УДК 519.816

K. N. Murty
Aurora Engineering College
(Bhongir, Nalgonda Dist. A.P 508116, India,
E-mail: nkanuri@hotmail.com),
V.V.S.S.S Balaram
Aurora's Technological and Research Institute
(Parvathapur, Uppal, Hyderabad — 500039, India,
E-mail: vadrevu_kinnera@yahoo.com),
K. Viswanadh
(1 Court Sq, Long Island City, NY — 11120,
E-mail: kasikv@hotmail.com)

Solution of Kronecker Product Initial Value Problems Associated with First Order Difference System via Tensor— based Hardness of the Shortest Vector Problem

(Recommended by Prof. E. Dshalalow)

This paper presents criteria for the existence and uniqueness of solution to Kronecker product initial value problem associated with general first order matrix difference system. A modified least square method and a modified QR algorithm are developed to find the best least square solution of the Kronecker product of matrices. Using these methods as a tool the general solution of the Kronecker product initial value problem whose initial condition matrix is over determined is established. Using the method developed by Ishey Haviv and Oded Regev, on finding shortest vector problem we improve further the best least square solution. To boost the hardness factor we simply apply the standard Kronecker product or tensor product of lattices.

Предложен критерий существования и единственности решения задачи кронекеровского произведения с начальными условиями, связанной с обобщенной разностной системой, имеющей матрицу первого порядка. Разработаны модифицированный метод наименьших квадратов и модифицированный QR алгоритм для нахождения наилучшего решения кронекеровского произведения матриц методом наименьших квадратов. Установлено, что при использовании этих методов для общего решения задачи кронекеровского произведения с начальными условиями ее матрица начальных условий является переопределенной. С использованием метода, разработанного Ishey Haviv и Oded Regev, при определении задачи кратчайшего вектора улучшено решение методом наименьших квадратов. Применено стандартное кронекеровское произведение или тензорное произведение на сетках для повышения коэффициента жесткости.

Key words: product initial value problem, existence and uniqueness of solution, the best least square solution, shortest vector problem.

1. Introduction. Kronecker product or tensor product of matrices is an interesting area of current research and a great deal of work has been done by many authors in recent years [1—3]. The application of Kronecker product matrix system has been extended to various fields of control engineering, method of lines and systems engineering. The importance of Kronecker products of matrices gained momentum because of its computational and notational advantages. In Cryptography the closet point search problem and shortest vector problem (SVP) associated with lattices are the two main computational problems. The closed vector problem (CVP) is inhomogeneous variant of SVP, in which given a lattice and some target point one has to find the closet lattice point. The hardness part of lattice problem mainly comes from the fact that there are many possible bases for the same lattice. One of the main reasons for research on the hardness of lattice problem is their application in Cryptography. In the year 2004 Ajtai [4], came up with a construction of Cryptography primitives, whose security relies on the worst case of hardness of certain lattice problems.

In this paper we shall be concerned with the general two first-order matrix difference systems of equations of the form:

$$x(n+1)=A(n)\,x(n),$$

$$y(n+1)=B(n)\,y(n),$$

where $A(n)$, $B(n)$ are square matrices of orders $(p\times p)$ and $(q\times q)$ respectively and whose components are all real defined on

$$N_{n_0}^{+}=\{n_0,\ n_0\pm1,\ n_0\pm2,\ \dots,\ n_0\pm k,\ \dots\}$$

where $k\in N^{+}$ and $n_0\in N$, N being the set of integers. Before, we present our results in this paper we need the following basic properties of the Kronecker product of matrices.

If $A\in R^{m\times n}$ and $B\in R^{p\times q}$ then the Kronecker product (or tensor product) of A and B denoted by $(A\otimes B)$ is defined as the partition matrix

$$(A\otimes B)=\begin{pmatrix} a_{11}b & \dots & a_{1n}b \\ \vdots & \ddots & \vdots \\ a_{m1}b & \cdots & a_{mn}b \end{pmatrix}$$

and is in $R^{mp\times nq}$.

The Kronecker product matrices defined above has the following properties:

$$(A\otimes B)^{T}=(A^{T}\otimes B^{T}),$$

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

$$(A\otimes B)^{-1}=A^{-1}\otimes B^{-1},$$
$$(A\otimes B)(n+1)=(A(n+1)\otimes B(n+1)),$$

where the matrices involved are of appropriate dimensions to be conformable for multiplication and inversion. For example $(A\otimes B)^{-1}=A^{-1}\otimes B^{-1}$ we implicitly assumed that A and B are non-singular square matrices. Initially we are not making use of the theory of generalized inverse of matrices; this concept will be used in our later discussions in developing modified-Gram-Schmidt algorithm and in encoding and decoding algorithms. Usually search problems involving lattices can be solved using modifications and extensions of the closest-point algorithm. Given a lattice $\Lambda\in R^m$, the shortest vector problem is to find a vector in $\Lambda-\{0\}$ that has the smallest Euclidean norm. In fact, the history of the shortest vector problem is closely interlinked with that of the closest point problem. Further, the closest point algorithm can be straight forwardly modified to solve the shortest vector problem [5].

This paper is organized as follows: in section 2 we present the general solution of the homogeneous Kronecker product difference system and then present the general solution of the Kronecker product initial value problem; section 3 is concerned with the method of least squares for Kronecker product system of equations. We develop the method of least square problems to solve the Kronecker product system by using modified QR-algorithm. Section 4 provides a brief work of khots work [6] together with the minor modifications; we boost the hardness factor of the standard tensor product of lattices. To our belief it improves the best least square solution and SVP technique further improves the existing methods to find the best least square solution of the Kronecker product initial value problem.

