Internat. J. Math. & Math. Sci.
Vol 9 No. 2 (1986) 253-260

THE RATIONAL CANONICAL FORM OF A MATRIX

J.S. DEVITT

Department of Mathematics
The University of Saskatchewan
Saskatoon, Saskatchewan
Canada S7N 2R5

R.A. MOLLIN

Department of Mathematics
The University of Calgary
Calgary, Alberta
Canada T2N 1N4

(Received July 24, 1985 and in revised form September 19, 1985)

ABSTRACT. The purpose of this paper is to provide an efficient algorithmic means of determining the rational canonical form of a matrix using computational symbolic algebraic manipulation packages, and is in fact the practical implementation of a classical mathematical method.

KEY WORDS AND PHARASES. Matrix, Rational Canonical Form, Algorithm
1980 MATHEMATICS SUBJECT CLASSIFICATION CODE. PRIMARY 15A21, SECONDARY 15-04.

1. INTRODUCTION.

One of the most useful and beautiful canonical forms of an n by n matrix over a field F is the rational canonical form which is sometimes called the Frobenius - Perron normal form (see §3). In the literature there are several articles which provide algorithms for reducing a matrix to rational canonical form. Generally ignored is an algorithm which is classical in nature in that it calculates the invariant factors of a matrix (with polynomial entries) among which is the minimal polynomial. Professor J. Rotman has highlighted this fact in [1 , p. 653] where he says:

> "- current proofs have a defect; given a matrix A, they do not indicate how to compute the invariant factors -. Thus there are two articles in the January 1983 issue of the monthly that seem to overlook an old theorem. (*An algorithmic derivation of the Jordan canonical form,* by Fletcher and Sorenson, and *An algorithm for the minimal polynomial of a matrix,* by Gelbaum.) The theorem says that if B is a matrix with (polynomial) entries in F[x], then one can put B in

diagonal form diag($g_1(x)$, $g_2(x)$, - , $g_n(x)$) where $g_i(x) \mid g_{i+1}(x)$, using elementary row and column operations. (In so doing, one needs the Euclidean algorithm for the g.c.d. of two polynomials.) In particular, this can be done for $B = xI - A$. The nonconstant $g_i(x)$ are the invariant factors of A, and $g_n(x)$ is the minimal polymomial of of A."

As Professor Rotman indicates, there is a simple, beautiful, classical method which exists for deriving canonical forms. While this method has a number of advantages, at least some of which will become apparent as we proceed, the method has generally been overlooked for reasons pertaining to the difficulty of it's practical implementation. In this paper, we discuss in detail the practical implementation of this algorithm. Our implementation relies heavily on the advances which have taken place in symbolic algebra packages over the last decade. One of the main goals of this paper is to focus attention on these advances and the ease with which these packages may be used.

2. DESIGN CONSIDERATIONS.

A well known algorithm for computing the characteristic polynomial of a given matrix is the Danilewsky method (see [2]). This algorithm has been used in a variety of settings, and has been incorporated successfully into at least one graph theory package for computing chromatic polynomials [3].

For more general applications, the numerical stability of the Danilewsky method has raised some concern. Chartras [4] and Hansen [5] introduce extended precision arithmetic to combat this problem. Other approaches (see [6]) introduce an elaborate procedure based on modular arithmetic to achieve stability. It is interesting to note that these modular methods are very similar to the techniques used in the symbolic packages for precisely the same reasons. It is a characteristic of symbolic computation that while initial and final results may appear quite innocent (eg. $(x-1)^{100}/(x-1)$ and $x^{99} + x^{98} +\ldots+ 1$ have small coefficients) while expanded intermediate results have large coefficients such as $100!/(50!)^2$.

In addition, one may encounter mathematically valid examples which require arbitrarily high precision. For example, the matrices

$$A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.1}$$

have minimal polynomials $(x-1)^2$ and $(x-1)$ respectively, if $a \neq 0$. If a of (2.1) is sufficiently small that the floating point representation of $1 - a$ is 1, then the computation of the minimal polynomial fails. Similarly, with the modular method, computed lower bounds on the product of the modulii (see [7, pp. 918-919]) can be forced to exceed any fixed limit.

It is precisely these extreme cases that we wish to address. One strategy that is available is to anticipate the degree of precision required for any given problem. Alternatively one can work with exact arithmetic and unbounded precision. This approach still does not deal with the above example if we insist that a be indeterminant. As well, estimating the degree of precision required may be difficult in general. (The modular algorithm addresses this problem to some extent). The unbounded precision approach has traditionally been avoided because of the difficulty of implementation. For example, because no upper bound exists on the size of an integer, the issue of dynamic memory allocation must be confronted, and the exclusive use of rational or integer arithmetic must be considered. These design issues are identical to those which must be addressed by symbolic algebra systems. Thus the proposed algorithm might be regarded as a natural consequence of the decision to go with unbounded precision.

