

Some explorations of linear algebra

Heng Wang^{1, *, †} and Changheng Zhao^{2, †}

¹ Beijing No.80 High School, Beijing 100102, China

² Beijing No.57 High School, Beijing 100045, China

* Corresponding email: tbufkin@une.edu

[†]These authors contributed equally to this work

Abstract. It is a fundamental problem in quantum information whether a particular quantum state of a composite system is entangled. It has enormous potential in quantum error correction, quantum cryptography, and quantum teleportation applications. This problem can be transferred in the form of a mathematical conjecture in language of linear algebra. In this paper, the authors explain the important applications, convenience, efficiency of using linear algebra in math physics, and computer science. The authors give some examples of linear algebra used in various areas, including datum coordinate system finding a location, encryption and decryption algorithm, storage of images, classical mechanics, and quantum physics. The authors list the definition of the matrix, real matrix, complex matrix, diagonal matrix, identity matrix, scalar matrix, trace, rank, and determinants of matrices. The authors explored Laplace expansion, transpose, inverse, conjugate of a matrix and addition, multiplication between matrices and between a scalar and a matrix, Kronecker product and their properties of matrices, the definitions and solving method of eigenvalue and eigenvector, and the diagonalisation and its conditions of matrices. The authors introduce the applications of matrix transformations and operations in programs. The authors explain two encryption and decryption algorithms based on linear algebra and their strengths and weaknesses.

Keywords: linear algebra, matrix, tensor product, determinant.

1. Introduction

Linear algebra is a mathematical discipline. It has a wide range of applications: linear transformations, vectors, vector spaces, and finite-dimensional systems of linear equations are among its research objectives. Linear algebra is widely employed in the social and natural sciences because nonlinear models in scientific study may often be represented as linear models.

Linear algebra has many vital applications in math, physics, and technical disciplines, so it plays a very important role in all branches of science and engineering [1-10]. In today's era of widely used computers, such as computer-aided design, virtual reality, computer graphics, cryptography, and other technologies, linear algebra is used as part of its theoretical and algorithmic foundations [1-10]. The link between geometric concepts and algebraic methods, as expressed in linear algebra, axiomatic methods abstracted from concrete conceptions, precise logical deduction, intelligent induction, and synthesis, is tremendously advantageous for improving people's mathematical training and attaining scientific intelligence. Second, convenience: linear algebra is an operating system found in linear norm space. This space is in its nature convenient for thinking and observing problems, and thus for finding a whole set of measurements, analyses, computational structures, and so on. With these, the actual problems in reality can be more easily translated into this abstract space, and these existing tools can be used directly to analyse and solve the problem

Third, high efficiency: if some complex problems meet some specific conditions, then they can be transformed into simple linear problems, and the advantage of linear problems is that they can be described mathematically, so it is easier to fully understand complex problems.

For example, if a man goes to a city and that is at an intersection, he sees what kind of building are around him, and then open his map, and find the intersection and the corresponding location. He calibrates the direction he is facing now. The map comes with a coordinate system of upper and lower north, south, left, right, and east. He also has a coordinate system of front and back left and right in

front of him, and the relationship between these two coordinate systems can be described by linear transformations. This way, any point on the map, such as a building southeast of an intersection, can correspond to a point in his coordinate system (such as a building in the right-hand direction in front of you). All of these operations can be reacted to by matrix after he have specified a datum coordinate system. Thus, the correspondence of all points becomes a matrix that goes left by multiplying (acting) one point (a coordinate vector of a location in the map coordinate system) and then getting another point (a coordinate vector with the same location in his coordinate system)

Pictures cannot be stored in computers directly. Thus a way that can convert pictures in to numbers is required, in order to communicate the image to computers. The image can be divided in to many colored squares called pixel. Given enough pixels and our brains regard it as an image, instead of colored squares.

For example, in a grayscale photo, a number is used to represent the shade of grey of a pixel, from 0 to 255, where 0 is totally black and 255 is totally white. If the image has a resolution of $m \times n$, then it can be expressed as an $m \times n$ matrix. Each entry of the matrix is a number from 0 to 255 which shows the intensity of the gray color of the pixel. A colored photograph can be stored with RGB scale. The R, G, and B stand for color red, green and blue respectively, for the human eye recognizes color with combinations of red, green, and blue. So a colored image stored in computers with three matrices, each expresses the intensity of a certain color.

