NEW PROPOSED METHODS FOR CODING INFORMATION USING DIRECT PRODUCT OF SYMMETRIC MATRICES AND CONTRACTION FUNCTIONS WITH NEW PROPERTIES OF HERMITIAN MATRICES

Adel Mohammad Hassan Rizak Al-Rammahi
Dept. of Math\ College of Mathematics and Computer Science\ Kufa University
E-mail: adelr@naharpost.com

ABSTRACT

In this paper, two separately methods were suggested for coding information .The first method was introduced using the directness of symmetric matrices .The contraction function was used for introducing the second method .For more complexity the presented two methods were gathered in one method . And it is proved that the direct product preserves the property of Hermitian positive definite matrices .

1. Introduction

Hermitian and symmetric matrices occur in various sciences, for instance, in Lyapunov control(1), polarimatic decomposition(2) preconditioners problems(3), coupled—oscillators networks multiple antenna block-coded(4) spatial time-frequency distribution (5), electricmagnetic eigenmode (6), robust stability(7), calculations of the frequency band structure of photonic (8) ,and Networks of Nonlinear Coupled Oscillators (9).

For more recent mathematical studies, Cao (10) study the regular of invertible Hermitian matrix, Castel (3) study the parallel two-stage methods ,Han (11) study the block structure of Hermitian matrices and Zhang (5) study spatial time frequency distribution .

In this paper, it is proved that the direct product of two Hermitian positive definite matrices is Hermitian positive definite .The Symmetric direct product approach was introduced for cipher theory A new procedure was programmed for reducing large symmetric matrix into direct product of smaller symmetric submatrices .

For application of fractal geometry in coding information , Pickover (12) considers a broad class of verbal sequences, but for simplicity, he focuses on the most typical sequence, which in (12) referred to as the ***ana*** sequence . This sequence of words (or strings) is defined in stages by induction . In (13) , Pickover's questions on the relative composition of sequence terms and the dimension of the fractal was solved. Also, it presents a beautiful variant of the ***ana*** constructions involving the golden ratio. In (13) and (12) , the code has no the formula of function .

Hutchinson (14) introduced the concept of fractal geometry by using the iterated function systems (IFS) .He proved that the fractal set satisfies two properties . The first is self similarity and the second is the Hausdorff fractional dimension .

In this paper , the code was introduced as contraction functions of iterated function systems which satisfying the self similarity and fractional dimension

2. Basic Known Concepts of Hermitian Matrices

Following are basic concepts of Hermitian matrices which needed in this paper:

Definition (2.1,(15)) A square matrix $A=(a_{ij})$ of complex numbers is called *Hermitian* if $A^* = A^t$ where A^* and A^t denote the conjugate and transpose of A respectively.

In other words, A is Hermitian if $A^H = A^t$ where A^H denotes the Hermitian conjugate $(A^*)^t$.

Definition (2.2,(16,17)) If A and B are m by n , and r by s matrices respectively , then an m.r by n.s matrix $C=(c_{ij})$ is called direct product of A and B and denoted by A⊗B such that $c_{ij}=a_{ij}B$.

Remark(2.1,(18,19) Let H be Hermitian matrix then:
R_1: All diagonal entries of H are real .
R_2: when all entries of H are real , then it is called symmetric .
R_3: All eigen values of H are real .

Definition (2.3,(17,19)) Given a Hermitian matrix $A=(a_{ij})$ of dimension m by m, then A is called Hermitian positive definite if it satisfies the following Sylvester condition : $Det(A_k) > 0$ for all k rainging from 1 to m where

$$A_k=\begin{pmatrix} a_{11} & a_{12} & \text{i} & a_{1k} \\ a_{21} & a_{22} & \text{i} & a_{2k} \\ \text{j} & \text{j} & \text{i} & \text{j} \\ a_{k1} & a_{k2} & \text{i} & a_{kk} \end{pmatrix}.$$

Theorem (2.1,(19)) Let A be m by m Hermitian matrix, then the following statements are equivalent:
T_1) $C^H AC > 0$ for all row vector $C=(c_1,c_2,...c_m)$.
T_2) $\lambda(A) > 0$ for all λ where λ denotes eigen value of A .
T_3) Sylvester condition is satisfied .

