of solutions not polynomials in A is easily established by example.

For instance

$$X^2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

has the solution

$$X = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

It is interesting, therefore, to study the general solutions of equations of the type discussed above. This is readily done for the equations $\theta(X)=A$, if A is nonderogatory, that is, its minimum equation is its characteristic equation. Since A is nonderogatory and every solution X is commutative with A, X is a polynomial in A. In this case our problem is completely solved. In case ϕ has scalar coefficients, the general solution of

$$\phi(X) = A$$

is determined as follows.[6]

If we find a matrix Y such that $\phi(Y)$ is similar to A, then a nonsingular matrix S may be found such that $A=S\phi(Y)S^{-1}=\phi(SYS^{-1})$ and hence SYS^{-1} is effective as X. Consider the invariant factors of $A-\lambda I$, $h_1, h_2, \cdots, h_k$. Then $\phi(Y)$ is similar to A if and only if the nullity of $h_i(\phi(Y))$ equals the nullity of $h_i(A)$. Hence the invariant factors of Y must be divisors of $h_1(\phi(\lambda))$. Under this restriction and the fact that the nullity of any polynomial ϕ in Y is determined as the sum of the degrees of the greatest common divisors of the invariant factors of Y, with the polynomial ϕ, diophantine equations may be written, any solution of which determines the invariant factors of a solution X, and hence determines X to within a transformation by a matrix commutative with A. All solutions are the transforms by matrices commutative with A of a certain finite dissimilar system of solutions $X_1, X_2, \cdots, X_k$. Those X_i which are polynomials in A are those solutions which are dissimilar to all other solutions. For example if

$$X^2 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

then

$$X = \begin{pmatrix} 0 & 0 & 0 \\ m & 0 & k \\ 1/k & 0 & 0 \end{pmatrix}$$

with $k \neq 0$.

This work generalizes with only moderate difficulty to the case where the scalars involved belong to a division algebra provided we ask the question correctly.[7] In the case where the scalars are in a field and $\phi=\sum\lambda^i a_i$ then $\phi(X)=A$ is equivalent to $\phi(X)\xi=\sum X^i\xi a_i$

[6] Ingraham [2].
[7] Ingraham [3].

$=A\xi$ for every vector ξ. This is not the case if the a_i belong to a noncommutative division algebra $\mathfrak{D}$. The correct question which can be answered is not to find a solution of $\phi(X)=A$, but given a set $[a_i]$ in $\mathfrak{D}$ to find a matrix X such that $\sum X^i\xi a_i=A\xi$ for every ξ. This problem turns out to be equivalent to a system of equations

$$\phi_i(X) = A_i$$

where the coefficients of ϕ_i are in the centrum of the division algebra $\mathfrak{D}$.

Let us now consider the general unilateral matrix equation

$$\sum A_iX^i = 0, \tag{8}$$

where the A_i are $n\times n$ matrices of constants.

Fundamental to the consideration of (8) is the fact that if X is any constant matrix then $A(\lambda)=\sum A_i\lambda^i$ can be expressed in one and only one way as

$$(\sum B_i\lambda^{i-1})(\lambda I - X) + B_0$$

and in fact

$$B_0 = \sum A_iX^i.$$

Hence

THEOREM 4. *X is a solution of $\sum A_iX^i=0$ if and only if $\lambda I-X$ is a right factor of the matrix $A(\lambda)=\sum A_i\lambda^i$.*

Theorem 5, which is a corollary of a theorem due to Phillips,[8] yields us an algorithm better than the W.P.A. This theorem is as follows:

THEOREM 5. *If X is a solution of $\sum A_iX^i=0$, then the determinant of the matrix $\lambda I-X$ divides the determinant of the matrix $\sum A_i\lambda^i$.*

This is, of course, a corollary of Theorem 4. The proof originally given was far more complicated than this proof which is due to C. C. MacDuffee. Phillips' theorem yields a necessary condition on the invariant factors of any solution. If Y has such invariant factors and $X=PYP^{-1}$ is a solution, then $\sum A_iPY^i=0$. The problem is then reduced to finding all P's satisfying this equation for canonical Y's with possible invariant factors.

Far stronger conditions can be secured from Theorem 6, which is a consequence of the following lemma.

[8] Phillips [5].