Thinking a traveling particle in space, its velocity and displacement can be described by vectors in the form $\begin{bmatrix} a \\ b \\ c \end{bmatrix}$, which represents the sum of its velocity or displacement in three orthogonal directions. In this way it's simplified to vectors in three irrelevant directions.

In structural mechanics, matrix analysis of structure has matrix as representation, classical structure mechanics as basic theory, and computers as computational methods.

A bridge, for example, contains loads that must be computed at different places. To express the direction and amount of the force at these sites, vectors are necessary.

Maxwell's equations cope with three-dimensional vector fields that change over time.

For differential equations

$$\begin{cases} \frac{du_1}{dt} = -u_1 + 2u_2 \\ \frac{du_2}{dt} = u_1 - 2u_2 \end{cases} \quad (1)$$

A matrix form can be constructed.

$$\frac{du_1}{dt} = Au \quad (2)$$

Which is

$$\begin{bmatrix} \frac{du_1}{dt} \\ \frac{du_2}{dt} \end{bmatrix} = \begin{bmatrix} -1 & 2 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad (3)$$

And A represents the coupling relations between u_1 and u_2 .

The relationship between geometric objects and algebraic techniques inherent in linear algebra, as well as axiomatic approaches abstracted from tangible conceptions, precise deductive reasoning, intelligent induction, and synthesis, are all extremely valuable in increasing people's mathematical knowledge and attaining scientific awareness.

2. Main Works

2.1. Matrix

A matrix is a table of numbers a_{ij} . A matrix consists of m rows and n columns is denoted as an $m \times n$ matrix. For example, $\begin{bmatrix} 1 & 1 \\ 4 & 5 \\ 3 & 4 \end{bmatrix}$ is a 3×2 matrix.

Square matrices are matrices with same number of rows and columns. $\begin{bmatrix} 1 & 1 \\ 4 & 5 \end{bmatrix}$ is a size 2 matrix.

A column vector is a column of entries.

Similarly, a row vector is a row of entries. For example, $[a_1, a_2, \dots, a_n]$

A matrix's main diagonal runs from top-left to bottom-right.

A zero matrix or null matrix is a matrix all consists of zero entries.

A real matrix and a complex matrix are matrices with real entries and complex entries respectively.

A diagonal matrix is defined as a matrix which all off-diagonal entries are zero. For example: $\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$.

An identity matrix is a diagonal matrix same size and ones on the main diagonal.

The trace of a square matrix $\mathbf{A}$ is the sum of entries on the main diagonal, referred as $\text{tr}(\mathbf{A})$.

The rank of matrix $\mathbf{A}$ is the maximal number of linearly independent columns of $\mathbf{A}$, or the dimension of the vector space its columns generated, normally referred as $\text{rank}(\mathbf{A})$. For example, the matrix $\begin{bmatrix} 1 & 1 & 2 \\ 1 & 9 & 10 \\ 4 & 1 & 5 \end{bmatrix}$ has rank 2: the first two columns are linear independent, but the third column is a linear combination of the first two columns, so the rank is less than 3.

2.2. Determinants

The determinant is a function of the entries of a square matrix. A 2×2 matrix has determinant

$|\mathbf{Z}| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$. For a larger matrix, the determinant of a $n \times n$ matrix $\mathbf{A}$ is the sum of $(n-1) \times (n-1)$ submatrices of $\mathbf{A}$. For all i , $\det(\mathbf{Z}) = \sum_{j=1}^n (-1)^{i+j} Z_{i,j} M_{i,j}$, where $Z_{i,j}$ is the entry of the i th row and j th column of $\mathbf{Z}$, and $M_{i,j}$ is the determinant of the submatrix obtained removing the i th row and j th column of $\mathbf{Z}$. For a 3×3 matrix, the determinant is

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a \begin{vmatrix} e & f \\ h & i \end{vmatrix} - b \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c \begin{vmatrix} d & e \\ g & h \end{vmatrix} \quad (4)$$

If the determinant of a matrix is 0, the matrix is irreversible and called singular matrix. Otherwise it's reversible.

2.3. Matrix transformations

The transpose of a matrix $\mathbf{A}$, referred as $\mathbf{A}^T$, can be obtained by reflecting $\mathbf{A}$ over its main diagonal. For instance,

A square matrix $\mathbf{A}$ is invertible if there exists an matrix $\mathbf{B}$ satisfies $\mathbf{AB} = \mathbf{BA} = \mathbf{I}$. $\mathbf{B}$ is referred as $\mathbf{A}^{-1}$.