In the proposed algorithm, we work directly with the symbolic representation of the matrices with entries which are polynomials over the rational number field. Most operations performed (beginning with the characteristic matrix) are integer operations though rational coefficients do occur as intermediate results. All calculations are exact.

3. THE RATIONAL CANONICAL FORM. (See [8])

First we introduce some required concepts. If F is a field and $p(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$ with ai, i = 0,...,n, all elements of F; i.e. $p(x)$ is in $F[x]$; then the <u>companion matrix</u> of $p(x)$ is:

$$C_p = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ 0 & 0 & 1 & \ldots & 0 & -a_3 \\ \ldots & & & & & \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix} \tag{3.1}$$

It turns out that for any $n \times n$ matrix A over F, there are uniquely determined monic polynomials $q_i(x)$, $i = 1\ldots r$, such that $q_{i-1}(x)$ divides $q_i(x)$, $i = 2\ldots r$, and $q_r(x)$ is the minimal polynomial of the matrix A. If C_i is the companion matrix of $q_i(x)$, then the <u>rational canonical form</u> of A is the matrix with the block diagonal form

$$\begin{bmatrix} C_1 & 0 & 0 & \ldots & 0 \\ 0 & C_2 & 0 & \ldots & 0 \\ 0 & 0 & C_3 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \ldots & & & & \\ 0 & 0 & 0 & \ldots & C_r \end{bmatrix} . \tag{3.2}$$

We have deliberately avoided any reference to the underlying vector space and the attendant relationship to the C_i's and invariant subspaces so as to achieve a simple description of the rational canonical form at least at the outset.

As noted by Professor Rotman [1], the usual derivation of canonical forms for $n \times n$ matrices over a field F involves such matters as invariant subspaces and cyclic vectors. They key to the proposed algorithm lies in a more detailed explanation of this proof.

First we require some definitions. Let B be a matrix with coefficients in the polynomial ring $F[x]$, and let d_k be the monic g.c.d. of all non-zero $k \times k$ minors of B. (set $d_0 = 1$.) It is easy to check that d_{k-1} divides d_k for $k = 1\ldots r$, where r is the largest integer for which the $r \times r$ minors are not all zero; i.e. r is the rank of B. The polynomial $a_k\, d_k/d_{k-1}$ is the k^{th} torsion order of B and is set to 0 if $k > r$. In the special case where A is an $n \times n$ matrix over F, $B = xI_n - A$, and the k^{th} torsion orders are called the elementary divisors of A.

In what follows V is an n dimensional vector space over the field F, and $Hom_F(V,V)$ is the ring of F-endomorphisms of V. Thus A is an element of $Hom_F(V,V)$. For any polynomial p(x) in F[x], the mapping $p(x) \to p(A)$ is a ring homomorphism of F[x] into $Hom_F(V,V)$, and so the scalar multiplication given by $p(x)v = p(A)v$ for any v in V, defines an F[x] module structure on V which we denote by V^A. It can be shown that V^A is isomorphic as an F[x]-module to the direct sum $F[x]/(q_1) \oplus \ldots \oplus F[x]/(q_n)$, where $(q_i) = (q_i(x))$ denotes the principal ideal of F[x] generated by the i^{th} elementary divisor of A. Conversely, each F[x]-module $F[x]/(q_i)$ corresponds to an F-vector space V_i and associated endomorphism A_i defined by $A_i v = xv$ for all v in V_i; i.e. the restriction of A to V_i.

If $q_i(x) = a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} + x^m$ then as an F-vector space, V_i has $\{\pi_i(1), \pi_i(x), \ldots, \pi_i(x^{m-1})\}$ as a basis where $\pi_i: F[x] \to F[x]/(q_i(x))$ is the i^{th} projection map. Since $T_i\pi_i(x^k) = \pi_i(x^{k+1})$, for $k = 0,1,\ldots,m-1$, and $T_i\pi_i(x^m) = -(a_0\pi_i(1) + a_1\pi_i(x) + \ldots + a_{m-1}\pi_i(x^{m-1}))$ then the matrix of T_i relative to the given basis of V_i is just the companion matrix of $q_i(x)$. Now, $q_i(T_i)(V_i) = q_i(x)\pi_i(F[x]) = \pi_i(q_i(x)F[x]) = 0$. Moreover, for any p(x) in F[x] with degree less than m, we have $p(T_i) \neq 0$ since $p(T_i)\pi_i(1) = p(x)\pi_i(1) = \pi_i(p(x)) \neq 0$. Consequently $q_i(x)$ is the minimal polynomial of T_i.

