1-2010

On the Eigenstructures of Functional K-Potent Matrices and Their Integral Forms

Yan Wu
Georgia Southern University

Daniel F. Linder
Georgia Southern University, dflinder@georgiasouthern.edu

On the Eigenstructures of Functional *K*-Potent Matrices and Their Integral Forms

Yan Wu[1] and Daniel F. Linder[2]
[1]Department of Mathematical Sciences
Georgia Southern University
Statesboro, GA 30460
yan@georgiasouthern.edu

[2]Department of Biostatistics
Medical College of Georgia
Augusta, GA 30901
USA

Abstract: - In this paper, a functional *k*-potent matrix satisfies the equation $A^k = \alpha I + \beta A^r$, where *k* and *r* are positive integers, α and β are real numbers. This class of matrices includes idempotent, Nilpotent, and involutary matrices, and more. It turns out that the matrices in this group are best distinguished by their associated eigen-structures. The spectral properties of the matrices are exploited to construct integral *k*-potent matrices, which have special roles in digital image encryption.

Key-Words: Nilpotent, Idempotent, Involutary, Unipotent, Skewed *k*-potent Matrix, Diagonalizability, Image Encryption

1 Introduction

Let $A \in C^{n\times n}$ be an *n* by *n* complex matrix and it is said to be idempotent if $A^2 = A$. This definition can be generalized to a higher power on *A*, if $A^k = A$ for some positive integer $k \geq 2$. With the same condition on *A*, if $A^k = 0$, a zero matrix, for some positive integer *k*, the matrix is called a nilpotent matrix. Another important class of matrices is called involutary, i.e. $A^2 = I$, the identity matrix. We define the unipotent matrix as a natural extension of the involutary matrix as follows: a matrix *A* is unipotent if it satisfies $A^k = I$, for some positive integer *k*. A skew-periodic matrix satisfies $A^k = -A$, while a skew unipotent matrix is defined as $A^k = -I$. All the above mentioned special matrices can be unified by a single equation:

$$A^k = \alpha I + \beta A, \qquad (1)$$

where $\alpha\beta = 0, \alpha, \beta \in \{-1, 0, 1\}$, and $k \geq 2$. A matrix *A* is said to be *k*-potent if it satisfies (1). Consequently, we introduce the class of *k*-potent matrices,

$$\Omega_{<\alpha,\beta>} = \left\{ A \,|\, A^k = \alpha I + \beta A,\ \alpha\beta = 0, \alpha, \beta \in \{-1, 0, 1\},\ k \geq 2 \right\} \qquad (2)$$

With (2), the relation between the subset of periodic matrices and unipotent matrices are readily seen, so are the skew-periodic and skew-unipotent matrices. It is not difficult to verify that $\Omega_{<1,0>} \subset \Omega_{<0,1>}$ and $\Omega_{<-1,0>} \subset \Omega_{<0,-1>}$. The results can be made stronger if we impose that the matrices in $\Omega_{<0,\pm 1>}$ be invertible. In that case, those subsets are identical, i.e. $\Omega_{<1,0>} = \Omega_{<0,1>}$ and $\Omega_{<-1,0>} = \Omega_{<0,-1>}$. Next, we introduce an index number for a matrix in $\Omega_{<\alpha,\beta>}$. It turns out that such an index number is closely related to the eigen-structure of the matrix. The index number of a *k*-potent matrix, $I_{<\alpha,\beta>}$, is defined as

$$I_{<\alpha,\beta>} = \min_{\substack{A^k = \alpha I + \beta A \\ k \geq 2}} k \qquad (3)$$

which is understood as the smallest positive integer that satisfies $A^k = \alpha I + \beta A$.

Some of the *k*-potent matrices, for instance, the nilpotent matrix, are mentioned occasionally in linear algebra textbooks, such as [1] and [2], in the context of

eigenvalue problems of a matrix. However, they are not studied in details in those books. It is also hard to find relevant discussions over such matrices, let alone the more generalized the *k*-potent matrices defined in (1), in those more research-oriented handbooks in matrix theory, such as [3], [4], and [5]. The eigen-structures of rational functions of tridiagonal matrices with closed form expressions were obtained in [6], where the tridiagonal matrix is raised to a positive integral power. Steinberg, *et. al.* [7] studied the solvability of differential algebraic equations with a nilpotent matrix as the descriptor. Bakasalary, *et. al.* published a series of papers [8-11] on the idempotency of linear combinations of idempotent and tripotent matrices. However, a thorough discussion on the eigen-structures of the various matrices of interest is missing from the literature. The purpose of this paper is to characterize these *k*-potent matrices via the canonical forms associated with the matrices. The result turns out to be useful for systematic construction of such matrices via a similarity transformation over the integer field. The proposed algorithm could be favored by instructors who teach linear algebra or numerical analysis at time they want to come up with their own special matrices for their examinations or projects. The results of this paper can be appealing to the cryptography community because *k*-potent matrices are useful in digital signal encryption, which will also be explored in this paper.