The conjugate of a matrix $\mathbf{A}$ with complex entries is obtained from taking the complex conjugate of each entry, denoted as $\mathbf{A}^*$. For real matrices, $\mathbf{A}^* = \mathbf{A}$.

The conjugate transpose of a matrix $\mathbf{A}$ is obtained by taking the transpose of its conjugate matrix, denoted as $\mathbf{A}^H$.

$$\begin{bmatrix} 1 & 1 \\ 4 & 5 \\ 3 & 4 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 & 3 \\ 1 & 5 & 4 \end{bmatrix} \quad (5)$$

2.4. Eigenvalues and eigenvectors

An eigenvector or characteristic vector is a nonzero vector that the direction is not changed when a linear transformation is applied on it. The factor that the vector scales is called an eigenvector, usually referred to λ .

A square matrix A is called diagonalizable when there exists an invertible matrix B and a diagonal matrix C such that $B^{-1}AB=C$. An $n \times n$ matrix is diagonalizable if and only if there exists n eigenvectors of the matrix.

2.5. Matrix operations

Two matrices must have same number of rows and columns to be added. The sum of A and B has same number of rows and columns. The sum is computed by adding corresponding entries of them.

For example $\begin{bmatrix} 1 & 1 & 4 \\ 5 & 3 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 9 & 1 \\ 9 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 1+1 & 1+9 & 4+1 \\ 5+9 & 3+2 & 4+4 \end{bmatrix} = \begin{bmatrix} 2 & 10 & 5 \\ 14 & 5 & 8 \end{bmatrix}$.

Some properties of addition:

$$A + B = B + A \text{ commutativity} \quad (6)$$

$$A + (B + C) = (A + B) + C \text{ associativity} \quad (7)$$

The number of columns of the first matrix must equals the number of rows of second matrix to multiply. The product of A and B is referred as AB .

The product C has entries such that $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$ for a $i \times n$ matrix A and a $n \times j$ matrix B .

For example,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 4 \end{bmatrix} \times \begin{bmatrix} 6 & 6 & 7 \\ 7 & 8 & 9 \end{bmatrix} = \begin{bmatrix} 1 \times 6 + 2 \times 7 & 1 \times 6 + 2 \times 8 & 1 \times 7 + 2 \times 9 \\ 3 \times 6 + 4 \times 7 & 3 \times 6 + 4 \times 8 & 3 \times 7 + 4 \times 9 \\ 5 \times 6 + 4 \times 7 & 5 \times 6 + 4 \times 8 & 5 \times 7 + 4 \times 9 \end{bmatrix} \quad (8)$$

The multiplication of matrices has following properties,

$$A(BC) = (AB)C \quad (9)$$

$$A(B + C) = AB + AC \quad (10)$$

Specially, when it obeys law of commutation when one matrix is identity matrix or the inverse of the other matrix.

2.6. Kronecker product

Let M and N be $a \times b$ and $m \times n$ matrices, respectively. Kronecker sum of two matrices M and N denoted by $\otimes$ is the block diagonal matrix $M \otimes N = \begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$ of dimension $(m + p) \times (n + q)$.

Kronecker product of two matrices M and N denoted by $\otimes$ is defined as

$$M \otimes N = \begin{pmatrix} m_{11}N & m_{12}N & \cdots & m_{1n}N \\ m_{21}N & m_{22}N & \cdots & m_{2n}N \\ \vdots & \vdots & \ddots & \vdots \\ m_{m1}N & m_{m2}N & \cdots & m_{mn}N \end{pmatrix} \quad (11)$$

Where $M \otimes C$ is an $(mp) \times (nq)$ matrix. Note that $M \otimes N \neq N \otimes M$. Kronecker product of matrices possesses a few useful properties:

$$(A + B) \otimes C = A \otimes C + B \otimes C \quad (12)$$

$$(A \otimes B) \otimes C = A \otimes (B \otimes C) \quad (13)$$

$$xA \otimes yB = xy A \otimes B \quad (14)$$

$$x(A \otimes B) = (xA) \otimes B = A \otimes (xB), \text{ where } x \in \mathbb{R} \quad (15)$$

$$(X \otimes Y)^T = X^T \otimes Y^T \quad (16)$$

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}, \quad (17)$$

Where A and B are square matrices.