In summary, for any endomorphism A, of an n-dimensional F-vector space, there is a basis for V with respect to which the matrix of A has the block diagonal form

$$\begin{bmatrix} C_1 & 0 & 0 & \ldots & 0 \\ 0 & C_2 & 0 & \ldots & 0 \\ 0 & 0 & C_3 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & C_r \end{bmatrix} \qquad (3.3)$$

where the i^{th} block is the companion matrix of the i^{th} elementary divisor of A (distinct from 1). This form is known as the rational canonical form.

Since F[x]/(1) yields the zero subspace we need only consider the non-trivial elementary divisors. The following observations should also be made.

1. The elementary divisor corresponding to C_r is the minimal polynomial of A.

2. The product of the elementary divisors $q_i(x)$, $i = 1,\ldots,r$, is the characteristic polynomial $\beta(x) = \det(xI_n - A)$.

3. $\beta(x) \mid q_r(x)^r$ so the minimal polynomial is the characteristic polynomial if and only if $r = 1$.

From the proof outlined above it is clear that one approach to obtaining the rational canonical form is to obtain the elementary divisors directly. Apart from the points mentioned earlier, this approach has the advantage that it can also be used to find the torsion orders of an arbitrary $n \times n$ matrix over $F[x]$.

4. THE ALGORITHM.

Throughout, we work with matrices whose entries are in $F[x]$ and calculate the k^{th} torsion orders directly. Given a matrix **A** over **F**, we work with the characteristic matrix $B = I - xA$ to obtain the rational canonical form.

The basic procedure for finding the invariant factors is essentially to reduce the matrix **B** to a diagonal of the form $diag(b_1,\dots,b_n)$ with $b_1|b_2,\dots,b_{n-1}|b_n$, by elementary row and column operations in such a way that:

1. No elements of the quotient field $F(x)$ which are not in $F[x]$ are introduced.
2. No row or column of B is ever multiplied by a non-trivial polynomial.

We proceed along the main diagonal, at each stage moving a polynomial of minimum degree into the next diagonal position. The bulk of the work involves ensuring that this polynomial divides all the elements in the remaining submatrix. When it does, we can force the off-diagonal entries corresponding to the row and column of the current diagonal position to zero by means of standard row and column pivots.

First a polynomial of minimal degree is selected and moved to position [1,1] by elementary row and column operations. If row and column pivots can now be carried out on the entry $p(x)$ in position [1,1] without introducing into the matrix elements of the quotient field $F[x]$, this is done. If not, there must be some polynomial $t(x)$ in say position [1,k], which is not divisible exactly by $p(x)$. An appropriate multiple of row 1 is subtracted from row k to leave in position [1,k] the remainder of $t(x)$ divided by $p(x)$. This entry is now of smallest degree and is moved to row 1 by swapping rows. This is essentially the Euclidean algorithm for computing g.c.d.'s of polynomials by using elementary operations on matrices.

This reduction process is repeated until the row and column pivots can be carried out. After these pivots we must still establish that $p(x)$ divides every element of the remaining submatrix. If this is not the case, we add the row (column) containing the offending entry to row (column) 1. This does not change the pivot element because of the earlier pivots, but allows us to reduce the degree of the pivot element by the reduction described above, and then try again.

This whole reduction process continues until the pivot element is the g.c.d. of the entire matrix. The algorithm continues by applying the above procedure recursively to the $(n - 1) \times (n - 1)$ submatrix occupying rows and columns 2 through n. A detailed description of the algorithm is listed in Figure 1.

As already indicated, the rational canonical form can be obtained directly from the result of applying the above algorithm to the characteristic matrix I - xA. One just uses the companion matrices of the resulting polynomials.

During the past two decades considerable effort has gone into the development of computer software for symbolic algebra. Many of the features and techniques that have been considered for the efficient implementation of an algorithm for computing the rational canonical form are common to the general questions of efficiency of many algebraic operations and, in fact, have been explored at great length in this context. (For example, see [9].)

The algorithm outlined above for computing the rational canonical form has been implemented by the authors in the symbolic language Maple [10] for matrices of polynomials over the rational number field. The implementation allows for the representation of field elements by unknowns. The richness of the built in functions and abstract data structures of Maple, and the user extendability of these features were of significant help in reducing the programming effort required. The program has been used on up to 20 × 20 examples. Copies of the source code are available from the authors.

