International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 01 | Jan 2021 www.irjet.net p-ISSN: 2395-0072

Cryptographic Algorithm to Find Best Least Square Solutions of Kronecker Product Boundary Value Problems

Divya L.N[1], Yan Wu[2], SriRam Bhagavathula[3], K. N. Murty[4]

[1]*SGWS Inc, Dallas, TX, USA.*
[2]*Department of Mathematical Sciences, Georgia Southern University, GA 30460 USA.*
[3]*Conns Inc.USA.*
[4]*Department of Applied Mathematics, Andhra University, Waltair, A. P.*

Abstract: *A cryptographic algorithm is presented to solve Kronecker product two-point boundary value problems. Cryptographic algorithm we presented in this paper protects users by providing encryption and decryption of data and allows authorized users only. This algorithm is used as a tool to obtain the best least square solution of the Kronecker product first order matrix system. The use of AES technique in cryptography is useful to solve two-point boundary value problems.*

Keywords: Encryption, Decryption, Kronecker product of matrices, best least square solution, Security of data, Variation of parameters formula.

AMS (MOS) classifications: 94A60, 34B15, 68P30, 68P25

1. Introduction

Cryptography plays an interesting role in achieving the primary aims of security, authentication, integrity, confidentiality, and non-repudiation. Cryptographic algorithms are presented to achieve the above goals. Cryptography is a fundamental tool for cyber security and privacy which must be protected for long periods of time. The use of cryptography to solve boundary value problems is due to Viswanadh V. Kanuri, et. al. [8,14,16] and the use of Kronecker product boundary value problems and $(\Phi \times \Psi)$ bounded solutions are also due to Kasi Viswanadh, K. N. Murty and P. S. Anand, Sailaja P and Vellanki N. Lakshmi [2-5,7,9-14,15,17]. We present in this paper encryption and decryption algorithms to solve linear system of first order equations and exhibit the best least square solutions of the boundary value problems. In fact cryptography is an ever growing, unending subject and it must remain so for its healthy growth. There are many ways and many techniques in cryptography and among them the most used technique is AES. This technique in fact preserves confidentiality, authenticity, and integrity, and is popularly applied in defense and satellite communication technology. We use cryptographic algorithm to find the best least square solution of the Kronecker product boundary value problems in the non-invertible case. This paper is organized as follows: section 2 presents properties of Kronecker product of matrices and develop variation of parameters formula for the Kronecker product non-homogeneous equation. Section 3 presents solution of the Kronecker product boundary value problem in terms of Green's matrix, and section 4 presents least square solution to the Kronecker product boundary value problem. This section presents an important algorithm on cryptographic encryption and decryption and present least square vector which is the best least square solution of the Kronecker product boundary value problem in the rank deficiency case and also in non-invertible case.

2. PRELIMINARIES

Kronecker product of matrices is an interesting area of current research and the use of Kronecker product matrices in boundary value problems is due to K. N. Murty, Balaram and Kasi Viswanadh V. Kanuri [6]. The idea of Kronecker product of matrices is used as a tool to obtain existence and uniqueness criteria for two-point boundary value problems associated with first order system of difference equations by Kasi Viswanadh, et. al. [2]. In cryptography the closest and shortest vector problem associated with lattices are the two ever growing computational problems. The closest vector problem (CVP) in inhomogeneous variant of the shortest vector problem (SVP) in which given a lattice and some target one has to find the closest lattice point. The hardness part of the lattice problem mainly comes from the fact that there are many possible bases for the same lattice. We present cryptographic algorithm in section 4. We now consider two different non-homogeneous first order systems of the form

$x'(t) = A(t)x(t) + f(t)$ (2.1)

$y'(t) = B(t)y(t) + g(t)$ (2.2)

where x is an m-vector, A is an (m×m) continuous matrix,$f(t)$is also an m-vector, y is an n-vector, B is an (n×n) continuous matrix, and $g(t)$is an n-vector. (2.1) and (2.2) can concurrently be embedded in a single Kronecker product system as

$[x(t) \otimes y(t)]' = [A(t) \otimes I_n + I_m \otimes B(t)][x(t) \otimes y(t)] + [f(t) \otimes I_n + I_m \otimes g(t)]$ (2.3)

where I is a unit matrix. We shall now present the definition of Kronecker product of matrices and some of their properties:

Definition 2.1 If $A \in \mathbb{R}^{m\times m}$ and $B \in \mathbb{R}^{n\times n}$, then the Kronecker product or tensor product of A and B, denoted by $A \otimes B$, is defined as

$$(A \otimes B) = \begin{bmatrix} a_{11}B & \dots & a_{1m}B \\ \dots & \dots & \dots \\ a_{m1}B & \dots & a_{mm}B \end{bmatrix}$$

i.e. $(A \otimes B) = (a_{ij}B)$ for all $i, j = 1,2,\dots,m$.

The Kronecker product of matrices defined above has the following properties:

(i) $(A \otimes B)^T = (A^T \otimes B^T)$ (T stands for transpose)

(ii) $(A \otimes B)(C \otimes D) = (AC \otimes BD)$

(iii) $(A \otimes B)^{-1} = (A^{-1} \otimes B^{-1})$

(iv) $(A \otimes B)' = (A' \otimes B + A \otimes B')$ ($'$ stands for derivative)

where the matrices involved are of appropriate dimensions to be conformable and invertible.

The homogeneous Kronecker product system associated with (2.3) is given by

$[x(t) \otimes y(t)]' = [A(t) \otimes I_n + I_m \otimes B(t)][x(t) \otimes y(t)]$. (2.4)

Let X be a fundamental matrix of $x' = A(t)x$ and Ybe a fundamental matrix of $y' = B(t)y$. Then, we have the following result:

Theorem 2.1 $(X(t) \otimes Y(t))$is a fundamental matrix of (2.4) if and only if $X(t)$is a fundamental matrix of $x' = A(t)x$ and $Y(t)$is a fundamental matrix of $y' = B(t)y$.

Proof: First suppose that X and Y be fundamental matrices of $x' = A(t)x$ and $y' = B(t)y$, respectively. Then it is claimed that $(X(t) \otimes Y(t))$is a fundamental matrix of (2.4) For

$[X(t) \otimes Y(t)]' = X'(t) \otimes Y(t) + X(t) \otimes Y'(t)$

$= A(t)X(t) \otimes Y(t) + X(t) \otimes B(t)Y(t)$

$= [A(t) \otimes I_n + I_m \otimes B(t)][X \otimes Y]$. (2.5)

Hence the claim. Conversely, suppose $(X(t) \otimes Y(t))$is a fundamental matrix of the homogeneous system (2.4). Then from (2.5), we have

$(X'(t) - A(t)X) \otimes Y = -X \otimes (Y' - B(t)Y)$.

Multiply both sides of the equation by $X^{-1} \otimes Y^{-1}$, we get

$X^{-1}(X' - A(t)X) \otimes I_n = -I_m \otimes Y^{-1}(Y' - B(t)Y)$.

The above relation is true if each side is either a null matrix or an identity matrix, i.e.

$X^{-1}(X' - A(t)X) = 0$, or $X' - A(t)X = 0$as such X is a fundamental matrix of $x' = A(t)x$.

If

$X^{-1}(X' - A(t)X) = I_m$, then, $X' - A(t)X = X$ or $X' = (I + A(t))X$, which is a contradiction to the hypothesis. Similar contradiction arises with the other side. Hence the proof.

We now turn our attention to establish variation of parameter formula for the Kronecker product first order non-homogeneous system (2.3). Let $(x(t) \otimes y(t))$be any solution of (2.3) and $(\hat{x}(t) \otimes \hat{y}(t))$be a particular solution of (2.3). Then, $(x(t) \otimes y(t)) - (\hat{x}(t) \otimes \hat{y}(t))$is a solution of the homogeneous system (2.4). Hence,

$$x(t) \otimes y(t) = (\hat{x}(t) \otimes \hat{y}(t)) + [X(t) \otimes Y(t)][c_1 \otimes c_2]$$

where c_1 and $c_2$are constant m-vector and n-vector, respectively. Since

$[X(t) \otimes Y(t)][c_1 \otimes c_2]$ cannot be a solution of (2.3) unless $f(t) \otimes I_n + I_m \otimes g(t) \equiv 0$. Hence, we seek a particular solution of (2.3) in the form

$\hat{x}(t) \otimes \hat{y}(t) = [X(t) \otimes Y(t)][c_1 \otimes c_2](t)$.