$$(A \otimes B)(C \otimes M) = (AC) \otimes (BM) \quad (18)$$

$$A \otimes B = (A \otimes C)(C \otimes B) \quad (19)$$

For $m \times m$ matrix A and $n \times n$ matrix B,

$$|A \otimes B| = |A|^n |B|^m \quad (20)$$

$$\text{tr}(A \otimes B) = \text{tr}(A)\text{tr}(B) \quad (21)$$

$$\text{rank}(A \otimes B) = \text{rank}(A)\text{rank}(B) \quad (22)$$

The vec operator creates a column vector from a matrix X by stacking the column vectors of X

$$= [a_1 a_2 \cdots a_n] \text{ below one another: } \text{Vec}(X) = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$$

$$\text{vec}(XYZ) = (Z^T \otimes Y)\text{vec}(X) \quad (23)$$

Some Properties of the vec Operator

$$\text{tr}(XYZ) = \text{vec}(X^T)^T (M \otimes Y) \text{vec}(Z) \quad (24)$$

2.7. Vector in python

2.7.1. Numpy

Numpy is one of the more common ways to represent vectors and the advantage of using numpy is that it can perform linear algebraic operations already listed in the previous section. For example, following code uses numpy, array to define a vector of four elements.

$$\text{import numpy as m} \quad (25)$$

$$a_np = m.\text{array}([1, 0, 3, 4, 5]) \quad (26)$$

2.7.2. List of vectors

We have a list of numpy arrays or a list of list. In this case, the vectors can have different dimensions.

2.7.3. Zero vector and ones vector in numpy

Create a zero vector (called `zero_np`) with same dimension as vector `a_np`. Create a ones vector (called `ones_np`) also with same dimension as vector `a_np`.

```
a_np = np.array ( [1, 0, 3, 4,5] )
```

 (27)

```
zero_np = np.zeros ( len(a_np) )
```

 (28)

```
ones_np = np.ones ( len(a_np) )
```

 (29)

```
print(zero_np, ones_np)
```

 (30)

2.7.4. Vector addition and subtraction

If `a` and `b` are equal-sized numpy arrays, we can have `a+b` and `a-b` for their addition and subtraction

```
a = np.array ( [5,6,7] )
```

 (31)

```
b = np.array ( [500,600,700] )
```

 (32)

```
v_sum = a + b
```

 (33)

```
v_diff = a - b
```

 (34)

```
print (f'Sum of vectors: {v_sum}')
```

 (35)

```
print (f'Difference of vectors: {v_diff}')
```

 (36)

2.7.5. Matrix operations and functions

Arithmetic operations

On numpy arrays, `+`, `-`, `*`, `/` and `**` arithmetic array operations are performed elementwise.

```
M = np.array( [ [2,4],[3,5] ] )
```

 (37)

```
print(M)
```

 (38)

2.7.6. The inverse matrix

For some (not all) square matrices A , there exists a special matrix called the Inverse Matrix, which is typically written as A^{-1} and when multiplied by A

Results in the identity matrix

```
I: A-1A=AA-1=I I = np.eye(4) print(I).
```

 (39)

2.7.7. Matrix powers

Import the function `matrix_power` from the subpackage `numpy.linalg`

```
from numpy.linalg import matrix_power as mpow; M = np.array ( [ [4,5],[-2,3] ] ); print(M).
```

2.7.8. Transpose

We can take the transpose with T attribute `print(M.T)`

2.7.9. Matrix multiplication

The @ operator is used to perform matrix multiplication with numpy arrays `M@M`

Find a python numpy command that will calculate the inverse of a matrix and use it invert the following matrix A. Store the inverse in a new matrix named `A_inv`

```
sym.Matrix(A) (40)
```

```
import numpy as n (41)
```

```
import sympy as s (42)
```

```
s.init_printing(use_unicode=True) (43)
```

```
A = n.matrix( [ [1, 2, 3], [4, 5, 6], [7,8,7] ] (44)
```

```
A_inv = n.linalg.inv(A) (45)
```

```
sym.Matrix(A_inv) (46)
```

2.8. Application in algorithm

2.8.1. The 1th encryption algorithm

Encryption: The advantage of using a diagonal matrix is that when decrypting the key matrix, only the transpose of the matrix needs to be calculated (because one of the properties of an orthogonal matrix is that its inverse is equal to its transpose), thus greatly speeding up the decryption process (the arithmetic power required to calculate the inverse of a large matrix is often much larger than the computation of its transpose) is more suitable for encryption and decryption of large files. The encryption object here is an array of bytes of the file.

Decryption: Calculate the inverse of the key matrix (the diagonal matrix belongs to the orthogonal matrix, and its inverse is equal to its transpose), then multiply the matrix of the bytes array of the encrypted file by the inverse of the key matrix to decrypt the original file.