In the past decade or so, image encryption techniques were developed to keep up with the pace of the growth of internet and multimedia communications. There are hard encryption and soft encryption approaches. Most digital images are scrambled with soft encryption, which is also the choice of encryption as a component of the proposed UAS. Most image encryption methods can be classified as the DCT-based techniques, DWT-based (Discrete Wavelet Transform) techniques, transformations, and chaotic maps. Both DCT and DWT-based techniques are known as compression oriented schemes. The well-received MPEG encryption was first proposed by Tang [12] and is called "zig-zag permutation algorithm". The idea is to substitute the fixed zig-zag quantized DCT coefficient scan pattern by a random permutation list. A number of improvements on MPEG encryption were developed thereafter [13-14]. The DWT-based method, [15-16], takes advantage of the efficient image compression capability of wavelet networks through multi-resolution analysis integrated with block cipher data encryption. Some public key cryptographic systems uses Jacobian group of Cab curves, which is defined by a multi-variable polynomial function to perform the encoder and space time operations [17]. The chaos-based encryption of images employs the principle of applying chaotic maps with strong perplexing characteristics, such as non-periodic, non-convergent, randomness, and ergodic to the visual data. The most common nonlinear chaotic maps inherit properties as discrete cryptographic systems. Such systems are hybrids between permutation and substitution ciphers with specific properties. Scharinger [18] was the first to apply a class of nonlinear maps known as Kolmogorov flows for the digital encryption purpose. More papers on chaotic encryption followed, such as the chaotic key-based algorithms [19], chaotic systems for permutation transformation in images [20], and high-dimensional Arnold and Fibonacci-Q maps [21]. However, some chaotic cryptosystems have been identified susceptible to cryptanalysis due to the design disfigurement of their part-linear characters. Some attack algorithms have been developed in [22-23]. A common concern of the aforementioned encryption methods arises from the decryption site, where the data is unscrambled. In many occasions, the perfect decryption is impossible due to slight disparity of the encryption/decryption keys or simply roundoff errors in and out of the transformation domain. In many applications, such as medical, military operations, and satellite image processing [24], the quality of the images transmitted to the receiver station is crucial during the decision making process. Therefore, perfect reconstruction of the original image from the encrypted data is imperative when selecting various encryption methods, in addition to robustness to various attacks.

Images are stored in two-dimensional arrays, which make matrices the natural candidates for the kernels of encrypting operators. Moreover, matrix multiplication is analogous to convolution/deconvolution between filters and signals. The matrix kernel leaves signatures onto the image pixels and grey levels strictly over the integer field. There will be no roundoff errors in the decrypted images; hence, perfect reconstruction of the original image is achieved. The matrix considered in this paper is called *k*-potent integral matrix. It is a generalization of nilpotent, idempotent, and involutary matrices.

2 Eigen-structure of functional *k*-potent matrix and integral form

As discussed in the previous section, we are looking for integral matrices that satisfy (1). Some of these matrices can be adopted in image encryption as the encryption keys. One of the requirements for a robust cryptosystem is that the key space is infinite dimensional. Well, how many integral matrices are there that satisfy (1)? The answer is infinitely many. The following study will reveal a systematic approach for constructing such matrices, which turns out be

closely related to the eigen-structure of the *k*-potent matrix. We will go through the case studies of some well-known matrices, and, more importantly, extend the results to higher *k*-values as in (1).

We first investigate the spectral decomposition of nilpotent matrices. A square matrix A is such that $A^k = 0$, the zero matrix, for some positive integer k known as the index number of Nilpotency if the integer is the smallest positive integer so that $A^{k-1} \neq 0$. Nilpotent matrices are useful in the design of digital FIR filter banks with unequal filter length. The eigen-structure of a nilpotent matrix is revealed in what follows. Note that most of the proofs are omitted due to limited space.

Proposition 2.1 The eigenvalues of a nilpotent matrix are all zeros.

Proof: Let λ be an eigenvalue and v the corresponding eigenvector of a nilpotent matrix A satisfying $A^k = 0$, with $k \geq 2$. Then, $Av = \lambda v$, which yields $0 = A^k v = \lambda^k v$. Therefore, $\lambda = 0$.

Proposition 2.2 Suppose the square matrix A is a nonzero nilpotent matrix, then A is not diagonalizable.

Proof: Assume A is diagonalizable, then the spectral decomposition of the matrix is given by $A = P\Lambda P^{-1}$. According to proposition 2.1.1, $A = 0$, a zeros matrix, contradicting that A is a nonzero matrix.

Proposition 2.2 implies that the eigen-space associated with the zero eigenvalues is degenerate. Such a matrix has a generalized spectral decomposition with Jordan canonical forms. In other words, there are decoupled Jordan blocks in Λ. In order to further explore the eigen-structure of a nilpotent matrix, we introduce a special nilpotent matrix called nilpotent Jordan block.

Definition 2.1 The elements of a nilpotent Jordan block J satisfy $J_{ij} = 1$, if $j = i + 1$, and $J_{ij} = 0$, if $j \neq i + 1$.

The following proposition will be used to link the index number of nilpotency for a nilpotent matrix to the size of the largest nilpotent Jordan block associated with the matrix.

Proposition 2.3 Let J_m be an m by m nilpotent Jordan block, and let $J_{ij}^{\langle k \rangle}$ be an element of the matrix J_m^k, $k = 2,3,...$, then,

$$J_{ij}^{\langle k \rangle} = \begin{cases} 1 & \text{if } j = i + k \\ 0 & \text{otherwise} \end{cases} \quad i, j = 1,2,...,m, \ \ k = 2,3,... \qquad (4)$$

Proof: Use mathematical induction. For the case $k = 2$, from the matrix product formula,

$$J_{ij}^{\langle 2 \rangle} = \sum_{s=1}^{m} J_{is}^{\langle 1 \rangle} J_{sj}^{\langle 1 \rangle} = \sum_{s=1}^{m} J_{is} J_{sj} = J_{i\,i+1} J_{i+1\,i+2} = 1$$

which implies that $J_{ij}^{\langle 2 \rangle} = \begin{cases} 1 & \text{if } j = i + 2 \\ 0 & \text{otherwise} \end{cases}$, satisfying (4).

