Vakhlakov Dmitriy Vladimirivich – FGUP "NTC "Orion"; e-mail: melnikov@linfotech.ru; 38, Obraztsova street, build. 1, Moscow, 127018, Russia; phone/fax: +74952499053.

Peresypkin Vladimir Anatolyevich – cand. of eng. sc.

Melnikov Sergey Yurievich – Linfo LLC; e-mail: melnikov@linfotech.ru; 38, Obraztsova street, build. 1, Moscow, 127018, Russia; phone/fax: +74952499053, mobile: +79037222824; cand. of eng. sc.; mathematical engineer.

УДК 004.056.55 DOI 10.18522/2311-3103-2020-7-45-52

Е.И. Духнич, А.Г. Чефранов

АППАРАТУРНО-ОРИЕНТИРОВАННЫЙ АЛГОРИТМ ДЛЯ БЫСТРОГО УМНОЖЕНИЯ КРОНЕКЕРОВА ПРОИЗВЕДЕНИЯ МАТРИЦ НА ВЕКТОР

В статье на основе использования свойств произведения Кронекера (КП) матриц предлагается новый алгоритм для повышения эффективности выполнения операции умножения КП на вектор. Указанная операция широко применяется при решении задач обработки сигналов, изображений, криптографии и т.п., где выполняется формирование матриц большого размера с заданными свойствами с помощью КП матриц малого размера. При этом используются матрицы со следующими свойствами: ортогональные (унитарные), обращаемые, инволютивные. Умножение квадратной матрицы размера $n \times n$ на вектор имеет вычислительную сложность $O(n^2)$. Поэтому при росте количества элементарных матриц-сомножителей размер результирующей матрицы КП и сложность умножения ее на вектор растут экспоненциально. Это обстоятельство существенно повышает время решения прикладных задач. Целью предлагаемой работы является построение алгоритма, ориентированного на аппаратную реализацию и ускоряющего процессы формирования КП и умножения вектора на него. Предлагается совместить во времени эти процедуры. Таким образом матрица КП в явном виде фактически не рассчитывается. Вместо этого матрицы-сомножители КП итеративно умножаются на компоненты вектора за время $O(n\log_2 n)$ и требуют линейной сложности памяти. Приведена схема вычислений с топологией гиперкуба для возможной аппаратной реализации предлагаемого алгоритма, которая легко поддается конвейеризации. В разделе 1 приведены определения и свойства КП, используемые при синтезе предлагаемого алгоритма. В разделе 2 рассмотрен иллюстрирующий предлагаемый алгоритм пример с $n = 8$, на основе которого в разделе 3 предложена аппаратурно-ориентированная структура его реализации для произвольного n.

Алгоритм, произведение Кронекера; элементарная матрица; сложность вычислений; конвейерная реализация.

E.I. Dukhnich, A.G. Chefranov

HARDWARE-ORIENTED ALGORITHM FOR FAST MULTIPLICATION OF A VECTOR BY A MATRIX KRONECKER PRODUCT

The article discusses new algorithm to increase the efficiency of the operation of multiplying a matrix Kronecker product (KP) by a vector. It is based on the use of the KP properties. This operation is widely used in solving problems of processing signals, images, cryptography, etc., where the formation of large matrices with specified properties is performed using small size matrices. In this case, matrices with the following properties are used: orthogonal (unitary), invertible, involutive. Multiplying an $n \times n$ square matrix by a vector has a computational complexity of $O(n^2)$. Therefore, with an increase in the number of elementary matrix factors, the size of the resulting KP matrix and the complexity of multiplying it by a vector grow exponentially. This circumstance significantly increases the time for solving applied problems. The aim of the proposed work is to construct an algorithm that accelerates the processes of forming the KP and multiplying

the vector by it. It is proposed to combine the process of multiplication with the process of forming the KP. Thus, the KP matrix is not actually calculated explicitly. Instead, the KP factor matrices are iteratively multiplied by the vector components in $O(n\log_2 n)$ time with linear memory complexity. The computational scheme with the hypercube topology for the possible hardware implementation of the proposed algorithm is presented. It can be easily pipelined. Section 1 presents the definitions and properties of the KP used in the synthesis of the proposed algorithm. Section 2 presents an example with n = 8 illustrating the proposed algorithm, on the basis of which, in Section 3, a hardware-oriented structure of its implementation for arbitrary n is proposed.