Figure 1. Torsion orders of a matrix over F[x]

```
FUNCTION CANONICAL (M: matrix over F[x], index, size: integer) if index < size then
     1.  move a smallest degree non-zero polynomial to position
         M[index, index] by row and column interchanges.

     2.  if M[index, index] divides every element of column index
         then zero the non-diagonal elements of column index by
              adding multiples of row index.
         else reduce a non divisible element to its remainder on
              dividing by M[index, index], by row operations and
              then swap rows.
              RETURN (CANONICAL (M, index, size))
         endif

     3.  if M[index, index] divides every element of row index
         then zero the non diagoanl elements of row index by
              adding multiples of column index.
         else reduce a non-divisible element to its remainder on
              division by M[index, index], by column operations
              and then swap rows.
              RETURN (CANONICAL (M, index, size))
         endif

     4.  if M[index, index] divides every element in
              M[index+1...size, index+1...size]
         then make M[index, index] monic by a row operation.
              RETURN (CANONICAL (M, index+1, size))
         else add a row (in the range index+1...size) containing an
              element of M which is not divisible to row index.
              RETURN (CANONICAL (M, index, size))
         endif
     else make M[index, index] monic by a suitable row operation.
         RETURN(M)
     endif
end;
```

5. PERFORMANCE OF THE ALGORITH.

As the derivation of the rational canonical form from the diagonal matrix of torsion orders of the polynomial matrix is straightforward, we discuss only the performance of the algorithm for obtaining the torsion orders. It should also be observed that by working with the factorizations of torsion orders, the Jordan canonical form can also be reconstructed.

For matrices with small integer entries, the following table gives some indication of performance.

Figure 2. Some timing results

size of matrix	Time in seconds
4 × 4	15
6 × 6	28 - 35
10 × 10	95 - 100
20 × 20	900

(5.1)

All timing is on a DECSYSTEM-20 with 1.25 megawords of main memory running Version 3.2a of Maple. In the worst case, about 350K words of memory were actually used, though automatic garbage collection was invoked. (The automatic garbage collection was done at the programming level. Version 3.3 of Maple has garbage collection fully implemented at the system level.)

These times are unacceptable for many purposes, and clearly reflect the overhead cost of algebraic computing. However, it does provide the user with a truly flexible tool which becomes part of, and is augmented by the increasingly sophisticated work environment of algebraic computation. For example, working in such an environment, algebraic factoring is already provided and can be invoked directly on the resulting elementary divisors.

In addition, the following example gives some indication of the generality of this approach. The characteristic matrix

$$\begin{bmatrix} x-a & -b & -c \\ -d & x-e & x-f \\ -g & -h & -i \end{bmatrix} \qquad (5.2)$$

where a,b,c,d,e,f,g,h,i are all unknowns in the rational field is transformed by the algorithm to the diagonal matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & r(x) \end{bmatrix} \qquad (5.3)$$

where

$$r(x) = x^3 - (a+e+i)x^2 + (ei + ea + ai - fh - db - cg)x + (dbi - dhc + fha - eai - fbg + ecg).$$

Various assumptions about non-zero divisors must of course be made. It is easily verified that, in this case, the minimal polynomial r(x) is the characteristic polynomial.

REFERENCES

1. ROTMAN, J. letter which appeared in the American Math. Monthly, 90(1983), p. 653.

2. DANILEWSKI, A. On a numerical solution of Vekua's equation, Mat. Sb. 2 (1937), pp. 169-171.

3. GODS, C. Private communication.

4. CHARTRES, B.A. Controlled Precision Calculations and the Danilewski Method, Brown University, Preprint (1964).

5. HANSEN, E.R. On the Danilewski method, J.A.C.M. 10 (1963, pp. 102-109.

6. HOWELL, JO ANN. An algorithm for the Exact Reduction of a Matrix to Frobenius Form Using Modular Arithmetic I, Math. Comp. 27 (1973), pp. 887-904.

7. HOWELL, JO ANN. An algorithm for the Exact Reduction of a Matrix to Frobenius Form Using Modular Arithmetic II, Math. Comp. 27 (1973), pp. 905-920.

8. HARTLEY, B.H. and HAWKES, T. Rings, Modules and Linear Algebra, Chapman and Hall, London, 1970.

9. BROWN, W.S. On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisions, Journal of the ACM 18 (1971), pp. 478-504.

10. GEDDES, K.O., GONNET, G.H. and CHAR, B.W. Maple User's Manual, 3rd Edition Department of Computer Science Research Report CS-83-41, December 1983.