Now, assume (4), we obtain $J_{ij}^{\langle k+1 \rangle}$,

$$J_{ij}^{\langle k+1 \rangle} = \sum_{s=1}^{m} J_{is}^{\langle k \rangle} J_{sj}^{\langle 1 \rangle} = \sum_{s=1}^{m} J_{is}^{\langle k \rangle} J_{sj} = J_{i\,i+k}^{\langle k \rangle} J_{i+k\,i+k+1} = 1$$

which establishes $J_{ij}^{\langle k+1 \rangle} = \begin{cases} 1 & \text{if } j = i + k + 1 \\ 0 & \text{otherwise} \end{cases}$. Therefore, formula (4) for an element of the matrix J_m^k is valid.

Proposition 2.3 reveals that the 1s' on the off-diagonal of a nilpotent Jordan block J_m are pushed over to the upper right corner as the power k increases. Consequently, it is easy to verify that J_m^k becomes a zero matrix if k is greater than or equal to the size of the matrix J_m, i.e. $J_m^k = 0$ (zero matrix) if $k \geq m$.

Introduce the Jordan canonical form Λ with nilpotent Jordan blocks along its main diagonal, and the off-diagonal blocks are zero matrices, i.e.

$$\Lambda = \begin{bmatrix} J_{m_1} & & & & & \\ & J_{m_2} & & \mathrm{O} & & \\ & & \ddots & & & \\ & \mathrm{O} & & J_{m_p} & & \\ & & & & \ddots & \\ & & & & & J_{m_n} \end{bmatrix} \qquad (5)$$

where the dimension of the Jordan block J_{m_i} is m_i by m_i, $i = 1,2,...,n$. We have the following result.

Proposition 2.4 Let Λ be the Jordan Canonical form (5) with nilpotent Jordan blocks along its main diagonal. If $m_p = \max\{m_1, m_2, ..., m_n\}$, then $\Lambda^{m_p - 1} \neq 0$ and $\Lambda^{m_p} = 0$.

Proof: It is easy to verify that

$$\Lambda^q = \begin{bmatrix} J_{m_1}^q & & & & & \\ & J_{m_2}^q & & & & \\ & & \ddots & & & \\ & & & J_{m_p}^q & & \\ & & & & \ddots & \\ & & & & & J_{m_n}^q \end{bmatrix} \quad (6)$$

Therefore, according to Proposition 2.3, the block matrix $J_{m_p}^{m_p-1}$ in Λ^{m_p-1} is a nonzero matrix because one element in $J_{m_p}^{m_p-1}$ is nonzero, i.e. $\left(J_{m_p}^{m_p-1}\right)_{1,m_p} = 1$. On the other hand, let $q = m_p$, from Proposition 2.3, each block matrix on the main diagonal of Λ^{m_p} is a zero matrix because the power m_p either exceeds or equals the size of any block matrix J_{m_i} because $m_p = \max\{m_1, m_2, ..., m_n\}$. Hence, $\Lambda^{m_p} = 0$.

Proposition 2.4 implies that the Jordan matrix Λ is a nilpotent matrix, and the index number of the Nilpotency for Λ equals the dimension of the largest nilpotent Jordan block in Λ.

The following result links the index number of a nilpotent matrix to the size of the largest nilpotent Jordan block associated with the matrix, which also plays an important role in the symbolic construction of nilpotent matrices to be discussed later.

Proposition 2.5 The index number of a nilpotent matrix equals the size of the largest nilpotent Jordan block associated with the matrix.

Proof: Let A be a nilpotent matrix. Then, there exists a nonsingular matrix P such that a Jordan decomposition of the matrix exists, i.e. $A = P\Lambda P^{-1}$, where Λ is given by (5). From $A^k = (P\Lambda P^{-1})^k = P\Lambda^k P^{-1}$, one can see that $A^k = 0$ if and only if $\Lambda^k = 0$. According to Proposition 2.4, the smallest positive integer k satisfying $\Lambda^k = 0$ equals the size of the largest nilpotent Jordan block in Λ. Therefore, the index number of a nilpotent matrix, $I_{<0,0>}$, equals the size of the largest nilpotent Jordan block associated with the matrix.

Our next group of matrices is in the category of periodic matrices. A square matrix A such that $A^k = A$ for k to be a positive integer is called a periodic matrix. If k is the least such integer, then the matrix is said to have period k-1. The well-known idempotent matrix i.e. $A^2 = A$, is obviously a special case of the periodic matrix to be studied here. Periodic matrices are useful in digital signal encryption such as image coding. We begin with exploring the spectral properties of a periodic matrix.

Proposition 2.6 Let A be a periodic matrix with index number k and let λ be an eigenvalue of A, then $\lambda \in \{0\} \cup \left\{e^{i2m\pi/(k-1)}, m = 0,1,...,k-2\right\}$.

Proof: Let λ and v be the eigenvalue and corresponding eigenvector of A respectively. From $Av = \lambda v$, one has $A^k v = \lambda A^{k-1} v = \lambda^k v$. Hence, $\lambda v = \lambda^k v$, which implies $\lambda^k - \lambda = 0$. The solution set of this equation is $\{0,1\} \cup \left\{e^{i2m\pi/(k-1)}\right\}_{m=1}^{k-2}$.