2. General solution of the kronecker product initial value problem. In this section, the general form of the Kronecker product difference equation we consider is of the form

$$[P(n)\otimes R(n)][X(n+1)\otimes Y(n+1)]+[Q(n)\otimes S(n)][X(n)\otimes Y(n)]=0, \quad (1)$$

where $P(n), Q(n)$ are invertible square matrices of order $(p\times p)$ and $R(n), S(n)$ are square matrices order $(q\times q)$ and $x(n)$ and $y(n)$ are vectors of orders $(p\times 1)$ and $(q\times 1)$ respectively. We now present the general solution of (1) in terms of fundamental matrix solutions of $P(n)x(n+1)+Q(n)x(n)=0$ and $R(n)y(n+1)+S(n)y(n)=0$ in the next theorem.

Theorem 1. $[\Phi(n)\otimes\Psi(n)]$ is a fundamental matrix of (1) if and only if $\Phi(n)$ and $\Psi(n)$ are fundamental matrices of $P(n)x(n+1)+Q(n)x(n)=0$ and $R(n)y(n+1)+S(n)y(n)=0$ respectively.

Proof. Suppose $\Phi(n)$ and $\Psi(n)$ are fundamental matrices of $P(n)x(n+1)+$ $+Q(n)x(n)=0$ and $R(n)y(n+1)+S(n)y(n)=0$ respectively. Then

$$[\Phi(n+1)\otimes\Psi(n+1)]=[P^{-1}(n)Q(n)\otimes R^{-1}(n)S(n)][\Phi(n)\otimes\Psi(n)]=$$

$$=[P^{-1}(n)\otimes R^{-1}(n)][Q(n)\otimes S(n)][\Phi(n)\otimes\Psi(n)].$$

Hence

$$[P(n)\otimes R(n)][\Phi(n+1)\otimes\Psi(n+1)]+[Q(n)\otimes S(n)][\Phi(n)\otimes\Psi(n)=0].$$

Hence $[\Phi(n)\otimes\Psi(n)]$ is a fundamental matrix of (1). Conversely, suppose $[\Phi(n)\otimes\Psi(n)]$ be a fundamental matrix of (1). Then

$$[P(n)\otimes R(n)][\Phi(n+1)\otimes\Psi(n+1)]+[Q(n)\otimes S(n)][\Phi(n)\otimes\Psi(n)]=0.$$

Therefore

$$[\Phi(n+1)\otimes R(n)]=[P^{-1}(n)\otimes R^{-1}(n)][Q(n)\otimes S(n)][\Phi(n)\otimes\Psi(n)].$$

This implies

$$[\Phi(n+1)+P^{-1}(n)Q(n)\Phi(n)]\otimes I_q=-[(I_p)\otimes\Psi(n+1)+R^{-1}(n)S(n)\Psi(n)].$$

This relation is true if and only if $\pm[\Phi(n+1)+P^{-1}(n)Q(n)\Phi(n)]\otimes I_q$ and $\pm\Psi(n+1)+R^{-1}(n)S(n)\Psi(n)$ are either identity matrices or null matrices of appropriate dimensions. Thus, we have the following two cases.

Case 1:

$$-[\Phi(n+1)+P^{-1}(n)Q(n)\Phi(n)]=I_p \text{ and } \Psi(n+1)+R^{-1}(n)S(n)\Psi(n)=I_q.$$

Then

$$\Phi(n+1)=-[I_p+P^{-1}(n)Q(n)\Phi(n)] \text{ and } \Psi(n+1)=I_q-R^{-1}(n)S(n)\Psi(n).$$

Case 2:

$$[\Phi(n+1)+P^{-1}(n)Q(n)\Phi(n)]=I_p \text{ and } -[\Psi(n+1)+R^{-1}(n)S(n)\Psi(n)]=I_q.$$

Then

$$\Phi(n+1)=I_p-P^{-1}(n)Q(n)\Phi(n) \text{ and } \Psi(n+1)=-[I_q+R^{-1}(n)S(n)\Psi(n)].$$

Case 1 and 2 contradict each other. Thus

$$\pm[\Phi(n+1)+P^{-1}(n)Q(n)\Phi(n)]=O_p \text{ and } \pm[\Psi(n+1)+R^{-1}(n)S(n)\Psi(n)]=O_q.$$

Thus $\Phi(n)$ and $\Psi(n)$ are fundamental matrices of $P(n)x(n+1)+Q(n)x(n)=0$ and $R(n)y(n+1)+S(n)y(n)=0$ respectively.

Theorem 2. Any solution of the Kronecker product system of difference equations (1) satisfying $[x(n_0)\otimes y(n_0)]=[C_1\otimes C_2]$ is of the form

$$[x(n)\otimes y(n)]=[\Phi(n,n_0)\otimes\Psi(n,n_0)][C_1\otimes C_2],$$

where $\Phi(n,n_0)=\Phi(n)\Phi^{-1}(n_0)$ and $\Psi(n,n_0)=\Psi(n)\Psi^{-1}(n_0)$ with the property $\Phi(n,n_0)=I_p$ and $\Psi(n,n_0)=I_q$.

Proof. Proof is elementary and hence omitted.

