BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES
Vol. 56, No. 4, 2008

An algorithm for the calculation of the minimal polynomial

S. BIAŁAS [1]* and M. BIAŁAS [2]

[1] The School of Banking and Management, 4 Armii Krajowej St., 30-150 Kraków, Poland
[2] Faculty of Management, AGH University of Science and Technology, 30 Mickiewicza St., 30-059 Kraków, Poland

Abstract. This paper gives the simple algorithm for calculation of the degree and coefficients of the minimal polynomial for the complex matrix $A = [a_{ij}]_{n\times n}$.

Key words: matrix, minimal polynomial, characteristic polynomial.

1. Introduction

We use the standard notation. We denote by $M_{m,n}$ the set of $m \times n$ real or complex matrices. In case $n = m$ we will write M_n instead of $M_{n,n}$.

A complex polynomial $f(\lambda)$ is called an annihilationy polynomial for a matrix $A \in M_n$ if $f(\lambda) \not\equiv 0$ and $f(A) = 0 \in M_n$. The complex polynomial

$$f(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0,$$

where $a_n \neq 0$, is called monic if its leading coefficient $a_n = 1$. The monic polynomial $\psi(\lambda)$ of least degree for which $\psi(A) = 0 \in M_n$ is called the minimal polynomial of the matrix $A \in M_n$.

The properties and the applications of the minimal polynomials in the control theory have been presented in [1, 2].

In this paper the simple algorithm is given for the calculation of the degree and coefficients of the minimal polynomial.

For the matrix $A = [a_{ij}] \in M_n$ we will use the following notations:
$\varphi(\lambda) = \det(\lambda I - A)$ – charecteristic polynomial of the matrix A,
$\psi(\lambda)$ – minimal polynomial of the matrix A,
$\mathrm{vecA} = [\mathrm{a_{11}\ a_{12} \ldots a_{1n}\ a_{21}\ a_{22} \ldots a_{2n} \ldots a_{n1}\ a_{n2} \ldots a_{nn}}]^{\mathrm{T}}$,
$A^0 = I \in M_n$,
$A^k = A^{k-1}A \quad (k = 1, 2, \ldots),$ (1)
$A^k = [a_{ij}^{(k)}] \quad (k = 0, 1, 2, \ldots),$
$a^{(k)} = \mathrm{vecA^k}$ $(\mathrm{k} = 0, 1, 2, \ldots)$,
$B_k = [a^{(0)}a^{(1)} \cdots a^{(k)}]$ $(k = 0, 1, 2, \ldots)$
where $a^{(k)}$ is $k+1$-th column of the matrix $B_k \in M_{n^2,k+1}$,

rank (B) – rank of the matrix B,
$N = \{1, 2, 3, \ldots\}$,
I or I_n – unit matrix,
$degf(x)$ – degree of the polynomial $f(\lambda)$,
$\emptyset$ – empty set.

Example 1. For the matrix $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ we have:

$$a^{(0)} = [1\ 0\ 0\ 1]^T, \quad a^{(1)} = [a_{11}\ a_{12}\ a_{21}\ a_{22}]^T, \ldots,$$
$$a^{(k)} = [a_{11}^{(k)}\ a_{12}^{(k)}\ a_{21}^{(k)}\ a_{22}^{(k)}]^T,\ B_0 = [a^{(0)}] = [1\ 0\ 0\ 1]^T,$$
$$B_1 = [a^{(0)}a^{(1)}] = \begin{bmatrix} 1 & a_{11} \\ 0 & a_{12} \\ 0 & a_{21} \\ 1 & a_{22} \end{bmatrix}.$$

2. An algorithm for the calculation of the degree and the coefficients of the minimal polynomial

For the matrix $A = [a_{ij}] \in M_n$ we will prove the following Lemma.

Lemma 1. If the matrix $A = [a_{ij}] \in M_n$, the matrix B_k is defined by (1), then

$$K = \{k \in N :\ \mathrm{rank\ B_k} =\ \mathrm{rank\ B_{k-1}}\} \neq \emptyset \ \text{ and } \ \mathrm{n} \in \mathrm{K}.$$

Proof. We see that if

$$\varphi(\lambda) = \det(\lambda I - A) = \lambda^n + b_{n-1}\lambda^{n-1} + \cdots + b_1\lambda + b_0,$$

then

$$A^n + b_{n-1}A^{n-1} + \cdots + b_1A + b_0I = 0 \in M_n,$$
$$a^{(n)} = -[b_{n-1}a^{(n-1)} + \cdots + b_1a^{(1)} + b_0a^{(0)}],$$
$$\mathrm{rank\ B_n} = \mathrm{rank}\ [\mathrm{a^{(0)}a^{(1)} \ldots a^{(n)}}]$$
$$= \mathrm{rank}\ [\mathrm{a^{(0)}a^{(1)} \ldots a^{(n-1)}0}] = \mathrm{rank\ B_{n-1}},$$

where $0 = [0\ 0 \ldots 0]^T \in M_{n^2,1}$. Therefore $n \in K$ and $K \neq \emptyset$.