LEMMA. *If A, B, C, are λ-matrices such that $A=BC$, then the invariant factors of B (or C) divide the corresponding invariant factors of A.*

Thus

THEOREM 6. *If X is a solution of $\sum A_i X^i=0$, then the invariant factors of the matrix $\lambda I-X$ are divisors of the corresponding invariant factors of the matrix $\sum A_i\lambda^i$.*

This eliminates many cases not strained out by the sieve of Phillips' theorem.

That these conditions or any conditions in terms of the invariant factors of $A(\lambda)$ are insufficient to guarantee the existence of solutions with a given set of invariant factors for $\lambda I-X$ is shown by the two equations

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}X^2+\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}=0$$

and

$$X+\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}=0.$$

The λ-matrices for these are respectively

$$\begin{pmatrix}\lambda^2 & 0\\ 0 & 1\end{pmatrix},\qquad \begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix},$$

each of which has invariant factors λ^2, 1; but the first equation has no solution and the second has the solution

$$\begin{pmatrix}0 & -1\\ 0 & 0\end{pmatrix}.$$

We now pass to the description of an algorithm believed to be new for the solution of (8).

We shall call a matrix with elements polynomials in λ unimodular if its determinant is a scalar not zero, or what is equivalent, if it is nonsingular in the field of rational functions of λ, and if its reciprocal has elements polynomials in λ.

We say that A is in triangular form if all the elements below the main diagonal are zero. We say it is in canonical triangular form if it is in triangular form and all the elements above the main diagonal are of lower degree than the elements in the same column on the main diagonal and if when a zero occurs on the main diagonal the whole row in which it occurs is zero. We also specify that the leading coefficients of the polynomials along the main diagonal be 1.

If U is unimodular, then $\lambda I - X$ is a right factor of A if and only if it is a right factor of UA. Moreover, a unimodular matrix U may be found such that UA is in canonical triangular form, this form being completely determined by[9] A. From now on we will assume that A is in such form.

Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \cdots & a_{1n} \\ 0 & a_{22} & a_{23} \cdots & a_{2n} \\ 0 & 0 & a_{33} \cdots & a_{3n} \\ \cdot & \cdot & \cdot \cdots & \cdot \\ \cdot & \cdot & \cdot \cdots & \cdot \\ 0 & 0 & 0 \cdots & a_{nn} \end{pmatrix}$$

where the a_{ij}'s are polynomials in λ.

If $A = H(\lambda I - X)$ and if U is the unimodular matrix such that $U(\lambda I - X)$ is in canonical triangular form, then

$$A = HU^{-1}U(\lambda I - X)$$

and $T = U(\lambda I - X)$ is a right factor of A.

Our problem is therefore reduced to finding the triangular factors of A which are the canonical triangular forms of matrices of type $\lambda I - X$ where X is independent of λ.

We study then the problem of finding canonical triangular factors T of the matrix A and then of selecting those which are the canonical triangular forms of matrices of type $\lambda I - X$ for some X.

If $A = ST$ where the matrices A and T are in triangular form, S is in triangular form, and

$$(9) \qquad a_{i,i+j} = \sum_{k=0}^{j} s_{i,i+k} t_{i+k,i+j}, \qquad i = 1, \cdots, n; j = 0, \cdots, n - i.$$

For the case $j = 0$ these relations reduce to

$$a_{ii} = s_{ii} t_{ii}$$

and hence to the fact that the diagonal elements of T are factors of the corresponding diagonal elements of A.

Equations (9) give linear congruences each conditioning (not necessarily uniquely) the possible t_{ij} in terms of previously determined elements of T below t_{ij} occurring in the jth column and elements of s to the left of s_{ij} in the ith row—these may be considered therefore

[9] MacDuffee [4].

as recursive formulae for the t_{ij}. In these congruences the coefficient of t_{ij} is s_{ii} and the modulus is t_{jj}, so that, in case $\mathfrak{R}$ has infinitely many elements, an infinitude of solutions exists if and only if s_{ii} and t_{jj} are not relatively prime and at least one solution exists.

It should be noted that if T is the triangular form of M, the product of the first i diagonal terms is the greatest common divisor of the determinants of the ith order minors of the first i columns of M. Hence if T is of the form $U(\lambda I - X)$ where U is unimodular, the sum of the degrees of the first i terms of the principal diagonal of T must be less than or equal to i and the sum of the degrees of all the diagonal terms is n, the order of T. I believe in most equations written at random these last conditions would preclude a solution.

We turn now to determining X such that a T satisfying the above conditions is the triangular canonical form for some $(\lambda I - X)$. It can be shown (but the proof is omitted) that X is unique if it exists.