The above solution may conveniently be written as

$$[x(n)\otimes y(n)]=[\Phi(n)\otimes\Psi(n)][C_1\otimes C_2], \qquad (2)$$

where C_1 and C_2 are constant column vectors of order p and q respectively. We now consider the Kronecker product Initial value problem of the form:

$$[P(n)\otimes R(n)][x(n+1)\otimes y(n+1)]+[Q(n)\otimes S(n)][x(n)\otimes y(n)]=0, \qquad (3)$$

$$(M_1\otimes N_1)(x(n_0)\otimes y(n_0)=(\alpha_1\otimes\alpha_2],$$

where M_1 and N_1 are constant matrices of orders $(p\times p)$ and $(q\times q)$ respectively and α_1 is $(p\times 1)$ and α_2 is $(q\times 1)$ column vectors. Substituting the general form solution given in (2) in (3), we get

$$[M_1\otimes N_1][\Phi(n_0)\otimes\Psi(n_0)][C_1\otimes C_2]=[\alpha_1\otimes\alpha_2].$$

Hence

$$[C_1\otimes C_2]=[M_1\otimes N_1]^{-1}[\Phi(n_0)\otimes\Psi(n_0)]^{-1}[\alpha_1\otimes\alpha_2]=$$
$$=[M_1^{-1}\Phi^{-1}(n_0)\otimes N_1^{-1}\Psi^{-1}(n_0)][\alpha_1\otimes\alpha_2].$$

We are now in a position to give the general solution of (1) satisfying (3) and is given by

$$[x(n)\otimes y(n)]=[\Phi(n)\otimes\Psi(n)][M_1^{-1}\Phi^{-1}(n_0)\otimes N_1^{-1}\Psi^{-1}(n_0)][\alpha_1\otimes\alpha_2]=$$
$$=[\Phi(n)M_1^{-1}\Phi^{-1}(n_0)\alpha_1\otimes\Psi(n)\,N_1^{-1}\Psi^{-1}(n_0)\alpha_2].$$

The solution of the initial value problem when M_1 and N_1 are invertible is unique. However when M_1 and N_1 are rectangular matrices of order $(m\times p)$ and $(n\times q)$ respectively, we develop modified QR algorithm in the next section [7].

We now establish variation of parameters formula associated with the non-homogenous first order difference system

$$[P(n)\otimes R(n)][x(n+1)\otimes y(n+1)]+[Q(n)\otimes S(n)][x(n)\otimes y(n)]=$$
$$=[F_1(n)\otimes F_2(n)], \qquad (4)$$

where $F_1(n)$ and $F_2(n)$ are column vectors of order $(p\times 1)$ and $(q\times 1)$ respectively.

Theorem 3. A particular solution of (4) is given by

$$[x(n)\otimes y(n)]=-[\Phi(n)\otimes\Psi(n)]\sum_{i=n_0}^{n}[Q^{-1}(i)\otimes S^{-1}(i)][F_1(i)\otimes F_2(i)].$$

Proof. Any solution of the homogeneous system (1) is of the form

$$[x(n)\otimes y(n)]=[\Phi(n)\otimes\Psi(n)][C_1\otimes C_2],$$

where $\Phi(n)$ is a fundamental matrix of $P(n)x(n+1)+Q(n)x(n)=0$ and $\Psi(n)$ is a fundamental matrix of $R(n)y(n+1)+S(n)y(n)=0$.

Since a solution cannot be a solution of (4) unless $[F_1(n)\otimes F_2(n)]=[0\otimes 0]$. Therefore, we seek a particular solution of (4) in the form

$$[x(n)\otimes y(n)]=[\Phi(n)\otimes\Psi(n)][C_1(n)\otimes C_2(n)].$$

Then

$$[P(n)\otimes R(n)][\Phi(n+1)\otimes\Psi(n+1)][C_1(n+1)\otimes C_2(n+1)]+$$
$$+[\Phi(n)\otimes\Psi(n)][C_1(n)\otimes C_2(n)]S=[F_1(n)\otimes F_2(n)]$$

ince $\Phi(n+1)=-P^{-1}(n)Q(n)\Phi(n)$ and $\Psi(n+1)=-R^{-1}(n)S(n)\Psi(n)$. We have

$$-[Q(n)\otimes S(n)][C_1(n+1)\otimes C_2(n+1)]+[Q(n)\otimes S(n)][C_1(n)\otimes C_2(n)]=$$
$$=[\tau(n+1)-C_1(n)\otimes C_2(n+1)-C_2(n)]=-[Q^{-1}(n)\otimes S^{-1}(n)][F_1(n)\otimes F_2(n)],$$
$$\Delta C_n=-[Q^{-1}(n)\otimes S^{-1}(n)][F_1(n)\otimes F_2(n)]$$

or

$$C(n)=-\sum_{i=n_0}^{n}[Q^{-1}(i)\otimes S^{-1}(i)][F_1(i)\otimes F_2(i)].$$

Therefore

$$[x(n)\otimes y(n)]=[\Phi(n)\otimes\Psi(n)]\left[[C_1\otimes C_2]-\sum_{i=n_0}^{n}[Q^{-1}(i)\otimes S^{-1}(i)][F_1(i)\otimes F_2(i)]\right].$$

Thus, we have the following theorem.

Theorem 4. Any solution of the first order difference system (4) is of the form

$$[x(n)\otimes y(n)]=[\Phi(n)\otimes\Psi(n)][C_1\otimes C_2]-$$
$$-[\Phi(n)\otimes\Psi(n)]\sum_{i=n_0}^{n}[Q^{-1}(i)\otimes S^{-1}(i)][F_1(i)\otimes F_2(i)].$$

Proof is immediate.

3. Method of least squares. In this section, we develop a method for least square problems to solve the Kronecker product system of equations

$$(A\otimes B)(x\otimes y)=\alpha\otimes\beta. \qquad (5)$$

We need the following results for constructing least square algorithm and the best least square algorithm.