Theorem (2.2,(16,17)) Given matrices A and B of dimension n by n and m by m respectively, then eigen values of A⊗ B are the m.n numbers $\lambda_i(A).\ \lambda_j(B)$ for i = 1,2,.. .,n and j =1,2,...,m.

3. Direct product Hermitian Matrices:

This section was concerned to study the direct product of Hermitian matrices as follows:
Given a Hermitian matrices A and B of dimension q by q and t by t respectively.
Let $C=A\otimes B$ C,for determine the diagonal entries C_{vv} of C with respect to definition (2), then $C_{vv}=a_{ii}b_{kk}$, $i=1,2,\text{h},q$, $k=1,2,\text{h},t$, $v=1,2,\text{h},q.t$.
Since each of A and B is Hermitian, by R_1, the diagonal elements of A and B are all real, that is meaning C_{vv} are all real.
For off diagonal entries:
Let $C_{uv}=a_{ij}b_{kl}$
Then

$$\begin{aligned} C^*{}_{uv} &= (a_{ij}b_{kl})^* \\ &= a^*_{ij}b^*_{ll} \\ &= a^t_{ij}b^t_{kl} \\ &= (a_{ij}b_{kl})^t \end{aligned}$$

then $C^*_{uv} = C^t_{uv}$

So one is in a position to introduce the following proposition:

Proposition(1) The direct product of two Hermitian matrices is Hermitian .

Now given A and B be two positive definite Hermitian matrices then by theorem (2.1): $\lambda(A) > 0$, $\lambda(B) > 0$

then by theorem(2.2):

$$\lambda(C) = \lambda(A).\lambda(B)$$

That implies that $\lambda(C) > 0$.

Then when Theorem (1) and definition (3) are taken, one can deduce that C is Hermitian positive definite .Therefore one can introduce the following proposition :

Proposition (2) The direct product of two Hermitian positive definite matrices is Hermitian positive definite .

4.Symmetric Direct Product Matrices Approach for Coding Systems

Matrices can be used to code and decode message. positive integers from 1 through 26 are arbitrarily assignment to the letters of the alphabet, where the assignment is as follows:

a	b	c	…	x	y	z
1	2	3	…	24	25	26

Both the sender and receiver of message have this same table of correspondence between letters and numbers .

Let C(P) = P M

where C is a row cipher text vector, p is a row plaintext vector and M is invertible matrix (20,21,22) .

Following method is introduced for coding massage using direct product of symmetric matrices instead of invertible matrices and as follows :

4.1 Direct Product Matrices Method

1. the massage P is ordered to 6-digits vectors $v = (v_1, v_2, v_3, v_4, v_5, v_6)$.
2. each vector v is encoded into two symmetric matrices

$$A = \begin{pmatrix} v_1 & v_2 \\ v_2 & v_3 \end{pmatrix} \quad and \quad B = \begin{pmatrix} v_4 & v_5 \\ v_5 & v_6 \end{pmatrix} .$$

3. compute the direct product of A and B , $c = A \otimes B$.
4. the cipher text of v becomes the high triangular elements of c , and is wrote as $u(v) = (c_{11}, c_{12}, c_{13}, c_{14}, c_{22}, c_{23}, c_{24}, c_{33}, c_{34}, c_{44})$.
5. for decoding matrix c , one can use the following introduced procedure (IDPM) :

Procedure inverse direct product matrices (IDPM)

Let C be n by n real symmetric matrix where n=r.h, then C may be written as a direct product of two submatrices A and B as follows:

Step 1) Input integer numbers r and h .

Step2) Put n=r.h .

Step3) Input test matrix C .

Step4) Divide C into r-submatrices say W_{ij} where each submatrix has h by h entries for all i , j = 1 , 2 , 3 , ... , r .

Slep5) If matrix is symmetric where i<j , then goto step(6); else goto step(1)with new factorization of n .

