# MATH2999 Directed Studies in Mathematics Matrix Theory and Its Applications

**Research Topic** 

## **Minimal Polynomials and Its Applications**

<sup>By</sup> Zhang Shixiao

Supervisors: Prof. Li Chi-Kwong and Dr. Chan Jor-Ting

### Contents

Abstract

- 1. Introduction: Background
- 2. Power of Matrices
  - 2.1 Characteristic Polynomial and Minimal Polynomial of a Matrix
    - 2.1.1 Basic Observations
    - 2.1.2 Existence of Minimal Polynomials
    - 2.1.3 Uniqueness of Minimal Polynomials
  - 2.2 Computation about Minimal Polynomials
  - 2.3 Three Schemes to Compute the Power of Matrices
    - 2.3.1 Diagonalizable Matrices
    - 2.3.2 Comparing with Cayley-Hamilton Theorem
    - 2.3.3 Remark: Extensions about the Power of Matrices
    - 2.3.4 Partial Fraction Decomposition
  - 2.4 Application in Controllability of Systems
- 3. Conclusion

#### Abstract

In this project, we present theory about minimal polynomials of matrices. Both theoretical notations and applications in various fields will be discussed. We will start with the general properties of minimal polynomials, and apply the techniques to compute the power of matrices and the stationary distribution of a finite Markov Chain.

#### 1. Introduction: Background

*Matrix Theory* (or *Linear Algebra*) sometimes is regarded as one of the two most basic concepts in mathematics (the other is *Calculus* of course). Matrices are widely used in both science and engineering. Matrix models are often used to represent different systems, simulate various processes and compute final tendency of frameworks. It is well-known that minimal polynomials are treated as one of the most pivotal concepts to reduce the power of matrices, which sometimes represent the long-term variation tendency. They probably have been full-understood and been transferred to not only mathematics applications, but also statistics, economics, dynamic systems, so on and so forth. Researchers have studied minimal polynomials for a long time, different measurements and methods have been developed to calculate the power of matrices, which is used to describe the flow direction of a particular system or process while the stationary distribution, which is the limiting behaviour of a stochastic process, sometimes could be fully-translated to be an eigenvalue-eigenvector problem. Therefore, we are aiming at figuring out the underlying foundation of these methods and make a connection and comparison among different sections.

#### 2. Power of Matrices

#### 2.1 Characteristic Polynomial and Minimal Polynomial of a Matrix

#### 2.1.1 Basic Observations

First note that the analysis for functions could be easily extended to matrices. Generally speaking, for analytic functions, if *S* is the set of all matrices *T* such that  $\sum_{n=0}^{\infty} \alpha_n T^n$  converges, then we define *f* to be  $f(T) = \sum_{n=0}^{\infty} \alpha_n T^n$  for all *T* belongs to *S* and we can see *f* is a matrix-valued function. As for a square matrix, there must exist some polynomials  $f(\lambda)$  such that when we plug in the matrix A, f(A) = 0. One famous such polynomial is called *characteristic polynomial* of a matrix A, which is denoted as  $p_A(z) = \det(zI - A)$ . The result  $p_A(A) = 0$ , one should recall, is the famous *Cayley– Hamilton Theorem*, which we will discuss in the latter section. On the other hand, among all such polynomials, there must one kind of polynomial with the lowest degree  $\mu$ , and when we divide such polynomials by the coefficient of  $\lambda^{\mu}$ , the result must be identical. Otherwise, if we obtain  $f_1(\lambda)$  and  $f_2(\lambda)$  which  $f_1(\lambda) \neq f_2(\lambda)$ , then

$$f_1(\lambda) - f_2(\lambda) = \sum_{i=0}^{\mu-1} \alpha_i \lambda^i$$
, substitute A, we will get  $f_1(A) - f_2(A) = \sum_{i=0}^{\mu-1} \alpha_i A^i = 0$ , which

contradicts with the lowest degree assumption. Therefore, we denote such lowest degree polynomials to be the minimal polynomial of a matrix and write as m(A).

#### 2.1.2 Existence of Minimal Polynomials

To be a minimal polynomial of a matrix, there are three conditions must be satisfied, namely, (1) p(A)=0 (2) p has the lowest degree which means if m' is another nonzero polynomial such that m'(A)=0,  $deg(m')\geq deg(m)$ . (3) p is monic.

As a sequence of matrices, we denote *m* to be the smallest integer such that *I*, *A*, ...,  $A^m$  are linearly dependent. By saying linearly dependent, we mean that there exist some coefficients  $\alpha_1$ ,  $\alpha_2$ , ...,  $\alpha_m$  which are not all equal to zero, and  $\sum_{i=1}^m \alpha_i A^i = 0$ .