Result 1. Let A be an ($m \times n$) given matrix with rank $p \leq \min\{m, n\}$. Then there exists a factorization $AP = QR$ with the following properties:

i) P is an $(n \times n)$ permutation matrix with the first p columns of AP form a basis of

$$I_m(A) = \{Ax \in R^m / x \in R^n\};$$

ii) Q is an $(m \times p)$ matrix with orthonormal columns and R is a $(p \times n)$ upper trapezoidal matrix of the form $R = [R_1 \;\; R_2]$, where R_1 is a non-singular $(p \times p)$ upper triangular matrix and R_2 is a $(p \times n - p)$ matrix.

Note that in (5), A is $(m \times n)$ and B is $(p \times q)$ rectangular matrices. Suppose that A and B are QR decomposed as $A=Q_1 R_1$ and $B=Q_2 R_2$, where Q_1 is $(m \times m)$ matrix with orthonormal columns, R_1 is $(m \times n)$ upper trapezoidal matrix where Q is $(p \times p)$ matrix with orthonormal columns and R_2 is $(p \times q)$ upper trapezoidal matrix. Assuming that full rank case, i.e. $\rho(A) = n < m$ and $\rho(B) = q < p$, R_1 is of the form

$$R_1 = \begin{pmatrix} r_{11}^{(1)} & r_{12}^{(1)} \ldots r_{1n}^{(1)} \\ 0 & r_{22}^{(1)} \ldots r_{2n}^{(1)} \\ \ldots\ldots\ldots & \ldots\ldots\ldots \\ 0 & 0 \ldots r_{nn}^{(1)} \\ 0 & 0 \ldots 0 \\ \ldots\ldots\ldots & \ldots\ldots\ldots \\ 0 & 0 \ldots\ldots 0 \end{pmatrix} = \begin{pmatrix} R^{(1)} \\ 0^{(1)} \end{pmatrix},$$

where $R^{(1)}$ indicates an $(n \times n)$ matrix and $0^{(1)}$ indicates an $((m-n) \times n)$ null matrix and similarly

$$R_2 = \begin{pmatrix} r_{11}^{(2)} & r_{12}^{(2)} & \cdots & r_{1q}^{(2)} \\ 0 & r_{22}^{(2)} & \cdots & r_{2q}^{(2)} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \cdots & r_{qq}^{(2)} \\ 0 & 0 & \cdots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} R^{(2)} \\ 0^{(2)} \end{pmatrix}$$

where $R^{(2)}$ is a $(p \times p)$ matrix and $0^{(2)}$ is $(p - q \times q)$ null matrix.

Theorem 5. If A and B have a QR factorizations of the form $Q_1\,R_1$ and $Q_2\,R_2$ respectively, then $A\otimes B$ has a permitted QR factorizations as

$$(A\otimes B)=(Q_1R_1\otimes\, Q_2R_2)=(Q_1\otimes\, Q_2)(R_1\otimes R_2).$$

Proof. Consider

$$(Q_1\otimes Q_2)^T(Q_1\otimes Q_2)=(Q_1^TQ_1\otimes Q_2^TQ_2)=(I_m\otimes I_p)=I_{mp}.$$

This implies $Q_1\otimes Q_2$ is orthogonal also to $Z(R_1\otimes R_2)=\begin{pmatrix}x\\0\end{pmatrix}$ where τ is $(nq\times nq)$ square matrix, 0 is an $((mp-np)\times nq)$ null matrix and z is a permutation matrix.

Theorem 6. $(R_1\otimes R_2)^T(R_1\otimes R_2)=(R^{(1)}\otimes R^{(2)})(R^{(1)}\otimes R^{(2)})$.

Proof. We know that

$$(R_1\otimes R_2)^T(R_1\otimes R_2)=(R_1^T\otimes R_2^T)(R_1\otimes R_2)=$$

$$=\begin{pmatrix} r_{11}^{(1)}R_2^T & 0_{q\times p}\cdots & 0_{q\times p}\cdots & 0_{q\times p}\cdots & 0_{q\times p}\\ r_{12}^{(1)}R_2^T & 0_{21}^{(1)}R_2^T & 0_{q\times p}\cdots & 0_{q\times p}\cdots & 0_{q\times p}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ r_{1n}^{(1)}R_2^T & r_{2n}^{(1)}R_2^T & r_{nn}^{(1)}R_2^T & 0_{q\times p}\cdots & 0_{q\times p}\end{pmatrix}\begin{pmatrix} r_{11}^{(1)}R_2 & r_{12}^{(1)}R_2 & \cdots & r_{1n}^{(1)}R_2\\ 0_{p\times q} & r_{21}^{(1)}R_2 & \cdots & r_{2n}^{(1)}R_2\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ 0_{p\times q} & 0_{p\times q} & \cdots & r_{nn}^{(1)}R_2\\ 0_{p\times q} & 0_{p\times q} & \cdots & 0_{p\times q}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ 0_{p\times q} & 0_{p\times q} & \cdots & 0_{p\times q}\end{pmatrix}.$$

The block element in block row i and block j column n element is given by

$$[(R_1\otimes R_2)^T(R_1\otimes R_2)]_{ij}\;=\sum_{l=1}^{\min\{i,\,j\}}(r_{li}^{(1)}r_{lj}^{(1)})(R_2^TR_2),\;1\le i,j\le n\,.$$

The element in row i and column j of $(R_2^TR_2)$ is given by

$$(R_2^TR_2)=\sum_{k=1}^{\min\{i,\,j\}}r_{ki}^{(2)}r_{kj}^{(2)},\;1\le i,j\le q.$$

Thus $(R_1\otimes R_2)^T(R_1\otimes R_2)=(R^{(1)}\otimes R^{(2)})^T\;(R^{(1)}\otimes R^{(2)})$.

Theorem 7. $\tau^T\tau$ is the cholesky factorization of $(A\otimes B)^T(A\otimes B)$, where $\tau=(R^{(1)}\otimes R^{(2)})$.

