EXTRACTA MATHEMATICAE Vol. 6, Núms. 2 y 3, 142 – 144 (1991)

An Algorithm to Compute the Change Basis for the Rational Form of K–Endomorphisms

K. MARTÍN AND J.M. OLAZÁBAL [1]

Department of Mathematics, Univ. of Cantabria, 39071 *Santander, Spain*

AMS *Subject Class.* (1980): 15A21, 15–04, 15A04 *Received October* 10, 1991

1. INTRODUCTION

There are in the literature many algorithms, the most of them based in the Danilevski's algorithm [1], [2], [5], performing similarity transformations in a matrix A over any field K, and therefore computing a regular matrix P so that $P^{-1}AP=B$ where B is a block–diagonal matrix of companion matrices.

However, such algorithms do not give the rational canonical form F of A in general, except the one by Ozello[2] [5, p. 89], because the characteristic polynomials of the companion matrices do not satisfy, in general, the divisibility condition. The obtained matrix B is called a cyclic form of A [2].

For such a cyclic form B of A let h denote the endomorphism of K^n given by $Y=BX$; we try to find a basis (v_i) of K^n so that the new equation of h is $Y=FX$ [3, Ch. VII, §5, p. 190].

It is well known that the minimum polynomial of K^n is both the minimum polynomial of v_1 and the $\operatorname{lcm}(f_1,\ldots,f_n)$, where $f_1,\ldots,f_n$ are the characteristic polynomials of the companion matrices in B [3, Ch. VII, §2, th. 2, p. 180]. Let m be the degree of the minimum polynomial of v_1; then the family $(v_1,\ldots,h^{m-1}v_1)$ is free. Ozello's procedures [5, Ch. II, §5, pp. 36, 37, 41] yields a basis of K^n such that the equation of h in this basis is $Y=B^*X$, with B^* a block–diagonal matrix $B^*=[C,D]$ where C is the companion matrix of the minimum polynomial of K^n. An iteration of this method over any cyclic form of D will give the wanted both rational form of h and basis (v_i) of K^n.

---

[1] Partially supported by CICyT PB 89/0379/C02/01

[2] Only valid if the characteristic of K is large.

2. COMPUTING THE VECTOR v_1

The well known methods, in the classical literature, for computing v_1 are not polynomial–time. Ozello [5, Ch. III, §4, corollary, pp. 73] shows that, if $\mathrm{char}(K)$ is large enough, there are positive integers $k_2,\ldots,k_r$ so that the minimum polynomial of $u_1+k_2u_2+\ldots+k_ru_r$ equals the $\mathrm{lcm}(\mathrm{min.pol}\,u_i)=\mathrm{min.pol}\,K[x]<u_1,\ldots,u_r>$. The next example shows that the hypothesis over $\mathrm{char}(K)$ cannot be avoided:

Let $h:K^4\longrightarrow K^4$, $\mathrm{char}(K)=2$, given by means of $h(e_1)=0$, $h(e_2)=e_2$, $h(e_3)=e_4$, $h(e_4)=e_3+e_4$; then, h restricts to the submodule $V=K[x]<e_1+e_2,e_1+e_3>$; it is easy to see that $\mathrm{min.pol}(V)=x(x+1)(x^2+x+1)$, but $\mathrm{min.pol}(e_1+e_2+(e_1+e_3))=(x+1)(x^2+x+1)$.

The problem may be solved by means of the following:

PROPOSITION. *Let M be an R–module and $m_1,\ldots,m_r$ torsion elements of M such that $N=R<m_1>+\cdots+<m_r>$ is a direct sum. Then* $\mathrm{Ann}(N)=\mathrm{Ann}(m_1+\cdots+m_r)$.

The interest of this proposition lies in the next situation: assume the equation of the K–endomorphism h with respect to a basis $(u_1,\ldots,u_n)$ of V is $Y=BX$, with B a block diagonal matrix of companion matrices of dimensions $n_1,\ldots,n_r$. Then $V=K[x]<w_1>\oplus\cdots\oplus K[x]<w_r>$ with $w_1=u_1$, $w_2=u_{n_1+1},\cdots,$ $w_r=u_{n_1+\cdots+n_{r-1}+1}$. So, the above proposition yields directly $w_1+\cdots+w_r$ as the searched vector v_1.

Now, if $P_{ij}(t)$ denotes the elemental matrix $E_{ii}+tE_{ij}$[3], we may apply the algorithm Frobenius [5, p. 42] to the matrix $P^{-1}BP$ where $P=P_{1,n_1+1}(1)\cdots P_{1,n_1+\cdots+n_{r-1}+1}(1)$, obtaining a cyclic form B^* of B such that $B^*=[C_1^*,\ldots,C_s^*]$ and $\mathrm{pol.char}(C_1^*)=\mathrm{min.pol}(w_1+\cdots+w_r)=\mathrm{min.pol}(V)$.

3. THE ALGORITHM RATIONAL

The algorithm we are going to propose in the following consists of an iteration of the above argument over $[C_2^*,\ldots,C_s^*]$. We assume we know a procedure, denoted by Ciclica, for computing a cyclic form of A and the corresponding change matrix P, for instance see [2], [5, Ch. II, p. 42]:

---

[3] E_{ij} is the matrix whose (k,r)–entry is 1, if $k=i$ and $r=j$, and 0 otherwise.

Algorithm **RATIONAL** (A)

Input: *A Matrix A of order n over K.*

Output: *The rational form F of A and a change matrix P such that* $P^{-1}AP=F$.

Begin

$A:=\left[\frac{A}{I_n}\right]$; $d:=1$;

$\{A,L\}:=$ Ciclica (A,d); %L keeps the indices, greater than d, of the columns heading the blocks of A.

While non vacuous L do

begin

1.– $A:=P_{L(r)d}(-1)\cdots P_{L(1)d}(-1)\cdot A\cdot P_{L(1)d}(1)\cdots P_{L(r)d}(1)$

2.– $\{A,L\}:=$ Ciclica (A,d);

3.– If non vacuous L then $d:=L(1)$; $L:=$rest(L)

end;

return A

end;

REFERENCES

1. A. DANILEVSKI, On a numerical solution of Vekua's equation, *Mat. Sob.* **2** (1937), 169–171 (Russian).
2. M. MATHIEU AND D. FORD, On p–adic computation of the rational form of a matrix, *J. Symb. Comput.* **10** (1990), 453–464.
3. F.R. GANTMACHER, "The Theory of Matrices", Chelsea Publishing Company, New York, 1977.
4. H. LUNEBURG, "On the Rational Normal Form of Endomorphisms", BI–Wissenschaftverlag, Mannheim, 1981.
5. P. OZELLO, Calcul exact des formes de Jordan et de Frobenius d'une matrice, Doctoral Thesis, Univ. of Grenoble, 1987.
6. J.H. WILKINSON, "The Algebraic Eigenvalue Problem", Oxford University Press, 1965.