Because of *m* is the minimal integer defined as above,  $\alpha_m \neq 0$ , then  $\alpha_m A^m + \sum_{i=1}^{m-1} \alpha_i A^i = 0$ 

could be rewritten as 
$$A^m + \sum_{i=1}^{m-1} \beta_i A^i = 0$$
 where  $\beta_i = \frac{\alpha_i}{\alpha_m}$  for  $i=1, 2, ..., m-1$ . Let

$$p_A(\lambda) = \lambda^m + \sum_{i=1}^{m-1} \beta_i \lambda^i$$
, observed that  $p_A(A) = 0$ , hence p is the minimal polynomial of A.

#### 2.1.3 Uniqueness of Minimal Polynomials

If *p* and *p*' are both minimal polynomials of *A*, we divide *p*' by *p*, use the Euclidean Algorithm for Polynomials, we will get  $p'(\lambda) = p(\lambda)q(\lambda) + r(\lambda)$ , substitute *A*, p'(A) = p(A)q(A) + r(A) which means r(A) = 0. On the other hand, deg(r) < deg(p), hence r=0 according to the lowest degree assumption. Therefore, p'(r) = p(r)q(r).

Moreover, p' and p must have the same degree, which means  $q(\lambda)$  is just a constant polynomial and equal to 1 according to the monic condition. That means p'=p, which proves the uniqueness of minimal polynomials.

#### 2.2 Computation about Minimal Polynomials

The existence of minimal polynomials also highlights a method for us to find it. We solve the equation,  $A = \beta_0 I$ , if no solution, we move on to solve  $A^2 = \beta_0 I + \beta_1 A$ , do such an algorithm step by step until we get a solution such that  $A^m = \sum_{i=1}^{m-1} \beta_i A^i$ . By looking at the definition, such an algorithm must stop by some finite number of steps. Moreover, given *A* is an *n* by *n* square matrix, from the perspective of *Cayley-Hamilaton theorem*, this kind of process will necessarily end within *n* steps.

On the other hand, for the matrix  $A = (a_{ij}) \in M_n$ , define

$$\begin{aligned} &\text{vecA} = [a_{11} \ a_{12} \dots a_{1n} \ a_{21} \ a_{22} \dots a_{2n} \dots a_{n1} \ a_{n2} \dots a_{nn}]^{\text{T}} \\ &A^{0} = I \in M_{n}, \\ &A^{k} = A^{k-1}A \quad (k = 1, 2, \dots), \\ &A^{k} = [a_{ij}^{(k)}] \quad (k = 0, 1, 2, \dots), \\ &a^{(k)} = \text{vecA}^{k} \ (k = 0, 1, 2, \dots), \\ &B_{k} = [a^{(0)}a^{(1)} \dots a^{(k)}] \ (k = 0, 1, 2, \dots) \\ &\text{where } a^{(k)} \text{ is } k + 1\text{-th column of the matrix } B_{k} \in M_{n^{2}, k+1} \end{aligned}$$

then  $K = \{k \in N : rank(B_k) = rank(B_{k-1})\} \neq 0$ . Moreover, if  $k_0 = \min K$  is the associated rank of matrix A and p is the minimal polynomial of A, then  $rank(B_k) = k+1$  for  $k = 0, 1, ..., k_0 - 1$ , and  $rank(B_k) = k_0$  for  $k \ge k_0$ ,  $deg(p) = k_0$ .

Now we consider  $B_n = (a^{(0)} a^{(1)} \cdots a^{(n)}) \in M_{n^2, n+1}$ , while  $B_n = (b_{ij})$ ,  $b_{11} = 1, b_{12} = a_{11}^{(1)}, \dots, b_{1, n+1} = a_{11}^{(n)}, \dots, b_{n^2, n+1}^{(n)} = a_{nn}^{(n)}$ , then we calculate the rank of  $B_n$ , which is

$$rank(B_{n}) = rank \begin{pmatrix} 1 & b_{12} & \cdots & b_{1,n+1} \\ 0 & b_{22}^{(1)} & \cdots & b_{2,n+1}^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & b_{n^{2},2}^{(1)} & \cdots & b_{n^{2},n+1}^{(1)} \end{pmatrix}, \text{ therefore, there exists } r \in N \text{ such that } r \leq N$$

and

If we set  $\alpha_0 + \alpha_1 A + \cdots + \alpha_{k_0-1} A^{k_0-1} + \alpha_{k_0} A^{k_0} = 0$ , where  $\alpha_i$ 's are the coefficients of the minimal polynomial of the matrix A, then the only solution is obtained by solving  $\tilde{B}\alpha = \tilde{b}$  where