Proof.

$$(A\otimes B)^T(A\otimes B)=(Q_1R_1\otimes Q_2R_2)^T(Q_1R_1\otimes Q_2R_2)=$$

$$=[(Q_1\otimes Q_2)(R_1\otimes R_2)]^T[(Q_1\otimes Q_2)(R_1\otimes R_2)]=$$
$$=(R_1\otimes R_2)^T(Q_1\otimes Q_2)^T(Q_1\otimes Q_2)(R_1\otimes R_2)=$$
$$=(R_1\otimes R_2)^T z^T z(R_1\otimes R_2)=$$
$$=[z(R_1\otimes R_2)]^T[z(R_1\otimes R_2)]=\tau^T\tau=GG^T,$$

where G^T is lower triangular.

Now, applying these results to our main problem

$$(A\otimes B)=(x\otimes y)_{n0}=(\alpha\otimes\beta)$$

the least square solution $(\bar{x}\otimes\bar{y})(n_0)$ to the normal equation

$$(A\otimes B)^T(A\otimes B)(\bar{x}\otimes\bar{y})(n_0)=(A\otimes B)^T(\alpha\otimes\beta)$$

can be obtained from the equivalent equation

$$\tau^T\tau(\bar{x}\otimes\bar{y})(n_0)=(A\otimes B)^T(\alpha\otimes\beta)=(h_1\otimes h_2).$$

Since the coefficient matrix is the product of the upper and lower triangular matrices, the solution can be computed by the usual two step procedure:

1. Solve by forward substitutions.
2. Solve $\tau(\bar{x}\otimes\bar{y})(n_0)=(w\otimes z)$ by backward substitutions.

If the dimension of τ $(nq\times nq)$ is too large to permit the direct solution of τ, the above two-step procedure can be further refined. Partition of each vector $(w\otimes z)$ and $(h_1\otimes h_2)$ into n-sub-vectors, with each sub-vector of dimension $(q\times 1)$ be an $(nq\times 1)$ matrix can be partitioned as $(w^{(i)}\otimes z^{(j)})$ for $i=1,2,\ldots,n$ and $j=1,2,\ldots,q$. Similarly $(h_1\otimes h_2)$ and the solution vectors $(\bar{x}\otimes\bar{y})(n_0)$ are partitioned. In step1, $\tau^T(w\otimes z)=(h_1\otimes h_2)$ may be written in partitioned form as

$$\begin{bmatrix} r_{11}^{(1)}[R^{(2)}]^T & \cdots & 0_q & \cdots & 0_q \\ r_{12}^{(1)}[R^{(2)}]^T & \cdots & r_{22}^{(1)}[R^{(2)}]^T & \cdots & 0_q \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ r_{1n}^{(1)}[R^{(2)}]^T & & r_{2n}^{(1)}[R^{(2)}]^T & & r_{nn}^{(1)}[R^{(2)}]^T \end{bmatrix}\begin{bmatrix} \omega^{(1)}\otimes z^{(j)} \\ \omega^{(2)}\otimes z^{(j)} \\ \omega^{(n)}\otimes z^{(j)} \end{bmatrix}=$$

$$=\begin{bmatrix} h_1^{(1)}\otimes h_2^{(j)} \\ h_1^{(2)}\otimes h_2^{(j)} \\ \cdots\cdots\cdots \\ h_1^{(n)}\otimes h_2^{(j)} \end{bmatrix},\quad j=1,2,\ldots,q. \tag{6}$$

Since $[R^{(2)}]^T$ is a lower triangular matrix, the forward substitution solution can be carried out in n sub-steps which is given in the following algorithm.

Algorithm.

1. Solve $r_{11}^{(1)}[R^{(2)}]^T(\omega^{(1)}\otimes z^{(j)})=(h_1^{(1)}\otimes h_2^{(j)})$ by forward substitution.

2. Solve $r_{22}^{(1)}[R^{(2)}]^T=[h_1^{(2)}\otimes h_2^{(j)}]-r_{12}^{(1)}[R^{(2)}]^T[\omega^{(1)}\otimes z^{(j)}]$ by forward substitution.

3. Solve

$$r_{nn}^{(1)}[R^{(2)}]^T[\omega^{(n)}xz^{(j)})=(h_1^{(n)}\otimes h_2^{(j)})-\sum_{i=1}^{n-1} rin^{(1)}[R^{(2)}]^T(\omega^{(1)}\otimes z^{(j)})$$

by forward substitution.

Thus $(\bar{x}\otimes\bar{y})(n_0)$ can be completed without explicit II formulation of R by this two-step approach.

The vector $(h_1\otimes h_2)$ defined in (6) can be constructed as follows:

$$(A\otimes B)^T(\alpha\otimes\beta)=h_1\otimes h_2$$

or

$$(h_1\otimes h_2)=(I_mM)^T\otimes(Q_2R_2)^T(\alpha\otimes\beta)=(M^T\otimes R_2^T)(I_m\otimes Q_2^T)(\alpha\otimes\beta)=$$

$$=(M^T\otimes R_2^T)\begin{pmatrix} Q_2^T(\alpha^{(1)}\otimes\beta^{(l)}) \\ Q_2^T(\alpha^{(2)}\otimes\beta^{(l)}) \\ Q_2^T(\alpha^{(m)}\otimes\beta^{(l)}) \end{pmatrix}=(M^T\otimes R_2^T)(\alpha_1\otimes\beta_1),\ l=1,2,\ldots,p,$$

where

$$(\alpha_1\otimes\beta_1)=(I_m\otimes Q_2^T)(\alpha\otimes\beta)=$$

$$=((Q_1R_1)^T\otimes(I_pR_2)^T(\alpha_1\otimes\beta_1)=(R_1^T\otimes R_2^T)(Q_1^T\otimes I_p)(\alpha\otimes\beta)=$$