Algorithm; Kronecker product; elementary matrix; computational complexity; pipeline implementation.

Введение. Кронекерово произведение (КП) матриц сходно с тензорным произведением и широко используется во многих приложениях, в том числе, при обработке сигналов и изображений [1–9]. Формирование матриц большого размера с заданными свойствами с помощью КП матриц малого размера может использоваться при разработке новых вычислительных алгоритмов. Для обработки сигналов и блочных криптографических алгоритмов используются матрицы со следующими свойствами: ортогональные (унитарные) [10], обращаемые [11], инволютивные [12, 13]. Умножение матрицы на вектор широко используется во многих приложениях, например, вращение объектов в мультимедиа-системах [14]. Очень важным направлением использования матричного произведения является шифрование информации [11, 13] и, в частности, медицинских DICOM изображений для телемедицины [15, 16].

Умножение квадратной матрицы размера $n \times n$ на вектор имеет вычислительную сложность $O(n^2)$ [17]. Размер КП элементарных матриц (ЭМ) может быть значительным, например, КП десяти ЭМ с $n = 10$ равен n^{10}, соответственно, умножение на вектор имеет сложность порядка 10^{20}. Известны эффективные алгоритмы выполнения умножения вектора на КП произвольных матриц [4-6], которые оптимизируют и организацию использования памяти системы. В [6] предложен эффективный алгоритм умножения КП произвольных матриц на вектор (далее, УКПВ), рассмотрена задача о выборе размера матриц, участвующих в КП, минимизирующего вычислительную сложность УКПВ, и показано, что минимальная сложность $O(n\log_2 n)$ достигается при использовании в КП элементарных квадратных матриц размера $n = 2$ [11]. На его основе в [11] предложен алгоритм быстрого УКПВ (АБУКПВ) вычисления УКПВ умножением очередной элементарной матрицы на части входного или промежуточного вектора. АБУКПВ допускает его параллельную реализацию за время $O(log_2 n)$.

В статье приведены определения и свойства КП, используемые АБУКПВ. Показан иллюстрирующий АБУКПВ пример с $n = 8$, на основе которого предложена аппаратурно-ориентированная структура его реализации для произвольного n, являющаяся гиперкубом [19, 20].

1. Кронекерово произведение матриц и его свойства. КП матриц $\boldsymbol{A}(\boldsymbol{m},\boldsymbol{n})$ и $\boldsymbol{B}(\boldsymbol{p},\boldsymbol{r})$ представляет собой блочную матрицу $(\boldsymbol{m}\cdot\boldsymbol{p},\boldsymbol{n}\cdot\boldsymbol{r})$ размера такую, что

$$(A \otimes B)_{ij} = A_{\lfloor (i-1)/p \rfloor+1,\,(\lfloor j-1)/r \rfloor+1} B_{(i-1)\bmod p+1,\,(j-1)\bmod r+1}, \quad (1)$$

$$i = \overline{1,mp}, j = \overline{1,nr},$$

где $\lfloor x \rfloor$ – целая часть x.

Из (1), если $m=n=p=r=2$, следует:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} = \\ = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

КП порядка K это произведение K элементарных матриц, $\boldsymbol{P}_j$. $j = \overrightarrow{1,K}$:

$$\boldsymbol{P} = \boldsymbol{P_1}\otimes(\boldsymbol{P_2}\otimes\ldots(\boldsymbol{P_{K-1}}\otimes\boldsymbol{P_K})\ldots) = \bigotimes_{j=1}^{K} P_j, \quad (2)$$

при этом размерности матриц:

$$sizeof(P_i) = (m_i, n_i),\ i = \overline{1,l}, \quad sizeof(P) = (\prod_{i=1}^{l} m_i, \prod_{i=1}^{l} n_i).$$

Свойство 1. Если A^{-1} и B^{-1} существуют, то

$$(A\otimes B)^{-1}=A^{-1}\otimes B^{-1}. \quad (3)$$

Свойство 2. Пусть $C(mp,nr) = A(m,n)\otimes B(p,r)$. Тогда сложность матрично-векторного умножения

$$Y(mp) = C(mp,nr)X(nr) \quad (4)$$

равна *O(mnpr)*, но может быть уменьшено до *O(npr + pmn)*, если использовать структуру КП матрицы *C*.