Substituting this form of solution in (2.3) to get

$$[X(t) \otimes Y(t)]'[c_1 \otimes c_2](t) + [X(t) \otimes Y(t)][c_1 \otimes c_2]'(t)$$

$$= [A(t) \otimes I_n + I_m \otimes B(t)][X(t) \otimes Y(t)][c_1 \otimes c_2] + [f(t) \otimes I_n + I_m \otimes g(t)].$$

The first term on the left side equals the first term on the right side in the above equation, hence they cancel each other. We are left with

$$[X(t) \otimes Y(t)][c_1 \otimes c_2]'(t) = f(t) \otimes I_n + I_m \otimes g(t).$$

Hence,

$[c_1 \otimes c_2]'(t) = [X^{-1}(t) \otimes Y^{-1}(t)][f(t) \otimes I_n + I_m \otimes g(t)]$.

or

$[c_1 \otimes c_2](t) = \int_a^t [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds$.

Hence, a particular solution of (2.3) is given by

$\hat{x}(t) \otimes \hat{y}(t) = [X(t) \otimes Y(t)] \int_a^t [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds.$ (2.6)

Now, any solution of (2.3) is given by

$x(t) \otimes y(t) = [\hat{x}(t) \otimes \hat{y}(t)] + [X(t) \otimes Y(t)][c_1 \otimes c_2]$. (2.7)

We now give our attention to the two two-point boundary value problems

$x' = A(t)x + f(t), M_1x(a) + N_1x(b) = \alpha_1$, (2.8)

and

$y' = B(t)y + g(t), M_2y(a) + N_2y(b) = \alpha_2$ (2.9)

where $\alpha_1$and $\alpha_2$are (m×1) and (n×1) given vectors, respectively. Equations (2.8) and (2.9) can be embedded in a Kronecker product boundary value problem as

$$[x(t) \otimes y(t)]' = [A(t) \otimes I_n + I_m \otimes B(t)][x(t) \otimes y(t)] + [f(t) \otimes I_n + I_m \otimes g(t)]$$

$[M_1 \otimes I_n + I_m \otimes M_2][x \otimes y](a) + [N_1 \otimes I_n + I_m \otimes N_2][x \otimes y](b) = [\alpha_1 \otimes I_n + I_m \otimes \alpha_2]$. (2.10)

3. EXISTENCE AND UNIQUENESS

In this section, we establish the existence and uniqueness of the solution of the boundary value problem (2.10) in terms of the integral involving Green's matrix. Substituting the general form of $x(t) \otimes y(t)$ given in (2.7) in the boundary condition matrix given in (2.10), we get

$$\{[M_1 \otimes I_n + I_m \otimes M_2][x(a) \otimes y(a)] + [N_1 \otimes I_n + I_m \otimes N_2][x(b) \otimes y(b)]\}$$

$$= [M_1 \otimes I_n + I_m \otimes M_2][X(a) \otimes Y(a)][c_1 \otimes c_2] + [N_1 \otimes I_n + I_m \otimes N_2]\{[X(b) \otimes Y(b)][c_1 \otimes c_2] +$$

$[X(b) \otimes Y(b)] \int_a^b [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds\} = 0.$

Let $D = [M_1 \otimes I_n + I_m \otimes M_2][X(a) \otimes Y(a)] + [N_1 \otimes I_n + I_m \otimes N_2][X(b) \otimes Y(b)]$,

then, our initial assumption that the homogeneous Kronecker product boundary value problem has only the trivial solution ensures that D is non-singular. Hence

$c_1 \otimes c_2 = -D^{-1}[N_1 \otimes I_n + I_m \otimes N_2][X(b) \otimes Y(b)] \int_a^b [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds.$

Therefore, any solution of the Kronecker product boundary value problem is given by

$$x(t) \otimes y(t) = [X(t) \otimes Y(t)]\{\int_a^t [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds -$$

$D^{-1}[N_1 \otimes I_n + I_m \otimes N_2][X(b) \otimes Y(b)] \int_a^b [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds\}.$