Definition 1. A number $k_0 = \min K$ is called the associated rank of the matrix $A = [a_{ij}] \in M_n$.

Theorem 1. If k_0 is the associated rank of the matrix $A = [a_{ij}] \in M_n$ and $\psi(\lambda)$ is the minimal polynomial of this matrix then:

*e-mail: sbialas@uci.agh.edu.pl

1) $\mathrm{rank}\ B_k = k+1 \quad (k = 0, 1, \ldots, k_0 - 1)$,
2) $\mathrm{rank}\ B_k = k_0 \quad (k \geq k_0)$,
3) $\deg \psi(\lambda) = k_0$,

where the matrix B_k is defined by the relation (1).

Proof. Let $B_k = [a^{(0)}a^{(1)} \cdots a^{(k_0-1)}a^{(k_0)}a^{(k_0+1)} \cdots a^{(k)}]$.

First we will prove that $\mathrm{rankB_k} = k+1$ ($k = 0, 1, \ldots, k_0 - 1$). From the definition of k_0 it follows that $\mathrm{rankB_{k_0}} = \mathrm{rankB_{k_0-1}}$. For $k_0 = 1$ $\mathrm{rankB_1} = \mathrm{rankB_0} = 1$.

However, for $k_0 > 1$ we have:

$$\mathrm{rankB_1} > \mathrm{rankB_0} = 1 \Rightarrow \mathrm{rankB_1} = 2,$$

$$\mathrm{rankB_2} > \mathrm{rankB_1} = 2 \Rightarrow \mathrm{rankB_2} = 3,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\mathrm{rankB_{k_0-1}} > \mathrm{rankB_{k_0-2}} = k_0 - 1 \Rightarrow \mathrm{rankB_{k_0-1}} = k_0.$$

Therefore $\mathrm{rankB_k} = k+1$ for $k \in \{0, 1, 2, \ldots, k_0 - 1\}$ and $\mathrm{rankB_{k_0}} = \mathrm{rankB_{k_0-1}} = k_0$. Hence it follows that the columns $a^{(0)}, a^{(1)}, \ldots, a^{(k_0-1)}$ are linear independent and the column $a^{(k_0)}$ can be written as the linear combination of the columns $a^{(0)}, a^{(1)}, \ldots, a^{(k_0-1)}$, so there exists $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{k_0-1}) \in C^{k_0}$ such that

$$\alpha_0 a^{(0)} + \alpha_1 a^{(1)} + \cdots + \alpha_{k_0-1} a^{(k_0-1)} = -a_0^{(k_0)}.$$

It denotes that

$$\alpha_0 I + \alpha_1 A + \cdots + \alpha_{k_0-1} A^{k_0-1} + A^{k_0} = 0 \in M_n$$

and the polynomial $f(\lambda) = \alpha_0 + \alpha_1\lambda + \cdots + \lambda^{k_0}$ is the annihilationy polynomial of the matrix A.

For $k > k_0$, $m = k - k_0$ and any arbitrary numbers $\beta_0, \beta_1, \ldots, \beta_{m-1} \in C$ the polynomial $g(\lambda) = f(\lambda)(\beta_0 + \beta_1\lambda + \cdots + \beta_{m-1}\lambda^{m-1} + \lambda^m) = \gamma_0 + \gamma_1\lambda + \ldots + \gamma_{k-1}\lambda^{k-1} + \lambda^k$ is the annihilationy polynomial of the matrix A, too. Therefore

$$\gamma_0 I + \gamma_1 A + \cdots + \gamma_{k-1} A^{k-1} + A^k = 0 \in M_n,$$
$$\gamma_0 a^{(0)} + \gamma_1 a^{(1)} + \cdots + \gamma_{k-1} a^{(k-1)} + a^{(k)} = 0 \in M_{n^2,1}. \tag{2}$$