Proposition 2.6 tells us that the eigenvalues of a periodic matrix are distributed around the unit circle or possibly at the origin. The next proposition addresses the diagonalizability of periodic matrices.

Proposition 2.7 Periodic matrices are diagonalizable.

Proof: Let A be a periodic matrix. Assume A is not diagonalizable. Then, the matrix has a Jordan decomposition $A = P\Lambda P^{-1}$, where Λ is similar to (5). Since A is not diagonalizable, there exists a Jordan block in (5) such that it has the following form:

$$J_{m_s} = \begin{bmatrix} \lambda_s & 1 & 0 & \dots & 0 \\ & \lambda_s & 1 & \dots & 0 \\ & & \ddots & \ddots & \\ & & & \lambda_s & 1 \\ & & & & \lambda_s \end{bmatrix} \quad (7)$$

As discussed earlier, $A^k = P\Lambda^k P^{-1}$, where Λ^k has a similar expression to (6). We will show that $J_{m_s}^k \neq J_{m_s}$, which leads to the contradiction to A being periodic. To this end, we rewrite $J_{m_s} = \Lambda_s + N_s$, where Λ_s is a diagonal matrix with λ_s on the main diagonal, and N_s is a nilpotent Jordan block (see definition 2.1). Use binomial expansion to obtain the following

$$J_{m_s}^k = \left(\Lambda_s + N_s\right)^k = \sum_{n=0}^{k} C_k^n \Lambda_s^{k-n} N_s^n = \sum_{n=0}^{\min\{k,m_s\}} C_k^n \Lambda_s^{k-n} N_s^n \tag{8}$$

$$= \begin{bmatrix} \lambda_s^k & C_k^1\lambda_s^{k-1} & C_k^2\lambda_s^{k-2} & \cdots & C_k^{m_s-1}\lambda_s^{k-m_s+1} \\ & \lambda_s^k & C_k^1\lambda_s^{k-1} & C_k^2\lambda_s^{k-2}\cdots & C_k^{m_s-2}\lambda_s^{k-m_s+2} \\ & & \ddots & & \\ & & & \ddots & C_k^2\lambda_s^{k-2} \\ & & & & \lambda_s^k \end{bmatrix}$$

In deriving (8), we used Proposition 2.3. It is easy to see that $J_{m_s}^k \neq J_{m_s}$ from (8). Hence, a periodic matrix must be diagonalizable.

Unlike nilpotent matrices, the eigen-space of a periodic matrix is non-degenerate. A periodic matrix is similar to a diagonal matrix via a similarity transformation. This result is useful for numerical formation of periodic matrices.

The index number of a periodic matrix obviously relates to the periodicity of the matrix as seen from the definition of a periodic matrix. We would like to point it out that the eigenvalue (except zero) of a periodic matrix with period ν must satisfy the following equation:

$$\lambda^{\nu} - 1 = 0. \tag{9}$$

Condition (9) gives another criterion for identifying a periodic matrix with certain periodicity.

In what follows we look into the case of unipotent matrices. A unipotent matrix extends the involutary matrix to a higher-order power matrix. To be exact, a unipotent matrix satisfies $A^k = I, k \geq 2$. It is easily seen from the definitions that a unipotent matrix must also be a periodic matrix, but not the other way around unless the periodic matrix is also invertible. Again, we are interested in exploring the spectral properties of unipotent matrices.

Proposition 2.8 Let A be a unipotent matrix with index number k and let λ be an eigenvalue of A, then $\lambda \in \left\{e^{i2m\pi/k}, m = 0,1,2,...,k-1\right\}$

Proof: Let λ and v be the eigenvalue and corresponding eigenvector of A respectively. From $Av = \lambda v$, one has $A^k v = \lambda^k v$. Hence, $v = \lambda^k v$, which implies $\lambda^k = 1$. The solution set of this equation is $\{1\} \cup \left\{e^{i2m\pi/k}\right\}_{m=1}^{k-1}$.

Proposition 2.8 further reveals the connection between a unipotent matrix and a periodic matrix from the circular distribution of their eigenvalues.

Proposition 2.9 Unipotent matrices are diagonalizable

The proof of this proposition is almost identical to the proof of Proposition 2.7 due to the comparable structure between these two matrices. Similar to (9), the eigenvalue of a unipotent matrix with index number k must satisfy the following equation:

$$\lambda^k - 1 = 0. \tag{10}$$

Since the treatment for the skewed k-potent matrix is exactly the same as that for the previously discussed k-potent matrices, we summarize the results as follows on the skewed k-potent matrix.

A skew-periodic matrix A satisfies the constraint with index $k \geq 2$, $A^k = -A$. We have the following results for the spectral properties of skew-periodic matrices.

Proposition 2.10 Let A be a skew-periodic matrix with index number k and let λ be an eigenvalue of A, then $\lambda \in \{0\} \cup \left\{e^{i(2m+1)\pi/(k-1)}, m = 0,1,...,k-2\right\}$.

The eigenvalues (except zero) of a skew-periodic matrix are solutions of the following equation

$$\lambda^{k-1} + 1 = 0. \tag{11}$$

Proposition 2.11 Skew-periodic matrices are diagonalizable.

A skew-unipotent matrix A satisfies the constraint $A^k = -I$. We have the following results for the spectral properties of skew-unipotent matrices.

Proposition 2.12 Let A be a skew-unipotent matrix with index number k and let λ be an eigenvalue of A, then $\lambda \in \left\{e^{i(2m+1)\pi/k}\right\}_{m=0}^{k-1}$.