Splitting the second integral into $[a, t)$ and $(t, b]$, we write

$x(t) \otimes y(t) = [X(t) \otimes Y(t)]\{\int_a^t [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds -$

$D^{-1}[N_1 \otimes I_n + I_m \otimes N_2][X(b) \otimes Y(b)] \int_a^t [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds -$

$D^{-1}[N_1 \otimes I_n + I_m \otimes N_2][X(b) \otimes Y(b)] \int_t^b [X^{-1}(s) \otimes Y^{-1}(s)][f(s) \otimes I_n + I_m \otimes g(s)]ds\}$

$= \int_a^b G(t, s)[f(s) \otimes I_n + I_m \otimes g(s)]ds,$

where $G(t, s)$is the Green's matrix for the homogeneous boundary value problem.

In the previous discussion, we assumed that the characteristic matrix D is non-singular. If D is either singular or D is an (mp×nq) matrix with rank say r, then the solution of the Kronecker product boundary value problem is not unique and hence we need to develop a method known as best least square solution to the boundary value problem. Let us consider the Kronecker product system:

$(A \otimes B)(x \otimes y) = (\alpha_1 \otimes \alpha_2)$, (3.1)

where A is an m×p and B is an n×q matrix so that $(A \otimes B)$is an mn×pq matrix and $x \otimes y$is a column vector of order pq×1 and $\alpha_1 \otimes \alpha_2$is also a column vector of order pq×1. let $D = A \otimes B$ and $z = x \otimes y$. Then (3.1) can be written as

$D\ z = \alpha$, where $= \alpha_1 \otimes \alpha_2$. (3.2)

Since D an mn×pq matrix with $mn > pq$ and α is a pq×1 vector and equality holds in (3.2) if the solution for z is unique. It is only possible if D is square and non-singular. In general, equality is not possible as the equation (3.2) is an over determined system. Since $mn > pq$, our aim is to find the best least square solution of (3.2) such that the residual vector $r(z) = \alpha - Dz$ is small, i.e.

$$\min\|r(z)\|^2 = \min\|\alpha - D\ z\|^2$$

is least. Thus, in this section, we consider numerically stable and computationally efficient algorithms.

Definition 3.1 Let $S \subset \mathbb{R}^{mn}$. The orthogonal complement of S denoted by $S^{\perp}$is defined as the set of all vectors $z \in \mathbb{R}^{mn}$that are orthogonal to S.

One important property of orthogonal complement is that

$$\mathbb{R}^{mn} = V \oplus V^{\perp}$$

where $\oplus$is the direct sum which means any vector $z \in \mathbb{R}^{mn}$ can uniquely be written as

$$z = P + o$$

where $p \in V$and $o \in V^{\perp}$.

Theorem 3.1 Let D be an mn×pq matrix and $\alpha \in \mathbb{R}^{mn}$. Then $\hat{z}$ is a least square solution to the system (4.2) if and only if it is a solution of the augmented linear system

$D^T D\ \hat{z} = D^T \alpha$.

Proof: Let $z \in \mathbb{R}^{pq}$. Then, Dz is an arbitrary vector in the column space of D, which we write as $R(D)$. Let $r(z) = \alpha - Dz$ is minimum if Dz is the orthogonal projection of α onto $R(D)$. Since $R(D)^{\perp} = null(D^T)$, $\hat{z}$ is a least square solution if and only if

$D^T r(z) = D^T(\alpha - D\hat{z}) = 0$,

which is equal to the system of normal equations in the form

$D^T D\ \hat{z} = D^T \alpha$. (3.3)

For this solution to be unique, the matrix D must have full column rank.

Sensitivity and conditioning perturbation:

The condition number of D denoted by $\kappa(D)$ is defined as $\kappa(D) = \|D\|\|D^+\|$, where $D^+$is the generalized inverse of D and has the following properties:

(i) $DD^+D = D$, (ii) $D^+DD^+ = D^+$,

(iii) $(DD^+)^* = DD^+$, and (iv) $(D^+D)^* = D^+D$,

where * indicates conjugate transpose. If D is an mp×nq matrix, then $D^+$is nq×mp and such a D^+satisfying the above four properties is unique. If $\kappa(D) < 1$, then the system is said to be well conditioned and if $\kappa(D) \gg 1$, then the system is ill-conditioned.