Доказательство: Рассмотрим алгоритм вычисления $Y = CX$, используя структуру КП. Из (1)**,**

$$Y_i = Y_{(i_1-1)p+i_2} = \sum_{j=1}^{nr} C_{ij}X_j = \sum_{j_1=1}^{n}\sum_{j_2=1}^{r} A_{i_1j_1}B_{i_2j_2}X_{(j_1-1)r+j_2} = \\ \sum_{j_1=1}^{n} A_{i_1j_1}Y^1_{(j_1-1)r+i_2}, \quad (5)$$

где

$$i_1 = \lfloor (i-1)/p \rfloor + 1, i_2 = (i-1) \bmod p + 1,$$
$$j_1 = \lfloor (j-1)/r \rfloor + 1,\ j_2 = (j-1) \bmod r + 1$$
$$Y^1_{(j_1-1)r+i_2} = \sum_{j_2=1}^{r} B_{i_2j_2}X_{(j_1-1)r+j_2},\ i = \overrightarrow{1,mp}, j = \overrightarrow{1,nr}. \quad (6)$$

Из (5), (6) следует, что сложность вычисления (6) равна *O(nrp)*, а сложность вычисления (5), с помощью Y^1 из (6), равна *O(mnp)*. Таким образом, сложность вычисления (4) равна *O(nrp)+O(mnp)=O(pn(m+r))*, ЧТД.

Из Свойства 2 следует

*Следствие 1***.** Вычислительная сложность УКПВ (4) *K=2* при *m=n=p=r* равна

$$BC\_KП(2,m)=O(2m^3). \quad (7)$$

2. Пример КП порядка $\boldsymbol{n = 8, K = log_2 n = 3}$. АБУКПВ основан на использовании Свойства 2. Рассмотрим вычисление

$$\boldsymbol{Y = (A\otimes B\otimes C)\cdot X = (A\otimes(B\otimes C))\cdot X}. \quad (8)$$

При размерности матриц-сомножителей $m \times m$, где *m*=2, выражение (8) можно представить как

$$(y1, y2, y3, y4, y5, y6, y7, y8)^{Tr} =$$

$$= \begin{pmatrix} a11\begin{pmatrix} b11\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x1 \\ x2 \end{pmatrix} + & b12\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x3 \\ x4 \end{pmatrix} \\ b21\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x1 \\ x2 \end{pmatrix} + & b22\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x3 \\ x4 \end{pmatrix} \end{pmatrix} + \\ +a12\begin{pmatrix} b11\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x5 \\ x6 \end{pmatrix} + & b12\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x7 \\ x8 \end{pmatrix} \\ b21\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x5 \\ x6 \end{pmatrix} + & b22\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x7 \\ x8 \end{pmatrix} \end{pmatrix} \\ a21\begin{pmatrix} b11\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x1 \\ x2 \end{pmatrix} + & b12\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x3 \\ x4 \end{pmatrix} \\ b21\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x1 \\ x2 \end{pmatrix} + & b22\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x3 \\ x4 \end{pmatrix} \end{pmatrix} + \\ +a22\begin{pmatrix} b11\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x5 \\ x6 \end{pmatrix} + & b12\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x7 \\ x8 \end{pmatrix} \\ b21\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x5 \\ x6 \end{pmatrix} + & b22\begin{pmatrix} c11 & c12 \\ c21 & c22 \end{pmatrix}\cdot\begin{pmatrix} x7 \\ x8 \end{pmatrix} \end{pmatrix} \end{pmatrix} X \quad (9)$$

Видим, что в правой части (9) каждая матрица С четыре раза умножается на одну и ту же часть вектора X (из четырех). Умножая, получаем:

$$\begin{pmatrix} a11\begin{pmatrix} b11\begin{pmatrix} y1^3 \\ y2^3 \end{pmatrix} + & b12\begin{pmatrix} y3^3 \\ y4^3 \end{pmatrix} \\ b21\begin{pmatrix} y1^3 \\ y2^3 \end{pmatrix} + & b22\begin{pmatrix} y3^3 \\ y4^3 \end{pmatrix} \end{pmatrix} + a12\begin{pmatrix} b11\begin{pmatrix} y5^3 \\ y6^3 \end{pmatrix} + & b12\begin{pmatrix} y7^3 \\ y8^3 \end{pmatrix} \\ b21\begin{pmatrix} y5^3 \\ y6^3 \end{pmatrix} + & b22\begin{pmatrix} y7^3 \\ y8^3 \end{pmatrix} \end{pmatrix} \\ a21\begin{pmatrix} b11\begin{pmatrix} y1^3 \\ y2^3 \end{pmatrix} + & b12\begin{pmatrix} y3^3 \\ y4^3 \end{pmatrix} \\ b21\begin{pmatrix} y1^3 \\ y2^3 \end{pmatrix} + & b22\begin{pmatrix} y3^3 \\ y4^3 \end{pmatrix} \end{pmatrix} + a22\begin{pmatrix} b11\begin{pmatrix} y5^3 \\ y6^3 \end{pmatrix} + & b12\begin{pmatrix} y7^3 \\ y8^3 \end{pmatrix} \\ b21\begin{pmatrix} y5^3 \\ y6^3 \end{pmatrix} + & b22\begin{pmatrix} y7^3 \\ y8^3 \end{pmatrix} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} y1 \\ y2 \\ y3 \\ y4 \\ y5 \\ y6 \\ y7 \\ y8 \end{pmatrix}, \quad (10)$$

где

$$y1^3 = c11 \cdot x1 + c12 \cdot x2,\ y2^3 = c21 \cdot x1 + c22 \cdot x2,\ y3^3 = c11 \cdot x3 + \\ + c12 \cdot x4,\ y4^3 = c21 \cdot x3 + c22 \cdot x4,\ y5^3 = c11 \cdot x5 + c12 \cdot x6,\ y6^3 = \\ = c21 \cdot x5 + c22 \cdot x6,\ y7^3 = c11 \cdot x7 + c12 \cdot x8, y8^3 = c21 \cdot x7 + c22 \cdot x8.$$

Переставляя ряды в левой части и элементы вектора в правой части (10), получаем

$$\begin{pmatrix} a11\begin{pmatrix} \begin{pmatrix} b11 & b12 \\ b21 & b22 \end{pmatrix}\begin{pmatrix} y1^3 \\ y3^3 \end{pmatrix} \\ \begin{pmatrix} b11 & b12 \\ b21 & b22 \end{pmatrix}\begin{pmatrix} y2^3 \\ y4^3 \end{pmatrix} \end{pmatrix} + a12\begin{pmatrix} \begin{pmatrix} b11 & b12 \\ b21 & b22 \end{pmatrix}\begin{pmatrix} y5^3 \\ y7^3 \end{pmatrix} \\ \begin{pmatrix} b11 & b12 \\ b21 & b22 \end{pmatrix}\begin{pmatrix} y6^3 \\ y8^3 \end{pmatrix} \end{pmatrix} \\ a21\begin{pmatrix} \begin{pmatrix} b11 & b12 \\ b21 & b22 \end{pmatrix}\begin{pmatrix} y1^3 \\ y3^3 \end{pmatrix} \\ \begin{pmatrix} b11 & b12 \\ b21 & b22 \end{pmatrix}\begin{pmatrix} y2^3 \\ y4^3 \end{pmatrix} \end{pmatrix} + a22\begin{pmatrix} \begin{pmatrix} b11 & b12 \\ b21 & b22 \end{pmatrix}\begin{pmatrix} y5^3 \\ y7^3 \end{pmatrix} \\ \begin{pmatrix} b11 & b12 \\ b21 & b22 \end{pmatrix}\begin{pmatrix} y6^3 \\ y8^3 \end{pmatrix} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} y1 \\ y3 \\ y2 \\ y4 \\ y5 \\ y7 \\ y6 \\ y8 \end{pmatrix} \quad (11)$$

В (11) каждая матрица В умножается два раза на одну и ту же часть вектора X. Умножая, получаем:

$$\begin{pmatrix} a11\begin{pmatrix} \begin{pmatrix} y1^2 \\ y2^2 \end{pmatrix} \\ \begin{pmatrix} y3^2 \\ y4^2 \end{pmatrix} \end{pmatrix} + a12\begin{pmatrix} \begin{pmatrix} y5^2 \\ y6^2 \end{pmatrix} \\ \begin{pmatrix} y7^2 \\ y8^2 \end{pmatrix} \end{pmatrix} \\ a21\begin{pmatrix} \begin{pmatrix} y1^2 \\ y2^2 \end{pmatrix} \\ \begin{pmatrix} y3^2 \\ y4^2 \end{pmatrix} \end{pmatrix} + a22\begin{pmatrix} \begin{pmatrix} y5^2 \\ y6^2 \end{pmatrix} \\ \begin{pmatrix} y7^2 \\ y8^2 \end{pmatrix} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} y1 \\ y3 \\ y2 \\ y4 \\ y5 \\ y7 \\ y6 \\ y8 \end{pmatrix}, \quad (12)$$