The eigenvalues of a skew-unipotent matrix with index number k satisfy the following equation:

$$\lambda^k + 1 = 0. \tag{12}$$

Proposition 2.13 Skew-unipotent matrices are diagonalizable.

Finally, we examine the spectral properties of the functional *k*-potent matrix as follows,

$$A^k = \alpha I + \beta A^r,\ \alpha\beta \neq 0,\ k > r \geq 1 \qquad (13)$$

It can be verified that the eigenvalues of a functional *k*-potent matrix (13) are solutions of the following equation

$$\lambda^k - \beta\lambda^r - \alpha = 0 \qquad (14)$$

Since $\alpha \neq 0$, all the eigenvalues are nonzero. Therefore, the matrix is nonsingular.

Proposition 2.14 Functional *k*-potent matrices (13) are diagonalizable.

Proof: Assume the matrix is not diagonalizable. With the spectral decomposition of A, $A = P\Lambda P^{-1}$, where Λ is given by (5). The Jordan block in Λ is given by (7). Therefore, this Jordan block must satisfy (13). Given that $\lambda_s \neq 0$ because the eigenvalues are nonzero. One has, according to (8),

$$J_{m_s}^k = \left(\Lambda_s + N_s\right)^k = \sum_{n=0}^{k} C_k^n \Lambda_s^{k-n} N_s^n = \sum_{n=0}^{\min\{k,m_s\}} C_k^n \Lambda_s^{k-n} N_s^n$$

$$= \begin{bmatrix} \lambda_s^k & C_k^1\lambda_s^{k-1} & C_k^2\lambda_s^{k-2} & \cdots & C_k^{m_s-1}\lambda_s^{k-m_s+1} \\ & \lambda_s^k & C_k^1\lambda_s^{k-1} & C_k^2\lambda_s^{k-2}\cdots & C_k^{m_s-2}\lambda_s^{k-m_s+2} \\ & & \ddots & & \\ & & & \ddots & C_k^2\lambda_s^{k-2} \\ & & & & \lambda_s^k \end{bmatrix}$$

and

$$\alpha I + \beta A^r = \alpha I + \beta\left(\Lambda_s + N_s\right)^r = \alpha I + \beta\sum_{n=0}^{r} C_r^n \Lambda_s^{r-n} N_s^n$$

$$= \alpha I + \beta \sum_{n=0}^{\min\{r,m_s\}} C_r^n \Lambda_s^{r-n} N_s^n$$

$$= \begin{bmatrix} \alpha+\beta\lambda_s^r & C_r^1\beta\lambda_s^{r-1} & C_r^2\beta\lambda_s^{r-2} & \cdots & C_r^{m_s-1}\beta\lambda_s^{r-m_s+1} \\ & \alpha+\beta\lambda_s^r & C_r^1\beta\lambda_s^{r-1} & C_r^2\beta\lambda_s^{r-2}\cdots & C_r^{m_s-2}\beta\lambda_s^{r-m_s+2} \\ & & \ddots & & \\ & & & \ddots & C_r^2\beta\lambda_s^{r-2} \\ & & & & \alpha+\beta\lambda_s^k \end{bmatrix}$$

Comparing the two matrices, the off-diagonal entries are mismatched because $k > r$. Therefore, the functional *k*-potent matrices (13) are diagonalizable.

In summary, we categorize four groups of *k*-potent matrices: (i) nilpotent matrices, (ii) periodic and unipotent matrices, (iii) skew-periodic and skew-unipotent matrices, and (iv) the functional *k*-potent matrices. The classification is based on the characteristics of the eigenvalue/eigen-space of the matrices. The results presented above will be used to manufacture such matrices symbolically, i.e. all *k*-potent matrices are constructed over the integer field.

Our objective in this work is to develop an algorithm for constructing integral *k*-potent matrices. In particular, (skew-) periodic and (skew-) unipotent matrices are useful in digital signal encryption. Instructors who teach Linear Algebra and Numerical Analysis may find the proposed algorithm useful as they may want to come up with a number of such *k*-potent matrices for students to practice with the related concepts in matrix theory.

The idea is simple. A power-induced matrix can be easily constructed via the spectral decomposition formula, i.e.

$$A = P\Lambda P^{-1} \qquad (15)$$

where P is an invertible matrix and Λ is either a diagonal matrix or a block diagonal matrix in Jordan form. It is easy to see that, as long as Λ is *k*-potent, the matrix A is *k*-potent of the same type. In what follows, we introduce different ways for constructing the Λ-matrix so that it is a power-induced matrix satisfying a predetermined index number.

Case (i): Nilpotent matrices

According to Proposition 2.4, the Λ-matrix in (15) is guaranteed nilpotent with certain index number if Λ consists of nilpotent Jordan blocks, and the size of the largest nilpotent Jordan block equals the index number. The following matrix, for example, is a nilpotent matrix with index 4, i.e. $\Lambda^4 = 0$.

$$\Lambda = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \qquad (16)$$

Case (ii): Periodic matrices

Proposition 2.7 and equation (9) are the keys for constructing periodic Λ-matrix. For the sake of argument, let ν be the period of Λ and let