Example: Consider the linear system

$$\begin{pmatrix} 1 & 1 \\ 1 & 1+\varepsilon \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix},$$

where $0 < \varepsilon \ll 1$, has the solution $[2, 0]^T$. We claim that the above system is ill-conditioned because small perturbations on αlead to significant changes in the behavior of the solution of the system. If we choose $\alpha = [2, 2+\varepsilon]^T$, it has the solution $[1, 1]^T$, and it is significantly different from $[2, 0]^T$. We now examine the relationship between the error and relative error.

Consider the system $Dz = \alpha$ with the expected solution z and computed solution $\hat{z}$. Then, we write $e = z - \hat{z}$, $r = \alpha - D\hat{z} = \alpha - \hat{\alpha}$. Since z may not be obtained immediately, the accuracy of the solution is evaluated by writing $r = \alpha - D\hat{z} = DZ - D\hat{z} = De$. We take norm on e to get a bound on the absolute error.

$$\|e\| = \|z - \hat{z}\| = \|D^+(\alpha - \hat{\alpha})\| \leq \|D^+\|\|\alpha - \hat{\alpha}\| = \|D^+\|\|r\|$$

so that $\|e\| \leq \|D^+\|\|r\|$. Using this we can derive a bound for the relative error as $\|e\|/\|x\|$ and $\|r\|/\|b\|$. From

$$\|e_2\| \leq \|D^+\|\|r\| \frac{\|Dz\|}{\|b\|} \leq \|D^+\|\|D\|\|z\| \frac{\|r\|}{\|b\|}$$

thus

$$\frac{\|e_2\|}{\|x\|} \leq \kappa(D) \frac{\|r\|}{\|b\|}. \quad (3.4)$$

If $\kappa(D) < 1$ then the system is well conditioned, otherwise ill-conditioned. For well-conditioned problem $\kappa(D) \approx 1$. We also derive a residue bound as

$$\frac{1}{\kappa(D)} \frac{\|r\|}{\|b\|} \leq \frac{\|z-\hat{z}\|}{\|z\|} \leq \kappa(D) \frac{\|r\|}{\|b\|}.$$

These bounds are true for any matrix D. Consider the system

$$Dz = b$$

with

$$D = \begin{bmatrix} 1+\varepsilon & 1-\varepsilon \\ 1-\varepsilon & 1+\varepsilon \end{bmatrix}, \Delta D = \begin{bmatrix} -\varepsilon & \varepsilon \\ \varepsilon & -\varepsilon \end{bmatrix},$$

where $0 < \varepsilon \ll 1$. Then consider perturbation matrix

$$\hat{D} = D + \Delta D = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Clearly, $\hat{D}$ is singular, solving system $Dz = \alpha$ yields no solution.

Normal equations method: Now, we know that solving the system of equations

$Dx = \alpha$,

with columns of D linearly independent reduces to the system of normal equations of the form

$D^T Dx = D^T \alpha$.

The normal equations method computes the solution to the least square solution problem by transforming the rectangular matrix into a triangular form.

Cholesky factorization: If D is an mp×nq matrix with full column rank, then the following hold for $D^T D$:

(1) $D^T D$is symmetric, i.e. $(D^T D)^T = D^T (D^T)^T = D^T D$.

(2) $D^T D$ is positive definite, i.e. $z^T D^T Dz = (Dz)^T (Dz) = \|Dz\|^2 > 0$ if $z \neq 0$.

Since $D^T D$is symmetric, positive definite, we conclude $D^T D = LL^T$, where L is an nq×nq lower triangular matrix.

FLOP: complexity of numerical algorithm. Triangular matrices are extensively used in numerical algorithms such as Cholesky factorization or QR-factorization since triangular systems are one of the simplest systems to solve. A FLOP is a floating point operation (+, −, ×, /). In an nq×nq lower triangular system $Ly = b$, each y_k is obtained by writing $y_k = b_k - \sum_{j=1}^{k-1} l_{kj} y_j$, which requires $k-1$ multiplications and $k-1$ additions, Thus, y requires $(nq)^2 - nq$ FLOPS to compute. Since nq is usually sufficiently large to lower order terms, we say that nq×nq forward substitution costs $n^2 q^2$ FLOPS.