$$=(R_1^T\otimes R_2^T)\begin{pmatrix} q_{11}^{(1)}I_p & q_{12}^{(1)}I_p & \cdots & q_{1m}^{(1)}I_p \\ q_{21}^{(1)}I_p & q_{22}^{(1)}I_p & \cdots & q_{2m}^{(1)}I_p \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ q_{m1}^{(1)}I_p & q_{m2}^{(1)}I_p & \cdots & q_{mm}^{(1)}I_p \end{pmatrix}(\alpha_1\otimes\beta_1)=(R_1^T\otimes R_2^T)(\alpha_2\otimes\beta_2),$$

$$(\alpha_2\otimes\beta_2)=\begin{pmatrix} \alpha_2^{(1)}\otimes\beta_2^{(l)} \\ \alpha_2^{(2)}\otimes\beta_2^{(l)} \\ \cdots\cdots\cdots\cdots \\ \alpha_2^{(m)}\otimes\beta_2^{(l)} \end{pmatrix},$$

where

$$\alpha_2^{(k)} \otimes \beta_2^{(l)} = \sum_{r=1}^{m} q_{rk}^{(1)} (\alpha_1^{(k)} \otimes \beta_1^{(l)}), \quad k = 1, 2, \ldots, m,$$

$$\sum_{r=1}^{m} q_{rk}^{(1)} Q_2^T (\alpha^{(k)} \otimes \beta^{(l)}) = Q_2^T \sum_{r=1}^{m} q_{rk}^{(1)} (\alpha^{(k)} \otimes \beta^{(l)}) .$$

Therefore $(A \otimes B)^T (\alpha \otimes \beta) = (R_1^T \otimes R_2^T)(\alpha_2^{(k)} \otimes \beta_2^{(l)})$. Proceeding from here

$$(R_1^T \otimes R_2^T)(\alpha_2^{(k)} \otimes \beta_2^{(l)}) = \begin{pmatrix} R_2^T r_{11}^{(1)} (\alpha_2^{(1)} \otimes \beta_2^{(l)}) \\ R_2^T r_{12}^{(1)} (\alpha_2^{(1)} \otimes \beta_2^{(l)}) \\ + R_2^T r_{22}^{(1)} (\alpha_2^{(2)} \otimes \beta_2^{(l)}) \\ R_2^T \sum_{k=1}^{n} r_{kn}^{(1)} (\alpha_2^{(k)} \otimes \beta_2^{(l)}) \end{pmatrix} = \begin{pmatrix} h_1^{(1)} \otimes h_2^{(j)} \\ h_1^{(2)} \otimes h_2^{(j)} \\ h_1^{(n)} \otimes h_2^{(j)} \end{pmatrix},$$

i. e.

$$h_1^{(i)} \otimes h_2^{(j)} = R_2^T \sum_{k=1}^{l} r_{kj}^{(1)} (\alpha_2^{(k)} \otimes \beta_2^{(l)}) \quad \text{for } i = 1, 2, \ldots, n, \; j = 1, 2, \ldots, q.$$

Thus the vector $(h_1 \otimes h_2)$ can be computed block by block as needed without requiring the large matrix as claimed.

4. Modified Gram Schmidt process. In this section, we extend the method of modified Gram Schmidt process given in [7] to the Kronecker product system of equations. For let A be an $(m \times n)$ matrix with rank $r \le \min\{m, n\}$ and B be $a\,(p \times q)$ matrix with rank $s \le \min\{p, q\}$. Then there exists a factorization of the matrices A and B of the form $AP^1 = Q^1 R^1$ and $BP^2 = Q^2 R^2$, with the following properties:

1) P^1 and P^2 are $(n \times n)$ and $(q \times q)$ permutation matrices with the first r columns of AP^1 form a basis of $I_m(A)$ and the first q columns of BP^2 form a basis of $I_m(B)$;

2) Q^1 and Q^2 are $(m \times r)$ and $(p \times s)$ matrices both with orthnormal columns and R^1 and R^2 are $(r \times n)$ and $(s \times q)$ upper trapezoidal matrices to the form

$$R^1 = [R_1^{(1)} R_1^{(2)}] \text{ and } R^2 = [R_2^{(1)} R_2^{(2)}],$$

where $R_1^{(1)}$ and $R_1^{(2)}$ are non-singular $(r \times r)$ and $(s \times s)$ upper triangualar matrices and $R_2^{(1)}$ and $R_2^{(2)}$ are $(r \times n - r)$ and $(q \times q - s)$ matrices respectively.

Result 2. Let A and B be $(m\times n)$ and $(p\times q)$ matrices with ranks r and s respectively. Write $A=(a^1, a^2, ..., a^n)$ and $B=(b^1, b^2, ..., b^s, ..., b^q)$, where $a^i\in R^m$ and $b^j\in R^q$ then all the least square solutions of the Kronecker product system of equations can be obtained by solving the consistent Kronecker product system given by

$$(\bar{x}\otimes\bar{y})=[R_1^{(1)^{-1}}\otimes R_2^{(1)^{-1}}][(Q_1^*\otimes Q_2^*)(\alpha\otimes\beta)-(R_1^{(2)}\otimes R_2^{(2)})(v_1\otimes v_2)].$$