где

$$y1^2 = b11 \cdot y1^3 + b12 \cdot y3^3,\ y2^2 = b21 \cdot y1^3 + b22 \cdot y3^3,\ y3^2 =$$
$$= b11 \cdot y2^3 + b12 \cdot y4^3,\ y4^2 = b21 \cdot y2^3 + b22 \cdot y4^3,\ y5^2 = b11 \cdot y5^3 + +b12 \cdot y7^3,$$
$$y6^2 = b21 \cdot y5^3 + b22 \cdot y7^3,\ y7^2 = b11 \cdot y6^3 + b12 \cdot y8^3,\ y8^2 = b21 \cdot y6^3 + b22 \cdot y8^3.$$

Переставляя ряды матрицы в левой части и соответствующие элементы вектора в правой части (12), получаем

$$\begin{pmatrix} \begin{pmatrix} a11 & a12 \\ a21 & a22 \end{pmatrix} \cdot \begin{pmatrix} y1^2 \\ y5^2 \end{pmatrix} \\ \begin{pmatrix} a11 & a12 \\ a21 & a22 \end{pmatrix} \cdot \begin{pmatrix} y2^2 \\ y6^2 \end{pmatrix} \\ \begin{pmatrix} a11 & a12 \\ a21 & a22 \end{pmatrix} \cdot \begin{pmatrix} y3^2 \\ y7^2 \end{pmatrix} \\ \begin{pmatrix} a11 & a12 \\ a21 & a22 \end{pmatrix} \cdot \begin{pmatrix} y4^2 \\ y8^2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} y1^1 \\ y2^1 \\ y3^1 \\ y4^1 \\ y5^1 \\ y6^1 \\ y7^1 \\ y8^1 \end{pmatrix} = \begin{pmatrix} y1 \\ y5 \\ y2 \\ y6 \\ y3 \\ y7 \\ y4 \\ y8 \end{pmatrix}. \quad (13)$$

В (13) каждая матрица А умножается теперь однократно на каждую из четырех частей вектора X.

3. Вычислительная схема для реализации АБУКПВ. Преобразования (9)–(13) можно представить в виде схемы на рис. 1, где все матрицы A, B, C обозначены прямоугольниками и для каждого из четырех экземпляров каждой из этих матриц указаны соответствующие входные и выходные данные.

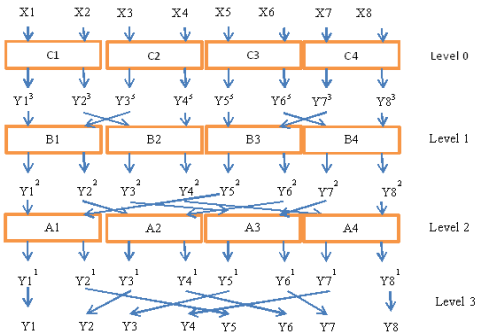

Рис. 1. Схема вычислений

На рис. 2 представлена эта же схема УКПВ, но уже с двоичными номерами входов и выходов каждого блока умножения.

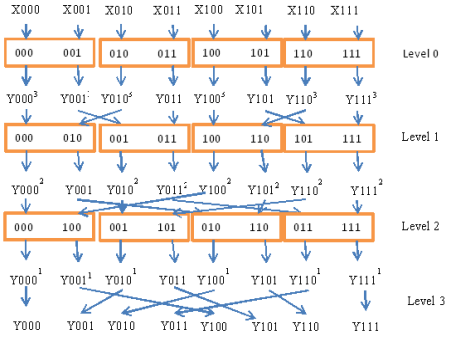

Рис. 2. Схема УКПВ с указанием двоичных номеров входов и выходов блоков умножения

Можно видеть, что схема УКПВ имеет $log_2 n = 3$ уровня, в каждом по $\frac{n}{2} = 4$ схемы матричного 2×2 умножения. Внутри прямоугольника каждой схемы проставлены два кода, которые показывают, какие компоненты выходного вектора предыдущего уровня соединены с этими входами. Можно видеть, что на рис. 2 соединены входы-выходы соседних уровней с одинаковыми номерами. На уровне 3 показаны окончательные значения результирующего вектора *Y*.