Algorithm for Cholesky factorization:

For a matrix D define $D_{ii'}, D_{jj'}$ to be the $(i' - i + 1) \times (j' - j + 1)$ submatrix of D with upper left corner of D_{ij} and lower right corner of $D_{i'j'}$.

Algorithm: Let $R = D$

for $k = 1$to mp

$R_{j,j:mp} = R_{j,j:mp} - R_{k,j:mp} R_{kj} / R_{kk}$

$R_{k,k:m} = R_{k,k:m} / \sqrt{R_{kk}}$.

The last line dominates the operation count for this algorithm. The FLOP count is

$\sum_{k=1}^{mp} \sum_{j=k+1}^{m} 2(mp - j) \sim 2 \sum_{k=1}^{mp} \sum_{j=1}^{k} j \sim \sum_{k=1}^{mp} k^2 \sim m^3 p^3 / 3$.

Thus, we have the following algorithm for the normal equations:

1) Calculate $E = D^T D$ (E symmetric, $mpn^2 q^2$ FLOPs).

2) Cholesky factorization $E = LL^T$ ($n^3 q^3 / 3$ FLOPs).

3) Calculate $d = D^T b$ ($2mpnq$ FLOPs).

4) Solve $Lx = d$by forward substitution ($n^2 q^2$ FLOPs).

5) Solve $L^T z = x$ by backward substitution ($n^2 q^2$ FLOPs).

This gives the cost, for large m, n, p, q, at $mpn^2 q^2 + n^3 q^3 / 3$ FLOPs.

4. Cryptographic algorithm to find the best least square solution

Cryptography prior to the modern age was effectively synonymous with encryption and decryption of information from a readable state to apparent nonsense. Modern cryptography is mostly based on mathematical theory and computer science practice; cryptographic algorithms are based on computational hardness assumptions, making sure algorithms are hard break in practice by any adversary. It is theoretically possible to break such a system, but it is impossible to do so by any unauthorized person. The growth of cryptographic technology has raised a number of legal issues in the present information age. The word of cryptography comes from Greek word “cryptos” that means hidden and “graphikos” which means writing. Encryption is the process of translating plain text into something that appears to be random and meaningless. Decryption is the process of converting cipher text back to plaintext. In the two-key system also known as public key system, one key encrypts the information and another key a private key that is never shared by anyone and only shared by the known person

to the sender. If a sending computer first encrypts the message with the intended receiver's public key and only with sender's secret public key, the sender and receiver are able to acknowledge one another and protect the secrecy of the message. We now present our main algorithm.

Main algorithm: our aim is to find the nest least square solution of the Kronecker product system

$$(A \otimes B)(x \otimes y) = (\alpha_1 \otimes \alpha_2), (4.1)$$

where A is an m×n matrix , B is a p×q matrix and $(x \otimes y)$ is a column vector of $1 \times nq$ and so it is with $(\alpha_1 \otimes \alpha_2)$. To make matters simple, we write

$(A \otimes B) = D$, $(x \otimes y) = z$, and $(\alpha_1 \otimes \alpha_2) = \alpha$,

where D is an mp×nq matrix and if we put $mp = k$, $nq = l$, then

$$D\ z = \alpha. (4.2)$$

We first present an algorithm that computes the closest vector without any representation choice, but the two different representations significantly reduce the speed.

Definition 4.1 A matrix is D is said to be a generator matrix if it has real entries and the rows of D are linearly independent on $\mathbb{R}$.

Firstly, we assume that a generator matrix D and an input vector z are given. Let D be a k×l matrix and $z \in K$. By means of a linear integer transformation, we first transform D into another matrix R_2which generates an identical lattice and then rotate and reflect R_2into a lower triangular matrix R_3 such that

$\Lambda(R_3) = \Lambda(R_2) = \Lambda(D)$.

It is essential to rotate and reflect the input vector z in the same way, so that the transformed input vector, say z, is in the same rotation to$\Lambda(R_3)$as z in rotation to$\Lambda(D)$. By reversing the operations of rotation and reflection enables us to produce $\hat{z}$, which is the lattice point closest to z in $\Lambda(A)$. Following these steps, we present the algorithm in details:

Algorithm, closest point (D, z).