$\Gamma_\nu = \{0\} \cup \left\{ e^{i2m\pi/\nu}, m = 0,1,...,\nu-1 \right\}$ be the set of eigenvalues of the periodic matrix. It is sufficient that

$$\Lambda = \text{diag}(\lambda_1, \lambda_2, ..., \lambda_s), \tag{17}$$

where $\lambda_i \in \Gamma_\nu$, $i = 1,2,...,s,$ which guarantees that the Λ-matrix (12) is a periodic matrix with period ν. The Λ-matrix can also be written as a block diagonal matrix as follows

$$\Lambda = \text{diag}(B_1, B_2, ..., B_m) \tag{18}$$

as long as the eigenvalues of each block B_i, $i = 1,2,...,m,$ belong to Γ_ν. This setting gives us some flexibility for constructing periodic matrices. One can also mix the eigenvalues of the Λ-matrix in (17) or (18) to construct periodic matrices with a higher index number. To this end, let the eigenvalues of Λ be chosen from the following set

$$\Gamma = \Gamma_{\nu_1} \cup \Gamma_{\nu_2} \cup ... \cup \Gamma_{\nu_t}, \tag{19}$$

and let

$$\nu^* = \text{LCM}(\nu_1, \nu_2, ..., \nu_t), \tag{20}$$

where LCM stands for least common multiple, then, it can be verified that the period of Λ is ν^*. For example, the following matrix is a periodic matrix with period 12,

$$\Lambda = \begin{bmatrix} 1 & 3 & 0 & 0 \\ -1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \tag{21}$$

because the eigenvalues of the first block are $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, which are solutions of (9) with $\nu = 3$, and the eigenvalues of the second block in (21) are solutions of (9) with $\nu = 4$.

The treatment for constructing the other Λ-matrices, i.e. unipotent, skew-periodic, and skew-unipotent matrices, is essentially the same as that for periodic matrices because the eigen-structures among those matrices are similar. When constructing such matrices, one should realize that the equations (9), (10), and (11) must be satisfied for the corresponding matrices.

For mathematics instructors, it is preferred to work with integral matrices, i.e. the elements of a matrix are all integers, mainly because the arithmetic is symbolic as far as additions and multiplications are concerned, which also implies that there are no roundoff errors. We are able to achieve this when constructing the Λ-matrix, see (21), for instance.

Instead of constructing the Λ-matrix, one can take advantage of the companion matrix for the characteristic polynomial [3]. In general, the companion matrix of an nth degree characteristic polynomial

$$P(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + ... + a_1\lambda + a_0$$

is given by

$$\Lambda_p = \begin{bmatrix} 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & ... & 0 & -a_1 \\ 0 & 1 & ... & 0 & -a_2 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix} \tag{22}$$

The characteristic polynomials of various kinds of k-potent matrices are given by equations (9)-(12) and (14). Formula (15) can be used if one wants to construct a dense integral *k*-potent matrix, where both P and P^{-1} in (15) have to be integral matrices. In what follows, let $Z^{n\times n}$ represent the set of *n* by *n* integral matrices. The following proposition gives the necessary and sufficient condition for $A^{-1} \in Z^{n\times n}$ if $A \in Z^{n\times n}$.

Proposition 2.15 Suppose $A \in Z^{n\times n}$ and A is a nonsingular matrix, then $A^{-1} \in Z^{n\times n}$ if and only if $\det(A) = \pm 1$.

Proposition 2.15 gives us a guideline for constructing such an integral *P*-matrix. We can simply use the following formula for *P*,

$$P = UL, \tag{23}$$

where U is an upper triangular integral matrix with 1's on the main diagonal and L is a lower triangular integral matrix with 1's on the main diagonal. It is obvious that $|P| = 1$, according to Proposition 2.15, P^{-1} is an integral matrix. With an integral *P*-matrix from (23), we obtain a dense integral nilpotent matrix calculate from (16),

$$A=\begin{bmatrix} 22 & 44 & 114 & 183 & 2 & -317 \\ -13 & -26 & -68 & -110 & -4 & 188 \\ 20 & 40 & 104 & 167 & 2 & -289 \\ 9 & 18 & 48 & 77 & 3 & -133 \\ -14 & -28 & -74 & -118 & -2 & 206 \\ 12 & 24 & 63 & 101 & 2 & -175 \end{bmatrix}$$

.

It is verified in MatLab that $A^4=0,$ which has the same index of nilpotency as that of (11). A more sophisticated algorithm for constructing integral similarity transformation matrices can be found in [25].

We also constructed an integral periodic matrix from (21) as follows

$$A=\begin{bmatrix} -8 & -1 & 2 & 4 \\ 22 & 4 & -5 & -12 \\ -42 & -8 & 9 & 21 \\ 11 & 3 & -2 & -6 \end{bmatrix}.$$

It is hard to tell that the matrix above is a periodic matrix with period 12 unless one literally calculates the power matrix A^{13} without peeking at the eigenvalues of A.

For more general k-potent matrices, the eigenvalues are usually non-integers. However, it is always feasible to make use of the companion matrix (22) for the characteristic polynomials of the k-potent matrices, such as (9)-(12) and (14), combined with the integral similarity transformation matrix P in (23). The following matrix satisfies matrix equation $A^4=3I-A^2$,

$$A=\begin{bmatrix} -9 & -16 & -7 & 24 \\ 7 & 12 & 6 & -17 \\ -2 & -3 & -1 & 5 \\ 1 & 2 & 2 & -2 \end{bmatrix}.$$

3 Applications to image encryption

An image is formed from MN samples arranged in a two-dimensional array of M rows and N columns such as a photo, an image formed of the temperature of a integrated circuit, x-ray emission from a distant galaxy, a satellite map from Google Earth.