Proof. Consider the system of equations $(A\otimes B)(x\otimes y)=(\alpha\otimes\beta)$. Let P^1 and P^2 be permutation matrices such that $AP^1=Q^1R^1$ and $BP^2=Q^2R^2$. Then

$$(A\otimes B)(x\otimes y)=(Q_1P^{1^T}\otimes R_2P^{2^T})(x\otimes y)=(Q_1^*\otimes Q_2^*)$$

and therefore,

$$(\bar{x}\otimes\bar{y})=(P^1\otimes P^2)\begin{pmatrix}u_1\otimes u_2\\ v_1\otimes v_2\end{pmatrix}=\begin{pmatrix}P_1u_1\otimes P_2u_2\\ P_1v_1\otimes P_2v_2\end{pmatrix}.$$

Hence $(u_1\otimes u_2)=(R_1^{(1)}\otimes R_2^{(1)})(Q_1^*\otimes Q_2^*)(\alpha\otimes\beta)-R_1^{(2)}(v_1\otimes v_2)$, where $v_1\in R^{n-r}$ and $v_2\in R^{q-s}$. Note that a basic least square solution is obtained by taking $(v_1\otimes v_2)=(0\otimes 0)$.

5. Shortest vector problem. In this section, we shall be concerned with the search problems for lattices viewed as infinite point's sets. It is quite clear that general special circumstances, the methods presented in [8] can be modified to solve search problems for finite subsets of lattices. This will have many important applications in Communications. Since the invention of public key Cryptography in 1976, a new direction in Cryptography came into existence. This was mainly due to Diffe and Hellman [9] and security of most Cryptosystem is based on the hardness of factoring / computing discrete logarithm. In the year 1996 Ajtai [4] presented an efficiently computable function and it is hard to invent on the average if the underlying lattice problem is intractable. Further, Ajtai and Dwork [10] designed a public key Cryptosystem based on the ill conditioned hardness of a lattice problem. However, in the year 1998 Ngayen and Stern [5] showed that breaking the Ajtai C.Dwork Cryptosystem is unlikely NP-hard and for realistic theories of the parameter one may even reach the private key from public key. In this section, we use the method described by Ishay Haviv and Oded Regv [8] to improve the best least square solution obtained in section 4 in the process of finding shortest vector in R^{pq}. In literature there are two main computational problems associated in the lattices are the SVP and the CVP. In the first one, we are supposed to find a shortest non-zero vector in the lattices. The problem CVP is an inhomogeneous variant of SVP, in which given a lattice and some target point, one finds the close lattice point. The hardness of lattice problem is probably due to the fact that there are many possible bases for the same lattice.

Definition. A lattice is a discrete additive sub groups of R^n. Equivalently, fix $n \geq 1$. Let $S \subseteq R^m$ be a finite non-empty set. The lattice generates by *S* is the set of integer linear combinations of the elements in *S*, i.e.

$$L(b_1 ... b_n) = \left\{ \sum \alpha_i b_i : \alpha_i \in Z \text{ for all } 1 \leq i \leq m \right\}$$

of *m* linearly independent vectors $b_1, b_2, \ldots, b_n$ in R^n $(n \geq m)$. If rank *n* equals the dimension *m*, then we say that the lattice is of full rank.

The set $\{b_1, b_2, \ldots, b_n\}$ is called a basis of the lattice. Note that a lattice has many possible bases. We often represent a basis by an $(m \times n)$ matrix having the base vectors as columns, and we say that the basis *B* generates the lattice *L*. The determinant of a lattice *L* is given by

$$\det L(A) : \sqrt{\det A^T A},$$

where *A* is any basis with $L(A) = A$.

In this section we use two trapdoors given [8] for the shortest vector problem based on the tensor product of two full dimensional lattices, $L_1 \subseteq R^n$. For let $L = L_1 \otimes L_2$ denote the tensor product and $L_2 \subseteq R^q$ the lattice point $b := (b_1, b_2, \ldots$ $\ldots, b_{pq}) \in L$ can be written as a two dimensional array consisting of elements

$$\begin{array}{c}\begin{bmatrix} b_1 & b_2 & \cdots & b_q \\ b_{q+1} & b_{q+2} & \cdots & b_{2q} \\ \vdots & & & \\ b_{n-1,q+1} & b_{n-1,q+2} & \cdots & b_{nq} \end{bmatrix} \begin{array}{l} \in L_2 \\ \in L_2 \\ \\ \in L_2 \end{array} \\ \in L_1 \in L_1 \in L_1 \end{array}$$

so, that the column vectors belong to the lattice L_1 and the row vector to L_2. We have the following very important proposition.

Proposition. Suppose L_1, L_2 are any two full dimensional lattices then the following are true:

$$\dim(L_1 \otimes L_2) = \dim L_1, \dim L_2,$$

$$\dim(L_1 \otimes L_2) = (\det L_1)^{\dim L_2} (\det L_2)^{\dim L_1}.$$

Note. Let $B := (b_1, b_2, \ldots, b_q)$ be an ordered set containing *q* linearly independent column vectors in R^n then the set of all integral linear combinations of the vectors

$$L = L(B) := \sum_{i=1}^{m} (t_i b_i / t_i \in ZZ) = \sum_{i=1}^{qn} ZZ b_i$$

is called the lattice generated by the base B. Its dimension is dim L: = q and if p=q, we call it a full dimensional lattice. The vectors L are called lattice A lattice points L sub $\subseteq$ L with dim L sum = dim L, is called a sub lattice of L. Suppose L_1 be a sub lattice of ZZ^p and the elements are called integer lattices.