Input: A lattice point $\hat{z} \in \Lambda(D)$, the closest to z.

Step 1: Let $R_2 = WD$where W is a k×k matrix with integer entries and $|W| = \pm 1$.

Step 2: Compute a (k×l) orthogonal matrix Q with ortho-normal columns such that $R_2 = R_3 Q$ where $R_3$is a (k×l) lower triangular matrix with diagonal entries positive.

Step 3: Let $H := R_2^{-1}$.

Step 4: Let $z_3 := zQ^T$.

Step 5: $\hat{u}_3$: =DECODE(R_3, z_3).

Step 6: Return $\hat{z} := \hat{u}_3 R_3$.

Note that Step1 is a basic reflection. If no reflection is needed, take W as a unit matrix. The speed and numerical stability can be improved significantly if proper search is made in Step 2. As an alternative to QR decomposition, R_3 can be obtained by Cholesky decomposition by writing $D = LU$in our context $R_3 = L$and the rotation matrix is given by $Q = R_3^{-1} R_2$. However, QR method is the generally recommended method to find least square solutions. Note that the decomposition of $D = QR$ is unique, whichever technique we adopt and ??? in our modified QR-algorithm, Q is orthogonal implies $|Q| = \pm 1$. If D is an ill-conditioned matrix, the method we are going to present is the most effective one.

In Steps 4-6 the input vectors are processed. They are transformed into the coordinate system of R_2, decoded, and transformed back again.

Algorithm DECODE(H, z)

Input: a (k×k) lower triangular matrix H with positive diagonal elements and a k-dimensional vector $z \in \mathbb{R}^k$ to decode in the lattice $\Lambda(H^{-1})$.

Output: a k-dimensional vector $\hat{u} \in \mathbb{Z}^k$ such that $\hat{u}H^{-1}$ is a lattice point $\hat{z}$ that is closest to z.

m: =the size of H

bestdist: $= \infty$

$K := k$ (dimension of the matrix)

$\text{dists}_k := 0$

$e_k := zH$

$u_k := e_{kk}$

$y := (e_{kk} - u_k)/h_{kk}$

$stepk := \text{sgn}^*(y)$

Loop

newdist: = distk + y^2

If newdist < bestdist then {

If $k \neq 1$ then {

$e_{k-1,j} = e_{kj} - y_{ki}$ for $i = 1, \ldots k-1$

$k := k - 1$

distk: =newdist

$u_k = e_{kk}$

$z := (e_{kk} - y_k)/h_{kk}$

stepk: = sgn^*(y)

} else {

$\hat{u} := u$

bestdist: =newdist

$k := k - 1$

$u_k := u_k + \text{stepk}$

$y := (e_{kk} - u_k)/h_{kk}$

stepk: =stepk-sgn*(stepk)

}

} else {

if $k = mp$ then return to $\hat{u}$ (and exit)

else {

$k = k + 1$

$u_k = u_k + \text{stepk}$

$y := (e_{kk} - u_k)/h_{kk}$

go to step 25

}

{

go to <loop>}

In the above algorithm, mp, k are in the dimension of the sublayer structure that is currently being investigated.

As an example, consider

$$D = (A \otimes B) = \begin{bmatrix} 1 & 3 & 3 & 2 \\ 2 & 6 & 9 & 5 \\ 1 & 3 & 3 & 0 \end{bmatrix}, z = \begin{bmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{bmatrix}, \text{and } \alpha = \begin{bmatrix} 15 \\ 6 \\ 22.5 \end{bmatrix}.$$

Then, min least square solution is given by

$\hat{x} = [-0.211009174 \quad -0.633027523 \quad 0.96330275 \quad 0.11009173]^T$.

Using the decode algorithm the shortest vector is found

$z = [-0.211000837 \quad -0.633127525 \quad 0.97340273 \quad 0.11008271]^T$.

Note the z given by above vector is the best least square solution of the Kronecker product two point boundary value problem. These results further supplements the results in [1] .

