An algorithm for a result on minimal polynomials

S.D. Agashe

Department of Electrical Engineering, Indian Institute of Technology, Powai, Bombay 400 076, India

Received 24 December 2000; accepted 4 February 2002

Submitted by R. Bhatia

Abstract

For a linear transformation on a finite-dimensional vector space, we give an algorithm, involving rational operations only, to obtain a vector whose minimal polynomial is the same as that of the whole space.

© 2002 Elsevier Science Inc. All rights reserved.

1. Introduction

Given a linear transformation $A$ on a finite-dimensional vector space $V$, it is an easy matter to compute the minimal polynomial (mp) of a non-zero vector and also to compute the mp of the whole vector space. It is not immediately clear, however, that the mp of the whole space is the mp of some vector. This assertion is a well-known theorem, see e.g. [1, p. 180].

Theorem. In a vector space there always exists a vector whose mp coincides with the mp of the whole space.

Such a vector, and not its mere existence, is needed in one approach to the construction of the Frobenius–Kowalewsky (Rational) canonical form of a matrix. In [1], this theorem is proved in three steps:

(a) Invoking the factorization of the mp of the whole space into a product of powers of prime (irreducible) polynomials.
(b) Using the following lemma [1, p. 181]: “If the mp’s of the vectors $e'$ and $e''$ are co-prime, then the mp of the sum vector $e' + e''$ is equal to the product of the mp’s of the constituent vectors”.

(c) Showing that if the mp of a space is a power of an irreducible polynomial, then for any basis, the mp of the space is the same as the mp of (at least) one of the basis vectors.

In the present note, we prove a new result (Lemma 1) about a factorization associated with a pair of polynomials. Then, starting with any non-zero vector, one can construct, using this lemma, a sequence of vectors whose mp’s have increasing degrees till one reaches the mp of the whole space and thus obtains a vector whose mp it is.

2. A lemma on factorization of a pair of polynomials

**Lemma 1.** Let $p_1$ and $p_2$ be two polynomials such that they are not co-prime and neither is a factor of the other. Then, one can calculate by rational operations the coprime-power-factorizations

$$p_1 = t_1^{m_1} t_2^{m_2} \cdots s_1^{n_1} s_2^{n_2} \cdots t_1,$$

$$p_2 = t_1^{n_1} t_2^{n_2} \cdots s_1^{m_1} s_2^{m_2} \cdots t_2,$$

where $m_1 \geq n_1$, $m_2 \geq n_2$, ..., $m_1 \leq n_1'$, $m_2 \leq n_2'$, ..., and the polynomials $r_1, r_2, \ldots, s_1, s_2, \ldots, t_1$ and $t_2$ are all pairwise co-prime. The LCM of $p_1$ and $p_2$ is given by

$$\text{LCM}(p_1, p_2) = (t_1^{m_1} t_2^{m_2} \cdots t_1)(s_1^{n_1'} s_2^{n_2'} \cdots t_2)$$

so that the first major factor on the right side above is a factor of $p_1$, the second one a factor of $p_2$, and the two factors are co-prime.

**Remark 1.** Such factorizations were introduced by Ingraham [2], who proved their existence by invoking the prime-power-factorization of each of the two polynomials, and comparing the factors. This, however, is a ‘non-constructive’ computation. In our proof, we make use of rational operations only.

**Remark 2.** Thus, although, perhaps, a single polynomial cannot be algorithmically factorized into its prime-power-factorization, given two polynomials, their LCM can be factorized into a co-prime-power-factorization. All the individual polynomials in the factorizations above need not be prime(irreducible). Further, if $p_1$ and $p_2$ are co-prime, $\text{LCM}(p_1, p_2) = p_1 p_2$ is itself a co-prime factorization.

**Proof of Lemma 1.** We proceed by induction on the sum of the degrees of $p_1$ and $p_2$, and use the fact that the Euclidean Division Algorithm enables us to algorithmi-
cally obtain the highest-common-factor (HCF) as well as the LCM of two polynomials.

Let \( q \) be the HCF of \( p_1, p_2 \) so that \( p_1 = q q_1 \) and \( p_2 = q q_2 \) where \( q_1 \) and \( q_2 \) can be algorithmically obtained. Now, apply the induction step to the pair \((q, q_1, q_2)\).

(Note \( \deg p_1 + \deg p_2 > \deg q + \deg q_1 q_2 \).) Let \( q = r_1^{m_1} r_2^{m_2} \cdots s_1^{n_1} s_2^{n_2} \cdots t_1 \), and \( q_1 q_2 = r_1^{m_1} r_2^{n_2} \cdots s_1^{n_1} s_2^{n_2} \cdots t_2 \). But \( q_1 \) and \( q_2 \) are co-prime, as also the polynomials \( r_1, r_2, \ldots, s_1, s_2, \ldots, t_1 \) and \( t_2 \). So, factorizations of each of \( q_1 \) and \( q_2 \) can be obtained by separating the powers and breaking up \( t_2 \) (by simply dividing \( q_1 q_2 \) by \( q_1 \), say) to get \( q_1 = r_1^{n_1} r_2^{n_2} \cdots s_1^{n_1} s_2^{n_2} \cdots t_2 \), and \( q_2 = r_1^{n_1} r_2^{n_2} \cdots s_1^{n_1} s_2^{n_2} \cdots t_2 \). where, if \( n_1 \) is not zero, then \( n_2 \) is zero, and so on. Now, compute \( p_1 = q q_1 \), \( p_2 = q q_2 \), and collect the powers together.

3. Computation of the vector whose mp is the same as the mp of the whole space

The following lemma is almost obvious.

**Lemma 2.** Let \( p \) be the mp of a vector \( e \) and let \( p \) have a factorization \( p = p_1 p_2 \). Then \( p_2 \) is the mp of the non-zero vector \( p_1(A)(e) \).

We now state the procedure for obtaining a vector whose mp is the same as the mp of the whole space.

**Procedure.** To compute the desired vector, choose any non-zero vector \( a_1 \) and let its mp be \( p_1 \). If \( \ker(p_1(A)) = V \), we are through. If not, there is a vector \( a_2 \) not in \( \ker(p_1(A)) \); let its mp be \( p_2 \). Then, \( p_2 \) cannot divide \( p_1 \), and also must be distinct from \( p_1 \). If \( p_2 \) is of degree higher than that of \( p_1 \), we continue with \( a_2 \) and \( p_2 \). If not, and if \( p_1 \) and \( p_2 \) are co-prime, we use Gantmacher’s lemma. If none of these conditions occur, then \( p_1 \) and \( p_2 \) are not co-prime, and using Lemma 1, we obtain a factorization of \( \text{LCM}(p_1, p_2) \) into co-prime factors, and using Lemma 2 and Gantmacher’s lemma, we obtain a vector \( b_1 \), say, whose mp, \( \text{LCM}(p_1, p_2) \), is of a degree higher than that of \( p_1 \). We continue with \( b_1 \) as we did with \( a_1 \). Since \( V \) is finite-dimensional, this process must end after a finite number of steps.

**References**