Схема УКПВ для $n = 2^K$ имеет $log_2 n = K$ уровней с $\frac{n}{2}$ матричными 2×2 умножителями, пронумерованными в каждом уровне $l = 0..K-1$ от 0 до $\frac{n}{2} - 1$ $(K-1)$-битными двоичными числами. При этом входы/выходы схемы с номером $i_{K-2}..i_0$ уровня l отличаются значением l-го бита с остальными битами со значениями бит из номера схемы, причем взаимный порядок этих бит в номере входа/выхода тот же, что и в номере схемы. Соединены между собой входы и выходы схем соседних уровней с одинаковыми номерами. Входы схем уровня 0 соединены с элементами входного вектора с теми же номерами. Выходы схем последнего уровня соединены с элеменами результирующего вектора с теми же номерами. Такой порядок соединений характерен для гиперкубов. При использовании физически параллельных схем матричного умножения время УКПВ имеет порядок $O(K) = O(log_2 n)$. При использовании схемы УКПВ в конвейерном режиме результаты выдаются с задержкой порядка $O(1)$ после заполнения конвейера.

Заключение. На основе предложенного метода ускоренного умножения кронекерова произведения матриц на вектор представлены аппаратурно-ориентированные вычислительные структуры, которые существенно повышают его эффективность за счет исключения предварительного отдельного вычисления КП и отсутствия необходимости хранения в памяти его результирующей матрицы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Van Loan C.F*. The ubiquitous Kronecker product // Journal of Computational and Applied Mathematics. – 2000. – No. 123. – P. 85-100.
2. *Jemderson H.V., Pukelsheim F., and Searle S.R.* On the history of the Kronecker product // Linear and Multilinear Algebra. – 1983. – Vol. 14, No. 2. – P. 113-120.
3. *Graham A.* Kronecker Products and Matrix Calculus with Applications (Dover Books on Mathematics), Dover Publications, 2018.
4. *Buchholz P., Ciardo G., Donatelli S., Kemper P.* Complexity of memory-efficient Kronecker operations with applications to the solution of Markov models // INFORMS J. Comput. – 2000. – P. 203-222.
5. *Tadonki C., Philippe B.* Parallel multiplication of a vector by a Kronecker product of matrices // Journal of Parallel and Distributed Computing and Practices. – 2000. – No. 3 (3). – P. 1-11.
6. *Tadonki C.* Large-scale Kronecker product on supercomputers // 2011 Second Workshop on Architecture and Multi-Core Applications (WAMCA 2011). 26-27 Oct. 2011. – Victoria, Brazil. IEEE. – P. 1-4.
7. *Doukhnitch E., Strelnikov O., Andreev A.,* Application of Kronecker Matrix Product for the Synthesis of Hardware-oriented DSP Algorithms // in Proc. of Intern. Conf. on Signal Proc. “DSPA-99”, Moscow, Sept. 1999. – P. 78-83.
8. *Doukhnitch E., Salamah M., Andreev A.* Effective Processor for Matrix Decomposition // Arabian Journal for Science and Engineering. – March 2014. – Vol. 39, Issue 3. – P. 1797-1804.
9. *Dayar T., Orhan M.C.* On vector-Kronecker product multiplication with rectangular factors // SIAM J. Sci. Comput. – 2015. – Vol. 37 (5). – P. S526-S543.
10. *Koukouvinos C., Lappas E., Simos D.E.* Encryption schemes using orthogonal arrays // Journal of Discrete Mathematical Sciences and Cryptography. – 2009. – No. 12 (5). – P. 615-628.
11. *Chefranov A., Dukhnich E.* One-time Kronecker product-based Hill cipher modification // International Journal of Information Assurance and Security. – 2017. – No. 12 (3). – P. 94-103.
12. *Lancaster P. and Tismenetsky M.,* The Theory of Matrices. – 2nd ed. – Orlando, Florida: AcademicPress, 1985.