In imaging terminology, each sample of the image is called a pixel. Each pixel is attributed a value called grayscale ranging from 0 to 255, where 0 is black, 255 is white, and the intermediate values are shades of gray. For the purpose of image encryption, we apply a series of encryption key matrices to mask an image via matrix multiplications. This will alter the gray level of each pixel so that the original image is no longer recognizable. This masking process is in essence a filtering process because each row (column) in the encryption key matrix is treated as a digital filter with finite impulse response. Due to the randomness and magnitude of the filter coefficients, the original image is transformed into a rather different image by way of a filter banks.

We adopt the previously studied k-potent matrices for the encryption key matrix, particularly the unipotent or periodic matrices. The nilpotent matrix can also be used for image encryption with some special treatment such as diagonal perturbation, but we will not elaborate here.

The cryptosystem proposed in this paper consists of associate keys and primary keys. The function of the associate key T_1 is to divide the original image into sub-images, not necessarily the same sizes, followed by another associate key T_2 to permute the pixels of the sub-image for pre-scrambling. The permutation key is nothing but a product of elementary matrices. The mathematical setting is given as following for the pre-encryption stage:

$$\begin{aligned} &T_{1i}: Z^{M\times N}\to Z^{m_i\times n_i},\ m_i<M,\ n_i<N,\ i=1,2,...,k \\ &\sum m_i=M,\ \sum n_i=N. \end{aligned} \tag{24}$$

$$\begin{aligned} &T_{2i}: Z^{m_i\times n_i}\to Z^{m_i\times n_i},\ i=1,2,...,k. \\ &T_{2i}=E_{i1}E_{i2}\cdots E_{is} \end{aligned} \tag{25}$$

where E_{ij} is an elementary matrix that exchange the rows of a matrix if left-multiplied or columns of the matrix if right-multiplied.

The primary key can be formulated via a product of unipotent and/or skew-unipotent matrices as follows

$$T_M=A_1^{k_1}A_2^{k_2}\cdots A_t^{k_t} \tag{26}$$

Let X_i be a sub-image from (24) to be scrambled, with matching dimensions to assure multiplicability between T_M and X_i , the encrypted image is obtained as $Y_i=T_MX_i$. The decryption key is given by

$$T_M^{-1}=(-1)^p A_t^{n_t-k_t}A_{t-1}^{n_{t-1}-k_{t-1}}\cdots A_1^{n_1-k_1} \tag{27}$$

where n_i is such that $A_i^{n_i}=\pm I, i=1,2,...,t$ and p represents the number of skew-unipotent matrices applied in (26). With (27), the original image is recovered from Y_i via $X_i=T_M^{-1}Y_i$. It is also ready to be seen that the decryption process only involves matrix

multiplication with additions and multiplications between integers. Therefore, lossless image encryption/decryption is guaranteed, see Fig. 1 for an example. The encryption key consists of three 5 by 5 unipotent matrices.

Interestingly enough, functional *k*-potent matrix can add more complexity to the encryption scheme, proposed as follows. Consider the functional *k*-potent matrix, which is also an extension of (13),

$$A^k = I + \sum_{i=1}^{m} \beta_i A^i \tag{28}$$

where $0 < m < k$. Let X be a sub-image as a result of the pre-encryption stage (24) and (25). Let Y be the scrambled image encrypted by the functional *k*-potent matrix (28), i.e. $Y = AX$. Now, the decryption process is carried out as follows:

Step 1. Pre-multiply Y by A^{i-1}, respectively, to get $Z_i = A^i X$, $i = 1,2,...,m$, with $A^0 = I$.

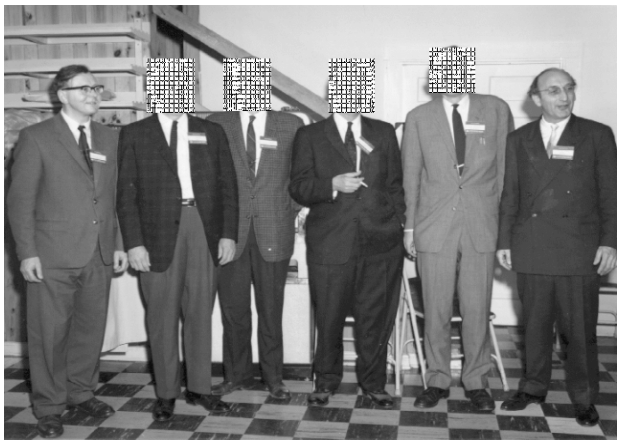
Step 2. Pre-multiply Z_m by A^{k-m} to get $W = A^k X$.

Step 3. $X = W - \sum_{i=1}^{m} \beta_i Z_i$ due to (28).

Another image encryption with the above proposed method is shown in Fig.2.

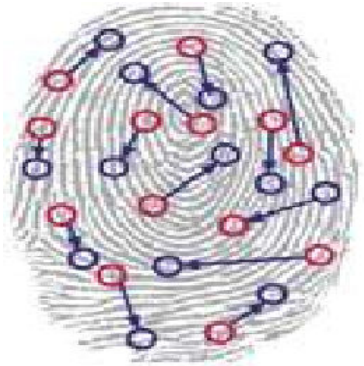
In this paper, we studied the eigen-spaces of various *k*-potent matrices, including Nilpotent, periodic, involutary, and skew-periodic matrices. Extensions are made to more general functional *k*-potent matrices. An immediate application of the results is seen in digital image encryption. The methodology proposed in this paper can also be extended to other functional matrices satisfying special constraints, similar to the ones for the *k*-potent matrices, and such constraints have imprints on the eigen-space structures of the matrices.