In the matrix $B_k = [a^{(0)}a^{(1)} \cdots a^{(k_0-1)}a^{(k_0)}a^{(k_0+1)} \cdots a^{(k)}]$ the column $a^{(j)}$ can be multiplied by $-\gamma_j$ ($j = 0, 1, \ldots, k-1$) and added to the column $a^{(k)}$. Hence and (2) we have

$$\mathrm{rankB_k} = \mathrm{rank}[a^{(0)}a^{(1)} \cdots a^{(k-1)}0] = \mathrm{rankB_{k-1}}.$$

Similary transformation can be used to the matrix B_{k-1}. At the end, we have

$$\mathrm{rankB_k} = \mathrm{rank}[a^{(0)}a^{(1)} \cdots a^{(k_0-1)}a^{(k_0)}0 \cdots 0] = \mathrm{rankB_{k_0}} = k_0$$

for $k \geq k_0$. This finishes the proof of 2) of the Theorem 1.

Now we prove that if $\psi(\lambda)$ is the minimal polynomial of the matrix A then $\deg \psi(\lambda) = k_0$.

Hence that $\mathrm{rankB_{k_0}} = \mathrm{rankB_{k_0-1}} = k_0$ it follows that the set of equations

$$B_{k_0-1}\alpha = -a^{(k_0)},$$

with the unknown $\alpha = [\alpha_0\alpha_1 \ldots \alpha_{k_0-1}]^T \in C^{k_0}$, has only one solution and

$$\alpha_0 I + \alpha_1 A + \cdots + \alpha_{k_0-1} A^{k_0-1} + A^{k_0} = 0 \in M_n,$$

besides

$$\alpha_0 + \alpha_1\lambda + \cdots + \alpha_{k_0-1}\lambda^{k_0-1} + \lambda^{k_0}, \tag{3}$$

is the annihilationy polynomial of the matrix A.

Hence that $\mathrm{rankB_k} = k+1$ ($k = 0, 1, \ldots, k_0 - 1$) it follows that the set of equations

$$B_{k-1}\alpha = -a^{(k)},$$

with the unknown $\alpha = [\alpha_0\alpha_1 \ldots \alpha_{k-1}]^T \in C^k$, has not the solutions.

This denotes that the polynomial (3) is the minimal polynomial of the matrix A and $\deg \psi(\lambda) = k_0$.

Now, we give the algorithm for the calculation of the degree and coefficients of the minimal polynomial of the matrix $A = [a_{ij}] \in M_n$.

Consider the matrix

$$B_n = [a^{(0)}a^{(1)} \ldots a^{(n)}] \in M_{n^2,n+1},$$

which is defined in (1).

The elements of the matrix B_n are denoted by b_{ij}, therefore $B_n = [b_{ij}] \in M_{n^2,n+1}$, where $b_{11} = 1$, $b_{12} = a_{11}^{(1)}, \ldots, b_{1,n+1} = a_{11}^{(n)}, \ldots, b_{n^2,n+1} = a_{nn}^{(n)}$.

We will calculate the rank of the matrix B_n by Gaussian elimination, except interchange and cancel of the null columns.

We obtain

$$\mathrm{rankB_n} = \mathrm{rank}\begin{bmatrix} 1 & b_{12} & \ldots & b_{1,n+1} \\ 0 & b_{22}^{(1)} & \ldots & b_{2,n+1}^{(1)} \\ 0 & b_{32}^{(1)} & \ldots & b_{3,n+1}^{(1)} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & b_{n^2,2}^{(1)} & \ldots & b_{n^2,n+1}^{(1)} \end{bmatrix},$$

where, for example $b_{22}^{(1)} = b_{22}, \ldots, b_{2,n+1}^{(1)} = b_{2,n+1}, b_{n^2,2}^{(1)} = b_{n^2,2} - b_{12}$.

From the Lemma 1 it follows that $n \in K = \{k \in N : \mathrm{rankB_k} = \mathrm{rankB_{k-1}}\}$.

Therefore there exists $r \in N$ such that $r \leq n$ and

$$\mathrm{rankB_n} = \mathrm{rank}\begin{bmatrix} 1 & b_{12} & b_{13} & \dots & \dots & \dots & \dots & \dots & \dots & b_{1,n+1} \\ 0 & b_{12}^{(1)} & b_{23}^{(1)} & \dots & \dots & \dots & \dots & \dots & \dots & b_{2,n+1}^{(1)} \\ 0 & 0 & b_{33}^{(2)} & \dots & \dots & \dots & \dots & \dots & \dots & b_{3,n+1}^{(2)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & b_{rr}^{(r-1)} & b_{r,r+1}^{(r-1)} \dots & \dots & \dots & b_{r,n+1}^{(r-1)} \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & b_{r+1,r+2}^{(r-1)} & \dots & b_{r+1,n+1}^{(r-1)} \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & b_{r+2,r+2}^{(r-1)} & \dots & b_{r+2,n+1}^{(r-1)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & b_{n^2,r+2}^{(r-1)} & \dots & b_{n^2,n+1}^{(r-1)} \end{bmatrix},$$

where $b_{ii}^{(i-1)} \neq 0$ $(i = 1, 2, \dots, r)$.