Step(6) Find the greatest common divisors (g.c.d) of each matrix in step(5) and named as g_{ij} then write $W_{ij} = g_{ij}.D_{ij}$.

Step(7) If matrix $D_{ij} = D, \quad i < j \quad \forall \quad i, j = 1,2, \mathsf{h}, r$, then goto Step(8) ;else write (C is not direct product with n=r.h) .

Step (8) Construct $G = (g_{ij})$.

Step (9) Write A = G , B=D .

Step(10) End .

4.2 Example For explain above method one can take v as $v = baghda$, then

1. $v = (b, a, g, h, d, a)$
2. $A = \begin{pmatrix} b & a \\ a & g \end{pmatrix}$ *and* $B = \begin{pmatrix} h & d \\ d & a \end{pmatrix}$ .And in number language A , and B has the forms $A = \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix}$ *and* $B = \begin{pmatrix} 8 & 4 \\ 4 & 1 \end{pmatrix}$.
3. $C = A \otimes B$

$$C = \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix} \otimes \begin{pmatrix} 8 & 4 \\ 4 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 16 & 8 & 8 & 4 \\ 8 & 4 & 2 & 1 \\ 8 & 4 & 56 & 28 \\ 4 & 1 & 28 & 7 \end{pmatrix}$$

4. $u(v) = (16,8,8,4,4,2,1,56,28,7)$.
5. For decoding u , construct matrix C ,

$C = \begin{pmatrix} 16 & 8 & 8 & 4 \\ 8 & 4 & 2 & 1 \\ 8 & 4 & 56 & 28 \\ 4 & 1 & 28 & 7 \end{pmatrix}$, and then use procedure (IDPM) :

$$\begin{pmatrix} 16 & 8 & 8 & 4 \\ 8 & 4 & 2 & 1 \\ 8 & 4 & 56 & 28 \\ 4 & 1 & 28 & 7 \end{pmatrix} = \begin{pmatrix} 2\begin{pmatrix} 8 & 4 \\ 4 & 1 \end{pmatrix} & 1\begin{pmatrix} 8 & 4 \\ 4 & 1 \end{pmatrix} \\ 1\begin{pmatrix} 8 & 4 \\ 4 & 1 \end{pmatrix} & 7\begin{pmatrix} 8 & 4 \\ 4 & 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix} \otimes \begin{pmatrix} 8 & 4 \\ 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} b & a \\ a & g \end{pmatrix} \otimes \begin{pmatrix} h & d \\ d & a \end{pmatrix}$$

then the plaintext is $v = baghda$.

5. Hutchinson Fractal Sets

In this section , the construction of fractal sets which introduced by Hutchinson (14) is summarized as follows :

Definition (5.1,(23)) (Metric Space): Let X be a non empty set .A real valued function d is defined on $X \times X$, such that ordered pairs of elements in X are called a metric or distance function on X iff it satisfies , for every $x, y, z \in X$, the following axioms :

$1. d(x, y) \geq 0, \quad d(x, x) = 0$

$2. d(x, y) = d(y, x)$

$3. d(x, z) \leq d(x, y) + d(y, z)$

The real number $d(x, y)$ is called the metric distance from x and y .

Definition (5.2,(24,25)) (Contraction Function): A continuous function $f : X \to X$ is contraction if there is an $\alpha \in (0,1)$ such that $d(f(x), f(y)) \leq \alpha d(x, y) \forall x, y \in X$.

Definition (5.3,(26)) (Iterated Function Systems): Let X be a complete metric space, and let $f_i : X \to X$ be contraction maps for $i = 1,2, \text{i}, n$.,with Constants $\alpha_1, \alpha_2, \ldots, \alpha_n$. Let α = max α_i . clearly all f_i are contraction maps with parameter α . The functions f_i *are called Iterated Function System* with parameter α.

Definition (5.4,(27)) (Attractor) *An* attractor for the iterated function system *(IFS)* $\{ f_i \}$ *is a non-empty compact set such that :*

$E = f_1(E) \text{ r } f_2(E) \ldots f_N(E)$.