$$\tilde{B} = \begin{bmatrix} 1 & b_{11} & \dots & b_{1r} \\ 0 & b_{22}^{(1)} & \dots & b_{2r}^{(1)} \\ 0 & 0 & b_{33}^{(2)} & \dots & b_{3r}^{(2)} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & b_{rr}^{(r-1)} \end{bmatrix}, \tilde{b} = \begin{bmatrix} b_{1,r+1} \\ b_{2,r+1}^{(1)} \\ \vdots \\ b_{r,r+1}^{(r-1)} \\ \vdots \\ b_{r,r+1}^{(r-1)} \end{bmatrix}$$
$$\alpha = [\alpha_0 \ \alpha_1 \ \dots \ \alpha_{k_0-1}]^T, \ r = k_0.$$

#### 2.3 Three Schemes to Compute the Power of Matrices

#### 2.3.1 Diagonalizable Matrices

In the simplest case, when the matrix is diagonalizable, we can always use the diagonality/similarity method to carry out the diagonal matrix. Recall that a  $n \times n$  matrix is diagonalizable if it has *n* distinct eigenvalues. In general, we write

$$SPS^{-1} = \begin{pmatrix} \lambda_1 & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$
 Observed that if the first row of S is normalized to  $\pi$ , then the

first column of  $S^{-1}$  must be normalized to **1** since  $SS^{-1} = I$  and hence  $(SV)_{11} = u_1v_1 = \pi v_1 = I$ where  $u_i$  and  $v_i$ 's are the row vectors and column vector of S and  $S^{-1}$  respectively.

Denote 
$$\Lambda = \begin{pmatrix} 1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}, P^t = S^{-1} \begin{pmatrix} 1 & & & & \\ & \lambda_2^t & & & \\ & & \ddots & & \\ & & & \lambda_2^t \end{pmatrix} S \xrightarrow{t \to \infty} \begin{pmatrix} v_{11}u_1 \\ v_{12}u_1 \\ \vdots \\ v_{1n}u_1 \end{pmatrix} = \begin{pmatrix} \pi \\ \pi \\ \vdots \\ \pi \end{pmatrix}$$

where  $v_{ij}$ 's are the *j*th entry of the column vector  $v_i$  since *P* has the unique largest eigenvalue  $\lambda_1 = 1$  by *Perron-Frobenius Theorem*. One may consider  $1 > |\lambda_2| \ge |\lambda_3| \ge \cdots \ge |\lambda_n|$ , generally, given an initial distribution  $q_0$ ,  $q^{(t)} = qP^t = \pi + \sum_{i=2}^n q_i^{-1} \lambda_i^i u_i$ 

where 
$$q_i = \frac{qu_i^T}{\|u_i\|^2}$$
,  $u_i$ 's are just the eigenvalue basis for P

Numerical Example:

Diagonalize 
$$P = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{3}{4} & \frac{1}{4} \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ -3 & 1 \end{pmatrix}^{-1} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{3}{4} & \frac{1}{4} \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{4} & 0 \\ 0 & 1 \end{pmatrix}$$
  
$$\lim_{n \to \infty} P^n = \lim_{n \to \infty} \begin{pmatrix} 2 & 1 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} (-\frac{1}{4})^n & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{3}{5} & \frac{2}{5} \\ \frac{3}{5} & \frac{2}{5} \\ \frac{3}{5} & \frac{2}{5} \end{pmatrix}$$
$$(I - zP)^{-1} = (1 + z + z^2 + z^3 + \cdots) \begin{pmatrix} \frac{3}{5} & \frac{2}{5} \\ \frac{3}{5} & \frac{2}{5} \\ \frac{3}{5} & \frac{2}{5} \end{pmatrix} + [1 - \frac{z}{4} + (\frac{z}{4})^2 - (\frac{z}{4})^3 + \cdots] \begin{pmatrix} \frac{2}{5} & -\frac{2}{5} \\ -\frac{3}{5} & \frac{3}{5} \end{pmatrix}$$