The lattice generated by the matrix A and L_2 be the lattice generated by the matrix B. Then the tensor product of L_1 and L_2 is defined as the mp dimensional lattice generated by $mp \times nq$ matrix $(A \otimes B)$ and is denoted by $L = L_1 \otimes L_2$. Equivalently, L is generated by the nq vectors obtained by taking the tensor product of two column vectors one from A and one from B. Let L_1 be the vectors obtained by taking the tensor of the two column vector $\bar{x}$ and $\bar{y}$. If we think of the vectors in L as $m \times p$ matrices, then we can define $L = L_1 \otimes L_2 = \{A \times B^T : x \in Z^{n \times q}\}$ with each entry in x corresponding to one of the nq generating vectors. In this section we are interested in the behavior of the shortest vector in a tensor product of lattices. For any two lattices L_1 and L_2, we have

$$\lambda_1^{(b)} L_1 \otimes L_1 \le \lambda_1^{(b)} L_1 \lambda_1^{(b)} L_2, \tag{7}$$

where $1 \le \rho < \infty$ [4]. Indeed for any two vectors $\bar{x}$ and $\bar{y}$ satisfying $(\bar{x} \otimes \bar{y})_p =$ $= \bar{x}_p \bar{y}_p$. Applying this to shortest non-zero vectors of L_1 and L_2, we get (7) Note that $\lambda_1^{(p)}(l)$ is the minimum L_p distance between two distinct points in the lattice L for any $p, 1 \le p < \infty$, The L_p norm of a vector $x \in R^q$ is defined as

$$\bar{x}_p = \left(\sum_{i=1}^{q} |x_i|^p \right)^{1/p}$$

and its L_∞ norm is denoted by $\bar{x}_\infty \max \bar{x}_i \lambda_i^{(p)}(L)$ is the L_p norm of a shortest non-zero vector:

$$\lambda_i^{(p)}(L) = \min\{r : \dim(\operatorname{span}(L \cap B_p(r)) \ge i\}.$$

Minkowski's first theorem: For any lattice L of rank r

$$\det(L) \ge \left(\frac{\lambda_i(L)}{\sqrt{r}} \right)^r.$$

For a full rank lattice $L \subseteq R^q$, its dual lattice denoted by L^* is defined as

$$L^* = \{x \in R^q / < x, y > \in z \text{ for all } y \in L\}.$$

And if $L = L^*$ we say that it is a self-dual lattice. It can easily be shortest if L is lattice generated by the basis B, then $(B^{-1})^T$ generates the lattice L^*.

Theorem 8. For any large q, there exists a q dimensional self-dual lattice L satisfying $\lambda_i\,(L \otimes L^*) \le \sqrt{q}$.

Proof. Let L be a lattice generated by a basis $B:=(b_1,\dots,b_q)$. Let $(B^{-1})^T=$ $=\{\bar{b}_1,\bar{b}_2,\dots,\bar{b}_q\}$ be the basis generated by the dual lattice L^*. Now the vector

$$e=\sum_{i=1}^{q} b_i\otimes\bar{b}_i\in L\otimes L^*.$$

This vector can be written as $BB^{-1}=I_q=BI_q((B^{-1})^T)^T$, or $B^{-1}B=I_q=$ $=((B^{-1})^T)^T I_q B$. And clearly has L_2 norm $\sqrt{q}$. The proof is complete. The shortest vector problem discussed above is of immense importance in practical applications.

Запропоновано критерій існування та єдиності розв'язку задачі кронекерового добутку з початковими умовами, яка пов'язана з узагальненою різницевою системою, що має матрицю першого порядку. Розроблено модифікований метод найменших квадратів і модифікований *QR* алгоритм для пошуку найкращого розв'язку кронекерового добутку матриць методом найменших квадратів. Встановлено, що при використанні цих методів для загального розв'язку задачі кронекерового добутку з початковими умовами її матриця початкових умов є переозначеною. З використанням методу, розробленого Ishey Haviv and Oded Regev, при визначенні задачі найкоротшого вектора покращено розв'язок методом найменших квадратів. Застосовано стандартний кронекерів добуток або тензорний добуток на сітках для збільшення коефіцієнта жорсткості.

1. *Fausett D. W., Fulton C. T.* Large Least Square Problem Involving Knocker Products// SIAM J. matrix Analysis and Applications. — 1994. — Vol 15, No 1. — P. 219—227.
2. *Brower J. W.* Kronecker Products and Matrix Calculus in System Theory// IEEE Trans. CVC System. — 1978. — Vol 25. — P. 772—781.
3. *Murty K.N., Shaw M.* On Kronecker Product Self Adjoint Boundary Value Problems// Engineering Simulation. — 2001. — Vol 18. — P. 475—488.
4. *Ajtai M.* Generating Hard Instance of Lattice Problems Quad// Mod. — 2004. — Vol 13. — P. 1—32. (Dept of Maths. Seconda univ. Napoli, Casetra).
5. *Nguyen P., Stevna J.* Crypto Analysis of the Ajtai Dwork Cryptosystem, Advances in Cryptology — Proc. Crypto '98', Lecture Notes in Computer Science. Vol 1294. — Berlin — Heidulburg: Springer — Verlag, 1998. — P. 223—242.
6. *Knot S.* Hardness of Approximating the Shortest Vector Problem in Lattices// J. of the ACM.— 2005. — Vol 52, No 5. — P. 789—808
7. *Atkinson K.* An Introduction to Numerical Analysis. Second Edition. — JohnWilley and Sons, 1987.
8. *Ias Hay Haviv, Odded Regev.* Tensor-based Hardness of the Shortest Vector Problem to Within Almost Polynomial Factors. Preprint. — March, 12. — 2007.
9. *Diffie W., Heleman M.* New Directions in Cryptography// IEEE Transactions of Information Theory. — 1976. — Vol 22, No 6. — P. 644—654.
10. *Ajtai M., Dwork C.* A Public Key Cryptosystem with the Worst Case / Average Case Equivalence// Proc. of the 29th Annual ACA symposium theory of computing (STOC). — ACM press. — 1997. — P. 293 — 193.

Поступила 15.02.08