From this it follows that $\mathrm{rankB_j} = \mathrm{j}$ $(j = 1, 2, \dots, n)$, $\mathrm{rankB_{r-1}} = \mathrm{r}$, $\mathrm{rankB_r} = \mathrm{r}$.

Therefore $k_0 = \min K = r$ and $\deg \psi(\lambda) = r = k_0$.

Thus, by Gaussian elimination we can compute the degree of the minimal polynomial of the matrix A.

Hence that $\det B_{r-1} = \det B_{k_0-1} \neq 0$ and $\mathrm{rankB_{k_0}} = \mathrm{rankB_{k_0-1}} = \mathrm{k_0}$ it follows that the set of equations

$$B_{k_0-1}\alpha = -a^{(k_0)}, \tag{4}$$

with the unknown $\alpha = [\alpha_0\alpha_1 \dots \alpha_{k_0-1}]^T \in C^{k_0}$, has only one solution and

$$\alpha_0 + \alpha_1 A + \dots + \alpha_{k_0-1}A^{k_0-1} + A^{k_0} = 0 \in M_n.$$

Therefore $\alpha_0, \alpha_1, \dots, \alpha_{k_0-1}, 1$ are the coefficients of the minimal polynomial of the matrix A. The set of Eq. (4) is equivalent to the set of equations

$$\tilde{B}\alpha = \tilde{b},$$

where

$$\tilde{B} = \begin{bmatrix} 1 & b_{11} & \dots & \dots & b_{1r} \\ 0 & b_{22}^{(1)} & \dots & \dots & b_{2r}^{(1)} \\ 0 & 0 & b_{33}^{(2)} & \dots & b_{3r}^{(2)} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & b_{rr}^{(r-1)} \end{bmatrix}, \tilde{b} = \begin{bmatrix} b_{1,r+1} \\ b_{2,r+1}^{(1)} \\ \vdots \\ b_{r,r+1}^{(r-1)} \end{bmatrix},$$

$\alpha = [\alpha_0 \ \alpha_1 \ \dots \ \alpha_{k_0-1}]^T$, $r = k_0$.

Example 2. We will calculate the minimal polynomial of the matrix

$$A = \begin{bmatrix} 3 & -3 & 2 \\ -1 & 5 & -2 \\ -1 & 3 & 0 \end{bmatrix}.$$

In this example we have

$$A^2 = \begin{bmatrix} 10 & -18 & 12 \\ -6 & 22 & -12 \\ -6 & 18 & -8 \end{bmatrix},$$

$$A^3 = \begin{bmatrix} 36 & -84 & 56 \\ -28 & 92 & -56 \\ -28 & 84 & -48 \end{bmatrix},$$

$$\mathrm{rankB_3} = \mathrm{rank}\begin{bmatrix} 1 & 3 & 10 & 36 \\ 0 & -3 & -18 & -84 \\ 0 & 2 & 12 & 56 \\ 0 & -1 & -6 & -28 \\ 1 & 5 & 22 & 92 \\ 0 & -2 & -12 & -56 \\ 0 & -1 & -6 & -28 \\ 0 & 3 & 18 & 84 \\ 1 & 0 & -8 & -48 \end{bmatrix}$$

$$= \mathrm{rank}\begin{bmatrix} 1 & 3 & 10 & 36 \\ 0 & -3 & -18 & -84 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = 2,$$

$$\tilde{B} = \begin{bmatrix} 1 & 3 \\ 0 & -3 \end{bmatrix}, \tilde{b}\begin{bmatrix} -10 \\ 18 \end{bmatrix}, \quad k_0 = 2,$$

$$\alpha = [\alpha_0 \ \alpha_1]^T = [8 \ -6]^T.$$

Therefore, $\psi(\lambda) = \lambda^2 - 6\lambda + 8$. is the minimal polynomial of the matrix A.

REFERENCES

[1] S. Barnett, *Matrices in Control Theory*, Van Nostrand Reinhold Company, London, 1960.

[2] T. Kaczorek, *Vectors and Matrices in Automatics and Electrotechnics*, WNT, Warszawa, 1998.