2.8.2. The 2th encryption algorithm

Encryption: Take the downward rounded square root of the total number of characters of the file to be encrypted as the dimension (number of rows and columns) to generate a square matrix, where each element of the square matrix is a random number picked from the range between two integers. You need to make sure that the determinant of this random number matrix is not zero, i.e., it is guaranteed to be invertible. All the characters of the file to be encrypted are converted to ASCII and then loaded into a square matrix of the same size, then the ASCII matrix of the encrypted file is multiplied by the random number matrix, and the new matrix is translated from ASCII back to characters, and then all the elements of the new matrix are taken out as ciphertext. The random number matrix needs to be saved as a key as well.

Decryption: The ASCII matrix of the ciphertext is multiplied by the inverse of the key matrix to get the ASCII matrix of the plaintext, which is then converted from ASCII to characters to decrypt it into plaintext.

Evaluation: This algorithm needs to calculate the inverse of the matrix when decrypting, so the number of operations is very large in the case of relatively large files, and the efficiency will be

problematic, so this algorithm is more suitable for encrypting small files, especially for encrypting text files, such as encrypting an article, encrypting links, encrypting some text information, and so on. But the biggest advantage of this algorithm is that the degree of encryption is very high, because each element of the encryption matrix is a random number, and the value of each element will have an impact on the content of the ciphertext (because it is the product of the encryption matrix and the ASCII matrix of the plaintext), so there is no possibility of exhaustive running dictionary brute force cracking, because this is much more than the possibility of a simple one-line password. The disadvantage is that for larger files, the encryption and decryption time takes a long time, so it is suitable for smaller files (about 1MB or less)

3. Conclusion

In this paper, the authors examine linear algebra and its applications, including the definition of matrices, special matrices, matrix operations, Kronecker product, determinants, Laplace expansion, and their applications in programming. The meaning of linear algebra has expanded with the development of mathematics. The theory and methods of linear algebra have penetrated into many branches of mathematics, and are also indispensable to the basic knowledge of algebra in theoretical physics and theoretical chemistry. So linear algebra is very important. In the future, the authors will investigate the distillability problem in quantum information in $\mathcal{C}^d \otimes \mathcal{C}^d$.

References

- [1] Alfsen, E., & Shultz, F. (2012). Finding decompositions of a class of separable states. *Linear Algebra and Its Applications*, 437 (10), 2613 – 2629. <https://doi.org/10.1016/j.laa.2012.06.01>.
- [2] Alfsen, E., & Shultz, F. (2012). Finding decompositions of a class of separable states. *Linear Algebra and Its Applications*, 437 (10), 2613 – 2629. <https://doi.org/10.1016/j.laa.2012.06.018>.
- [3] Chen, L., & Đoković, D. Ž. (2016). Distillability of non-positive-partial-transpose bipartite quantum states of rank four. *Physical Review A*, 94 (5). <https://doi.org/10.1103/physreva.94.052318>.
- [4] Chen, L., He, H., Shi, X., & Zhao, L.-J. (2021). Proving the distillability problem of two-copy 4×4 werner states for monomial matrices. *Quantum Information Processing*, 20 (4). <https://doi.org/10.1007/s11128-021-03098-w>.
- [5] Dür, W., Cirac, J. I., Lewenstein, M., & Bruß, D. (2000). Distillability and partial transposition in bipartite systems. *Physical Review A*, 61 (6). <https://doi.org/10.1103/physreva.61.062313>.
- [6] Huang, T.-Z., & Wang, L. (2007). Improving bounds for eigenvalues of complex matrices using traces. *Linear Algebra and Its Applications*, 426 (2-3), 841 – 854. <https://doi.org/10.1016/j.laa.2007.06.008>.
- [7] Nicholson, W. K. (2002). *Linear algebra with applications*. McGraw-Hill Ryerson.
- [8] *Linear algebra* Wilkinson et al. - Springer-Verlag – 1971.
- [9] *Kronecker products and matrix calculus: with applications* Graham - Horwood – 1981.
- [10] Zielke, G. (1987). Horn, R. A.; Johnson, C. R., *Matrix Analysis*. Cambridge etc., Cambridge University Press 1985. XIII, 561 s., £ 35.00. ISBN 0-521-30586-1. ZAMM - Journal of Applied Mathematics and Mechanics / Zeitschrift Für Angewandte Mathematik Und Mechanik, 67 (3), 212 – 212. <https://doi.org/10.1002/zamm.19870670330>.