When IFS has an attractor , then it is called hyperbolic (14,26,27).

Theorem (5.1 ,(14,26,27,28)) A complete metric space with a finite number of Contraction maps has a unique attractor E.

5.1 Pickover's Code

In Pickover's method (12,13) the first four terms of the ***ana*** sequence are:

a

ana

anaannana

anaannanaanaannannanaannana :

To see how the ***ana*** sequence arises from a verbal context , observe that a letter is replaced in the next stage by its description using the indefinite articles ***a*** and ***an*** , appropriately, **a** is described by "***ana*** " and **n** by " ***ann*** ".

Procedure (Pickover's ana code) :

1) let a $\to$ ana , n $\to$ ann

2) take a = black , and n = white , so the stages of ***ana*** code are:

the third stage of ***ana*** code be anaannana

5.2 Contraction Code Method

Pickover (12,13) introduces the ***ana*** sequence and fractal using two self-referential constructions arising from the use of language.

In (12,13) the code is represented by fractal figure instead of formula In this paper , the fractal code is represented by contraction hyperbolic iterated function systems.

In this section the proposition method of contraction code is introduced as in the following procedure .

Procedure (contraction code method)

1) Let a=dot ,and n=dash

2) Applying the two contraction functions on L = [0 , 1].

$w_1(x) = ax$

$w_2(x) = ax + b$

3)Let D be the dimension of the fractal curve (attractor) ,so

D = $\frac{Ln\left(\frac{1}{a}\right)}{Ln\left(\frac{1}{b}\right)}$,and that it is a fractal [1].where the number of iterated functions system be 2 and the scaling factor be a .

For explain the proposed method , the following examples are given :

Example (5.2.1) One can take the parameters a and b are $a = \frac{1}{3}, b = \frac{2}{3}$ .So the code in first three stages are :

a , **ana** , **anannnana**

And it is a similar result of Pickover's method when the axioms be

$a \to ana$

$n \to nnn$

And in dot –dash form is .-.---.-.

Example (5.2.2) One can take the parameters a and b are $a = \frac{1}{4}, b = \frac{3}{4}$ So the code in first three stages are :

a , **anna** , **annannnnnnnnanna**

And it is a similar result of Pickover's method when the axioms be

$a \to ana$

$n \to nnnn$

And in dot –dash form is .--.---------.--.

6. Product - Contraction Code Method

the hyperbolic iterated function system $w_1(x) = \frac{1}{3}x, w_2(x) = \frac{1}{3}x + \frac{2}{3}$ is transforming (encoding) the real interval [a,b] of length 1 into three subintervals each of length $\frac{1}{3}$ .so one

can used the idea of contraction hyperbolic iterated function system for encoding the letter into three letters and as in the following contraction table code:

letter	A	b	C	…	y	Z
code	Yza	zab	abc	…	wxy	Xyz

For more complexity one can gathered the direct product matrices method which studied in section(4.1) and contraction table code in the following product contraction method :

6.1 Product - Contraction Method

1. order the plaintext into 2-digits vectors $v=(v_1,v_2)$.
2. encoding v to contraction code $w(v)$ according to contraction code table .
3. using the procedure of *Direct Product Matrices Method* which studied in section(4.1) .

6.2 Example(6.1) For explain above method one can take v as $v=(c,d)$, then

1. $w(v)=(abc,bcd)$ by using contraction code table .
2. $A=\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ *and* $B=\begin{pmatrix} b & c \\ c & d \end{pmatrix}$ .And in number language A , and B has the forms $A=\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$ *and* $B=\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$.
3. $C=A\otimes B$

$$C=\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}\otimes\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$$

$$C=\begin{pmatrix} 2 & 3 & 4 & 6 \\ 3 & 4 & 6 & 8 \\ 4 & 6 & 6 & 9 \\ 6 & 8 & 9 & 12 \end{pmatrix}$$