#### 2.3.2 Comparing with Cayley-Hamilton Theorem

Minimal polynomials state out a framework for efficiently computing the power of matrices, while the famous Cayley-Hamilton theorem also wins a lot of attraction for determining the coefficients of the characteristic polynomial in terms of matrix components. Here we will give a brief description about this enchanting theorem. Suppose *A* is an  $n \times n$  matrix, then the characteristic polynomial we define above is  $p_A(z) = \det(zI - A)$ , then p(A)=0. Without loss of generality, let us write  $p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_0$ , denote  $B(\lambda)$  to be the adjoint matrix of  $\lambda I - A$ , then  $B(\lambda)(\lambda I - A) = |\lambda I - A|I = p(\lambda)I = \lambda^n I + a_{n-1}\lambda^{n-1}I + \dots + a_0I$ , on the other hand, write  $B(\lambda)$  as  $B(\lambda) = \lambda^{n-1}B_{n-1} + \lambda^{n-2}B_{n-2} + \dots + \lambda B_1 + B_0$ , where  $B_i$ 's are  $n \times n$  matrices. Then we get

$$B(\lambda)(\lambda I - A) = (\lambda^{n-1}B_{n-1} + \lambda^{n-2}B_{n-2} + \dots + \lambda B_1 + B_0)(\lambda I - A)$$
  
=  $\lambda^n B_{n-1} + \lambda^{n-1}(B_{n-2} - B_{n-1}A) + \lambda^{n-2}(B_{n-3} - B_{n-2}A) + \dots + \lambda(B_0 - B_1A) - B_0A$   
=  $\lambda^n I + a_{n-1}\lambda^{n-1}I + \dots + a_0I$ 

Compare the coefficients appearing in the each side of the above equation, we conclude that

$$B_{n-1} = I$$
  
 $B_{n-2} - B_{n-1}A = a_{n-1}I$   
:  
 $-B_0A = a_0I$ 

Moreover, we multiply  $A^n$ ,  $A^{n-1}$ , ..., A, I to each of the above equation respectively, add them together, we can easily get p(A)=0. In particular, given  $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$  is the minimal polynomial of A, which means  $A^m = -a_{m-1}A^{m-1} - \dots - a_1A - a_0I$ , then any power  $k \ge m$  could be expressed as  $A^k = f(A)q(A) + r(A) = r(A)$  if  $x^k = f(x)q(x) + r(x)$ . Cayley-Hamilton Theorem provides us with the conclusion that the degree of the minimal polynomial is just the size of the matrix, say n. In other words, there is no need for us to go through more than nsteps to obtain the minimal polynomial. As for the diagonalizable case, same as the previous notation, if we denote

$$S = (u_1 \quad u_2 \quad \cdots \quad u_n) \text{ and } S^{-1} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

Then

$$A^{m} = r_{n-1}S\begin{pmatrix}\lambda_{1}^{n-1} & \dots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_{n}^{n-1}\end{pmatrix}S^{-1} + r_{n-2}S\begin{pmatrix}\lambda_{1}^{n-2} & \dots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & \lambda_{n}^{n-2}\end{pmatrix}S^{-1} + \dots + r_{0}I$$

$$= S(r_{n-1} \begin{pmatrix} \lambda_1^{n-1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n^{n-1} \end{pmatrix} + r_{n-2} \begin{pmatrix} \lambda_1^{n-2} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n^{n-2} \end{pmatrix} + \dots + r_0 I) S^{-1}$$
$$= S \begin{pmatrix} \lambda_1^m & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n^m \end{pmatrix} S^{-1}$$

What we need to do is solve a batch of equations, namely

$$\begin{pmatrix} \lambda_1^m \\ \lambda_2^m \\ \vdots \\ \lambda_n^m \end{pmatrix} = \begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-1} \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{n-1} \end{pmatrix}$$

2.3.3 Remark: Extensions about the Power of Matrices

One may observed that, if we can efficiently determine the lower power of the matrix, then the higher powers could be obtained by multiplying these lower powers. Theoretically speaking, we can generate  $A^2, A^4, A^8, \cdots$  such kind of matrices by simply checking  $A, A^2, A^3, \cdots, A^n$ . Moreover, if the minimal polynomial of the matrix is  $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$  satisfying  $a_0 \neq 0$ , then

 $A^{-1} = \frac{-A^{m-1} - a_{m-1}A^{m-2} - \dots - a_1I}{a_0}$  given A is invertible. Hence, we can generate the

negative powers for the matrix.

#### 2.3.4 Partial Fraction Decomposition

Write  $(I - zA)^{-1}$  as a power series expansion, and then compare the coefficients of  $A^m$  to get the representative.

$$(I - zA)^{-1} = \frac{1}{\det(I - zA)} adj (I - zA) = \left(\sum_{k=0}^{\infty} \gamma_k z^k\right) \left(z^{n-1}B_{n-1} + z^{n-2}B_{n-2} + \dots + zB_1 + I\right)$$

This should involve the computation of minimal polynomials of a univariate polynomial matrix. You may refer to (Karampetakis 2005). Eventually this method may not be very efficient, but at least, it provides such a framework comparing with previous sections.