(a)

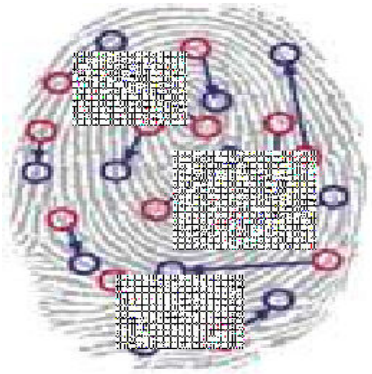


(b)

Figure 1. (a) original picture of mathematicians; (b) encrypted image of selected faces (courtesy of MatLab image processing toolbox)



(a)



(b)

Figure 2. (a) original fingerprint image; (b) scrambled image of selected areas of the fingerprint (courtesy of MatLab image processing toolbox)

References:

[1] S. H. Friedberg, A. J. Insel, L.E. Spence, *Linear Algebra*, 4th Ed., Prentice Hall, Upper Saddle River, NJ, 2002.

[2] G. Strang, *Introduction to Linear Algebra*, 3rd Ed., Wellesley-Cambridge Press, MA, 2003.

[3] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 2nd Ed., The Johns Hopkins University Press, Baltimore, Maryland, 1989.

[4] G. W. Stewart, *Matrix Algorithms, Volume II: Eigensystems*, SIAM, Philadelphia, PA, 2001.

[5] J. H. Wilkinson, *The Algebraic Eigenvalue Problem*, Oxford Science Publications, NY, 1965.

[6] J. Rimas, Computing of Positive Integer Powers for a Special Kind of Matrices, *WSEAS Trans. Math.*, v. 6, no.2, 289-295, 2007.

[7] S. L. Steinberg, J. P. Zingano, and P. R. Zingano, On nilpotent singular systems, *J. Comput. Appl. Math*. 137, 97-107, 2001.

[8] J. K. Baksalary and O. M. Baksalary, Idempotency of linear combinations of two idempotent matrices, *Linear Algebra Appl.* 321, 3-7, 2000.

[9] J. K. Baksalary, O. M. Baksalary, and G. P. H. Styan, Idempotency of linear combinations of an idempotent matrix and a tripotent matrix, *Linear Algebra Appl*. 354, 21-34, 2002.

[10] O. M. Baksalary, Idempotency of linear combinations of three idempotent matrices, two of which are disjoint, *Linear Algebra Appl*. 388, 67-78, 2004.

[11] J. K. Baksalary, O. M. Baksalary, and H. Özdemir, A note on linear combinations of commuting tripotent matrices, *Linear Algebra Appl*. 388, 45-51, 2004.

[12] L. Tang, Methods for encrypting and decrypting MPEG video data efficiently, Proc. ACM Multimedia, 219-229, 1996.

[13] S. U. Shin, K.S. Kim, and K. H. Rhee, A secrete scheme for MPEG video data using the joint of compression and encryption, Proc. Inform. Security Workshop (ISW '99), v. 1729 (*lecture notes on computer science*), 191-201, 1999.

[14] Wenjun Zeng and Shawmin Lei, Efficient frequency domain selective scrambling of digital video, *IEEE Trans. Multimedia*, v. 5, no.1, 118-129, 2003.

[15] P. P. Dang and P. M. Chau, Image encryption for secure internet multimedia applications, *IEEE Trans. Consum. Electron*., v. 46, no.3, 395-403, 2000.

[16] R. P. Elias, O. V. Villegas, M. L. Sanchez, and V. G. C. Sanchez, Automatic Inspection Using Edge Preserving Wavelet Lossy Image Coding by Means of Modified SPIHT, *WSEAS Trans. Signal Process*., v. 2, no. 11, 1515-1522, 2006.

[17] B. Ontiveros, I. Soto, and R. Carrasco, A New Cryptography Algorithm Using Cab Curves and LDPC for Wireless Communication Systems, *WSEAS Trans. Math.*, v. 6, no.2, 422-424, 2007.

[18] J. Scharinger, Fast encryption of image data using chaotic Kolmogorov flows, *Journal of Electron. Imaging*, v. 7, no. 2, 318-325, 1998.

[19] J.C. Yen and J. I. Guo, A new chaotic key-based design for image encryption and decryption, Proc. IEEE Int. Conference Circuits and Systems, v.4, 49-52, 2000.

[20] H. Zhang, X. F. Wang, Z. H. Li, D. H. Liu, and Y. C. Lin, A new image encryption algorithm based on chaos system, Proc. IEEE Intern. Conference Robotics, IS and Signal Process, 778-782, 2003.

[21] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Int. Journal Bifurcation & Chaos*, v. 8, no.6, 1259-1284, 1998.

[22] G. Jakimoski and L. Kocarev, Analysis of some recently proposed chaos-based encryption algorithms, *Physics Letters A*, v. 291, no. 6, 381-384, 2001.

[23] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision, *Computer Physics Communications*, v. 153, no. 1, 52-58, 2003.

[24] A. Kulkarni and S. Mccaslin, Knowledge Discovery from Satellite Images, *WSEAS Trans. Signal Process*., v. 2, no. 11, 1523-1530, 2006.

[25] Y. Wu and A. C. Vosler, An Anti-Symmetric Key Algorithm for Signal Encryption, Proceedings of the WSEAS Inter. Conf. on Signal Process., pp 140-145, 2007.