4. $u(w)=(2,3,4,6,4,6,8,6,9,12)$.
5. For decoding w , construct matrix C ,

$$C=\begin{pmatrix} 2 & 3 & 4 & 6 \\ 3 & 4 & 6 & 8 \\ 4 & 6 & 6 & 9 \\ 6 & 8 & 9 & 12 \end{pmatrix}$$, and then use procedure (IDPM) :

$$\begin{pmatrix} 2 & 3 & 4 & 6 \\ 3 & 4 & 6 & 8 \\ 4 & 6 & 6 & 9 \\ 6 & 8 & 9 & 12 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} & 2\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} \\ 2\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} & 3\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \otimes \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ b & c \end{pmatrix} \otimes \begin{pmatrix} b & c \\ c & d \end{pmatrix}$$

then $w(v) = (abc, bcd)$, and by using inverse contraction code function via contraction code table $v = (c, d)$.

7. Conclusion

It is proved that when each of A and B be Hermitian positive definite matrix , then the direct product of A and B is Hermitian positive definite. In other hand , it is known that the common method of matrix representation in coding theory ,is concerned on multiplying original plaintext message vector by invertible choosing constant matrix.

In this paper ,a new approach was introduced to encode plain text message by using original plain text with ought invertible matrix . The presented approach is summarized by following steps: *first* the letters (corresponding numbers) are partitioned into set of vectors. *Second* each vector transform into a symmetric matrix. *Third* a direct product of two sequence symmetric matrices was computed .*Finally* the output upper triangular numbers (letters) represent the code words.

Pickover`s code has no the formula of code function . It deals with figure only .The contraction functions and iterated function system were used here for constructing of contraction code instead of the fractal figure . Hutchinson fractal set was used in this proposed method .To generate a population , a practical procedure was introduced and used in finite number of stages .

For more complexity , the direct product matrices method which studied in section(4.1) and contraction table code were gathered in one method and named as product contraction method

References

[1] Ogata K., “Modem control Engineering” , prentic Hall mt .me., 3e, pp896- 958,1997.

[2] Pottier E. and Lee J. S .,“Application of the Polarimatric Decomposition Theorem for Unsuperrised Classification of Fully, Polarimatric sar Data Based on the Wishart Distribution “; email:eric. Pottier @ univrennes. fr,.

[3] Castel M.J., Migallon V., and Penades J.; “on Parallel two- Stage Mthods for Hermitian Positive Definite Matrices with Applications To Preconditioning”; J. of electronic Transactions on Numerical Analysis; vol. 12, pp. 88-112, 2001.

[4] Baccaralli E., Biagi M., and Fasano A.; “Optimized Design and Multiple-Antenna 4 Generation WIANS for Partially-Coherent Decoding” , CNR project ,2000.

[5] Zhang Y. Muw. And Amin M.G., “Subspace Analysis of Spatial Time Frequency Distribution Matrices” ;IEEE Trans. Sgnal process.vol .49, no.4,April,2000.

[6] Mondelli A.A.; An Advanced Eleclromgnetic Eigenmode Solver for Vacuum Electronics Derices- Ctlss”;Proceedings of the 1999 Particle Accelerator Conference, New York , pp. 360-362, 1999.

[7] Fuh C.C. and Tung P.C.; “Robust St Bounds for Lure Systems with Parametric Uncertainty”; J. of Marine Sc. and Tech. Vol.7, No.2, pp.73-78(1999).