2.4 Application in Controllability of Systems

In modern mathematical control theory, stability, controllability and observability are three essential characters describing a system. Here we mainly focus on controllability of systems, and try to highlight some applications of power of matrices and minimal polynomials involved. In general, the mathematical model for a linear time-invariant dynamical control system is represented by x'(t) = Ax(t) + Bu(t), where  $x(t) \in \mathbb{R}^n$  is a state vector,  $u(t) \in \mathbb{R}^m$  is an input vector, A, B are real matrices of appropriate dimensions. By the *Existence and Uniqueness Theorem* for differential equations, given an initial value  $x(0) \in \mathbb{R}^n$  and control  $u(t) \in \mathbb{R}^m$ , there must exist a unique solution for  $x(t; x(0), u) = e^{tA}x(0) + \int_0^t e^{(t-s)A}Bu(s)ds$ .

Definition: a system is said to be controllable if for every initial condition x(0) and every vector  $x^1 \in \mathbb{R}^n$ , there exist a finite time  $t_1$  and control  $u(t) \in \mathbb{R}^m$ ,  $t \in [0, t_1]$ , such that  $x(t_1;x(0),u) = x^1$ .

For a discrete time case, we write  $x_{t+1} = Ax_t + Bu_t$  to represent the system. The controllability concept could be transferred to the following equation

$$x_{t} = \begin{pmatrix} B & AB & A^{2}B & \cdots & A^{t-2}B & A^{t-1}B \end{pmatrix} \begin{pmatrix} u_{t-1} \\ u_{t-2} \\ \vdots \\ u_{0} \end{pmatrix}$$

where  $W_t = \begin{pmatrix} B & AB & A^2B & \cdots & A^{t-2}B & A^{t-1}B \end{pmatrix}$  is said to be the controllability matrix. By the *Cayley-Hamilton Theorem*, we can express each  $A^t$  for  $t \ge n$  as a linear combination of  $A^0$ , . . . , $A^{n-1}$ , hence  $rank(W_t) = rank(W_n)$ . Thus, the system is controllable if and only if  $rank(W_t) = n$ .

For a continuous time case, the idea is similar while the proof is slightly different, you may refer to (Klamka 2008), a sketch proof is that the dynamical system is controllable if and only if for certain time  $t=t_1$  the range of integral operator

 $\int_{0}^{t} e^{(t-s)A} Bu(s) ds = R^{n}$ . However, since  $\exp(t_{1}A)$  is nonsingular for any  $t_{1}$  if and only if  $\int_{0}^{t_{1}} e^{-sA} BB^{T} e^{-sA^{T}} ds$  is nonsingular. Taking into account Taylor series expansion of  $\exp(-sA)$  and *Cayley-Hamilton Theorem* we conclude that dynamical system is controllable if and only if  $rank(W_{t}) = n$ .

#### 3. Conclusion

In this paper, we focus on the minimal polynomials of matrices and revisit the existence and uniqueness of minimal polynomials. Eventually, we highlight a relatively efficient way to compute the minimal polynomial of matrices. Moreover, we conclude different interpretations to reduce the power of matrices, which is quite essential in computation of tendency of systems. And in the end, we give out an application of minimal polynomials about the controllability of systems. Also, there are many other extensions for future studies, for example, the minimal polynomial could be well-defined for Mn(R), where R is a commutative ring.

References

- Seneta, E. *Non-negative Matrices and Markov Chains*. New York: Springer. [2nd ed]. 2006.
- 2. Watkins, D. Fundamentals of Matrix Computations. New York: Wiley-Interscience. [2nd ed]. 2002.
- Pullman, N. Matrix Theory and Its Applications: Selected Topics. New York: M. Dekker. 1976.
- 4. Stewart, W. Introduction to Matrix. New York: Academic Press. 1973.
- Karampetakis, N. Tzekis, P. and Terzidis, H. On the Computation of the Minimal Polynomial of a Polynomial Matrix. Int. J. Appl. Math. Comput. Sci. Vol. 17, No. 4, pp463-470. 2007.
- Bialas, S. and Bialas, M. An Algorithm for the Calculation of the Minimal Polynomial. Vol. 56, No. 4. 2008.
- 7. Stanford. Controllability and Observability.
- 8. Klamka, J. *System Characteristics Stability, Controllability, Observability.* Institute of Automatic Control, Technical University, Gliwice, Poland.
- 9. Klamka, J. Controllability of Dynamical Systems. 2008.