References

1. E. Agrell, T. Eriksson, A. Vardy and K. Zeger, Closest point search in lattices, IEEE Transactions on Information Theory, vol. 48, no. 8, p: 2201-2214 (2002)

2. Kasi Viswanadh V. Kanuri, K.N. Murty, Three-Point boundary value problems associated with first order matrix difference system-existence and uniqueness via shortest and closest Lattice vector methods, J. of Nonlinear Sciences and Applications, vol. 12, p: 720-727 (2019).

3. Kasi Viswanadh V Kanuri, Existence Of Ψ-Bounded Solutions For Fuzzy Dynamical Systems On Time Scales, International Journal of Scientific & Engineering Research, 2020, Vol. 11, No. 5, 613--624.

4. Kasi Viswanadh V. Kanuri, R. Suryanarayana, K. N. Murty, Existence of Ψ-bounded solutions for linear differential systems on time scales, Journal of Mathematics and Computer Science, 20 (2020), no. 1, 1--13.

5. Murty, K. N., Andreou, S., Viswanadh, K. V. K., Qualitative properties of general first order matrix difference systems. Nonlinear Studies, 16(2009), no. 4, 359--370.

6. K. N. Murty, V. V. S. S. S. Balaram, K.V. K. Viswanadh, "Solution of Kronecker Product Initial Value Problems Associated with First Order Difference System via Tensor-based Hardness of the Shortest Vector Problem", Electronic Modeling, vol. 6, p: 19--33 (2008).

7. K.N. Murty, K.V.K. Viswanadh, P. Ramesh, Yan Wu, "Qualitative properties of a system of differential equation involving Kronecker product of matrices", Nonlinear Studies, Vol 20, No: 3, P: 459--467 (2013)

8. K.N. Murty, Yan Wu, Viswanadh V. Kanuri, "Metrics that suit for dichotomy, well conditioning of object oriented design", Nonlinear Studies, Vol 18, No: 4, P: 621--637 (2013)

9. Kasi Viswanadh V Kanuri, Y. Wu, K.N. Murty, "Existence of (Φ ⊗Ψ) bounded solution of linear first order Kronecker product of system of differential equations", International Journal of Science and Engineering Research, 2020, Vol 11, No. 6, P: 156—163.

10. Kasi Viswanadh V. Kanuri, Sailaja,P., Murty, K. N., A new approach to the construction of transition matrix with application to control systems, AIP Conference Proceedings, 2020, Vol. 2269, No. 1, Page 030044.

11. Kasi Viswanadh V. Kanuri, Bhagavathula, S., & Murty, K., (2020). Stability Analysis of Linear Sylvester System of First Order Differential Equations. International Journal of Engineering and Computer Science, 9(11), 25252--25259.

12. N., L. V. ., Vijaya, N. ., & J., M. . (2020). Existence of (Ø^α⊗ψ^α) bounded solutions of Kronecker product first order system of Differential equations. International Journal of Engineering and Computer Science, 9(10), 25240--25245.

13. Kasi Viswanadh V. Kanuri, Yan Wu, SriRam Bhagavatula, Existence of (F, Y) bounded solutions of linear Sylvester system of first order differential equations, 2020, International Journal of Scientific & Engineering Research, Volume 11, Issue 10. Pp. 995—1005.

14. Mourad Chelgham, Ali Boussayoud, Kasi Viswanadh V. Kanuri, A New Class of Symmetric Functions of Binary Products of Tribonacci numbers and other well-known Numbers. 2021, Online Journal of Analytic Combinatorics 16(1), In Press.

15. Sailaja,P., Kasi Viswanadh V. Kanuri, Murty, K. N., An innovative approach to the construction of transition matrix with application to control systems, October 2020, AIP Conference Proceedings 2269(1). Conference: AIP Conference Proceedings for International Conference on Multifunctional Materials, At Hyderabad, Telangana, India.

16. Nabiha Saba, Ali Boussayoud, Kasi Viswanadh V. Kanuri, Mersenne Lucas numbers and complete homogeneous symmetric functions, 2021, Journal of Mathematics and Computer Science, In Press.

17. Charyulu L.N.Rompicharla, Sundaranand V.Putcha and G.V.S.R.Deekshitulu, Existence of (Φ ⊗Ψ) bounded solutions for linear first order Kronecker product systems, International Journal of Recent Scientific Research, 2020, Vol. 11, No. 6, pp. 39047--39053.