[8] Modinos A., Stefanou N., and Yannopupas V.;" Applications of the Layer —KKR Method to Photonic Crystals"; Optical Society of America, Optics Express, vol.8,no.3,pp.197- 202,1999 ,
[9] Justh E.W. , Krishnaprasad P.S., and Kub F.J.; "Convergence Analysis and Analog Circuit Applications for a Class of Networks of Nonlinear Coupled Oscillators; The National Science Foundation Eng. Research Center Program, MarylandUn., 2000.
[10] Cao, Z.H.; "A note on P-Regular Splitting of Hermitian Matrix; Siam J. on Matrix Analysis and Appi.; vol.21, no.4, pp .1392- 1393, 2000.
[11] Han V. And Dramc Z.; "On Scaled Almost- Diagonal Hermitian Matrix Pairs; Siam J. on Matrix Analysis and Applications, vol.18,no.4,pp. 1000- 1012.1997
[12] Pickover,C.,Wonders of Numbers;Oxford University press;2001
[13] Joseph , L. PE ; ANA'S Golden Fractal ; Fractals, Vol. 11, No. 4 ,pp. 309-313 ; 2003
[14] Hutchinson J " Fractal and Self Similarity " , Indian University Mathematics Journal .vol.30 , pp. 713-740 , 1981 .
[15] Lang. S.; "Linear Algebra"; Addison— wesley pub . PP.200-204; 1980.
[16] Barnet ,S. and Storey, C.; "Matrix Method in Stability Theory" ; Nelson, 1970.
[17] Leech. J.W. and Newman, D.J.; "How To Use Group"; Chapman and Hall Ltd . pp.67; 1977.
[18] Saeed U.A. and Shukkue N.H. , Linear Algebra ,Mosul University press ,1984 .
[19] Lang S. ,linear algebra, second edition ,Addison wealey,1984.
[20] Gilbert W.J.,Modern Algebra with Applications,Wiley- Interscience Pub. PP.299;1984.
[21] Roberts F.S. ;"Applied Combinatorics" ; Printic-Hall ,Inc. England, 1984.
[22] Menezes, A., Orschot, P.V.,(1996)Handbock of Applied Cryptography ,CRC Press,pp.283-319.
[23] Kolman B.(1984), Introductory linear algebra with applications, Macmillan publishing company ,new york ,3e .
[24] Bartle R.G. ,The element of real analysis ,2e,john wiley and sons ,new york ,pp.105-123, (1976) .
[25] Josh K.D. ,Introduction to topology , john wiley and sons , New York ,pp.105-123, (1983) .
[26] Barnsley M. and Demko S.G. ,iterated function systems and the global construction of fractals ,proc.roy.soc.London ser.A 399,pp243-274,(1985) .
[27] Barnsley M. , Fractals Everywhere , (Academic Press) ,(1989)
[28] Mandelbrot D. , the fractal geometry of nature , freeman , san Francisco , (1982) .
[29] Alfonseca M . and Ortega A., Determination of Fractal, Dimensions From Equivalent L System ; IBM J.RES & DEV , VOL.45; NO.6 , November ; 2001 .

طرق مُقتَرَحةُ جديدة لتشفير المعلوماتِ بأستخدام الجداء المباشر للمصفوفاتِ المتماثلةِ ودوال الإنكماشِ مع صفات جديدة للمصفوفاتِ الهرميتية

عـــادل محمـــد حســـن رزاق الرمـــــاحي
قسم الرياضيات/ كلية الرياضيات وعلوم الحاسبات/ جامعة الكوفة

الخلاصة

فـــي هـــذا البحـــث، إثنان مـــن الطـــرق إقترحـــتْ لـــتـــشـــفـــير المـــعـــلـــومـــاتِ، الـــطـــريـــقـــة الأولى قـــدّمـــتْ إستـــعـــمـــال جـــــداءِ المـــصـــفـــوفـــاتِ المـــتـــمـــاثـــلـــةِ. دالـــةِ الإنـــكـــمـــاشَ إستـــــعـــمـــلـــتْ لتَـقـديـــــم الـــطـــريـــقـــةِ الثـــانـــيـــــةِ. للتعـــــقـــيـــدِ الأكـــثـــرِ، الـــطـــريـــقـــتـــان المـــمـــقـــدَّمـــتـــا ن جـمُـعـتـــا فـــــيطـــريـــقـــــةِ واحـــــدة. وتـــمـــــــت الـــبـــــرهـــنـــــة بـــأنّ الـــــجـــــداءِ الـــمـــبـــــاشـــــرَ تـــحـــافـــــظ عـــــلـــى الـــصـــفـــــة الـــمـــوجـــيـــــة يـقـيـنـــــا لـــلـــمـــــصـــفـــــوفـــــاتِ الـــــهـــــرمـــــيـــــتـــــيـــــة.