If $T = U^{-1}(\lambda I - X)$ where U is unimodular, then

$$U = (\lambda I - X)T^{-1}. \tag{10}$$

If we choose a matrix X, $(\lambda I - X)T^{-1}$ will have elements rational functions of λ but not, in general, polynomials.

The problem therefore reduces to seeking X such that $(\lambda I - X)T^{-1}$ is a matrix with elements polynomials in λ.

Let $T^{-1} = F/d$ where F is in triangular form and d is the determinant of T. The f_{ij} will be polynomials.

If (10) is fulfilled

$$u_{ij} = (\lambda f_{ij} - \sum x_{ik} f_{kj})/d;$$

hence u_{ij} is a polynomial if and only if

$$\sum x_{ik} f_{kj} \equiv \lambda f_{ij} \bmod d.$$

Since the f_{ij} are of degree less than d, these linear congruences are easily reduced, by equating coefficients, to n systems of linear equations for the x_{ik} (i fixed) all of the systems having the same matrix of coefficients, the rank of which must (in light of the uniqueness theorem) be n if a solution of all the systems exists.

Since this paper was delivered at Chicago Mr. J. H. Bell has furnished me with the following note on the conditions upon T for a matrix X to exist such that T is a triangular form of $\lambda I - X$.

The existence of X depends directly upon the coefficients of the elements of T.

We may obtain an $n \times n$ matrix D whose elements are scalars by the following steps.

1. Augment each element of T by the proper powers of λ with zero coefficients so that terms of the same degree as in the corresponding diagonal element appear.

2. Break up each column into separate columns, each one of which involves only monomials of the same degree in λ, for example,

$$\begin{pmatrix} a\lambda + b \\ c\lambda + d \end{pmatrix} \rightarrow \begin{pmatrix} a\lambda, & b \\ c\lambda, & d \end{pmatrix}.$$

3. Delete the columns which do not involve λ.

4. Set $\lambda = 1$ obtaining D.

A necessary and sufficient condition that there exist a matrix X such that $T = U^{-1}(\lambda I - X)$ is that $|D| \neq 0$.

If $T = \sum_r^0 T_i \lambda^i$ ($T_i^{n \times n}$ involving scalars only), then the above condition is equivalent to saying that n is the rank of

$$M = (T_r, T_{r-1}, \cdots, T_2, T_1).$$

X may be obtained quite readily from D. We first find $B = (b_{ik})$ as follows. If $t_{jj} \neq 1$, $(b_{j1} \cdots b_{jn}) = (0 \cdots 0, -1, 0 \cdots 0)D^{-1}$ where the -1 occurs in the position corresponding to the column of D containing $t_{1,jj}$ (where $t_{kj} = \sum_s^0 t_{i,kj}\lambda^i$). If $t_{ll} = 1$, $(b_{l1} \cdots b_{ln}) = \eta_l D^{-1}$ where η_l is a $1 \times n$ vector obtained by taking the lth row of the matrix obtained from the matrix in step 2 by deleting the columns involving the leading term of t_{kk}, for every k, and setting $\lambda = 1$.

Then

$$X = BT_0.$$

BIBLIOGRAPHY

1. P. Franklin, *Algebraic matric equations*, Journal of Mathematics and Physics, Massachusetts Institute of Technology, vol. 10 (1932), pp. 289–314.

2. M. H. Ingraham, *On the rational solution of the matrix equation* $P(X) = A$, Journal of Mathematics and Physics, vol. 13 (1934), pp. 46–50.

3. M. H. Ingraham, *On certain equations in matrices whose elements belong to a division algebra*, this Bulletin, vol. 44 (1938), pp. 117–124.

4. C. C. MacDuffee, *Matrices with elements in a principal ideal ring*, this Bulletin, vol. 39 (1933), pp. 564–584.

5. H. B. Phillips, *Functions of matrices*, American Journal of Mathematics, vol. 41 (1919), pp. 266–278.

6. W. E. Roth, *A solution of the matric equation* $P(X) = A$, Transactions of this Society, vol. 30 (1928), pp. 579–596.

7. A. Szücs, *Sur les équations définissant une matrice en fonction algébrique d'une autre*, Acta Litterarum ac Scientiarum, Szeged, vol. 7 (1934–1935), pp. 48–50.

8. M. H. Ingraham and H. C. Trimble, *On the matric equation* $TA = BT + C$, American Journal of Mathematics, vol. 63, pp. 9–27.

UNIVERSITY OF WISCONSIN