13. *Chefranov A., Dukhnich E., Shapel A.* One-Time Involutory Matrix-Based Hill Cipher Modification // International Journal of Information Assurance and Security (JIAS). – 2020. – Vol. 15, No. 4. – P. 165-174.
14. *Джамбруно М.* Трехмерная (3D) графика и анимация. – М.: Вильямс, 2002. – 640 с.
15. *Dzwonkowski M., Rykaczewski R.* Secure quaternion Feistel cipher (S-QFC) for DICOM images // IEEE Transactions on Image Processing. – 2019. – Vol. 28, No. 1. – P. 371-380.
16. *Dzwonkowski M., Papaj M., Rykac R.* A new quaternion-based encryption method for DICOM Images // IEEE Transactions on Image Processing. – 2015. – Vol. 24, No. 11. – P. 4614-4522.
17. *Гантмахер Ф.Р.* Теория матриц. – М.: Главная редакция физико-математической литературы издательства "Наука", 1966.
18. *Blair Jeffrey S.* The Biomedical Engineering handbook. CRC Press Taylor & Francis Group, New York, 2006. – P. 42-4–42-5.
19. *Deng Y., Guo M., Ramos A.F., et al.* Optimal low-latency network topologies for cluster performance enhancement // J. Supercomput. Published online 02 March 2020. – https://doi.org/10.1007/s11227-020-03216-y.
20. *Hayes J.P., Mudge T.* Hypercube supercomputers // Proceedings of the IEEE. – 1989. – Vol. 77 (12). – P. 1829-1841.

REFERENCES

1. *Van Loan C.F.* The ubiquitous Kronecker product, *Journal of Computational and Applied Mathematics*, 2000, No. 123, pp. 85-100.
2. *Jemderson H.V., Pukelsheim F., and Searle S.R.* On the history of the Kronecker product, *Linear and Multilinear Algebra*, 1983, Vol. 14, No. 2, pp. 113-120.
3. *Graham A.* Kronecker Products and Matrix Calculus with Applications (Dover Books on Mathematics), Dover Publications, 2018.
4. *Buchholz P., Ciardo G., Donatelli S., Kemper P.* Complexity of memory-efficient Kronecker operations with applications to the solution of Markov models, *INFORMS J. Comput*., 2000, pp. 203-222.
5. *Tadonki C., Philippe B.* Parallel multiplication of a vector by a Kronecker product of matrices, *Journal of Parallel and Distributed Computing and Practices*, 2000, No. 3 (3), pp. 1-11.
6. *Tadonki C.* Large-scale Kronecker product on supercomputers, *2011 Second Workshop on Architecture and Multi-Core Applications (WAMCA 2011). 26-27 Oct. 2011*. Victoria, Brazil. IEEE, pp. 1-4.
7. *Doukhnitch E., Strelnikov O., Andreev A.,* Application of Kronecker Matrix Product for the Synthesis of Hardware-oriented DSP Algorithms, *in Proc. of Intern. Conf. on Signal Proc. "DSPA-99", Moscow, Sept. 1999*, pp. 78-83.
8. *Doukhnitch E., Salamah M., Andreev A.* Effective Processor for Matrix Decomposition, *Arabian Journal for Science and Engineering*, March 2014, Vol. 39, Issue 3, pp. 1797-1804.
9. *Dayar T., Orhan M.C.* On vector-Kronecker product multiplication with rectangular factors, *SIAM J. Sci. Comput*., 2015, Vol. 37 (5), p. S526-S543.
10. *Koukouvinos C., Lappas E., Simos D.E.* Encryption schemes using orthogonal arrays, *Journal of Discrete Mathematical Sciences and Cryptography*, 2009, No. 12 (5), pp. 615-628.
11. *Chefranov A., Dukhnich E.* One-time Kronecker product-based Hill cipher modification, *International Journal of Information Assurance and Security*, 2017, No. 12 (3), pp. 94-103.
12. *Lancaster P. and Tismenetsky M.,* The Theory of Matrices. 2nd ed. Orlando, Florida: AcademicPress, 1985.
13. *Chefranov A., Dukhnich E., Shapel A.* One-Time Involutory Matrix-Based Hill Cipher Modification, *International Journal of Information Assurance and Security (JIAS)*, 2020, Vol. 15, No. 4, pp. 165-174.
14. *Dzhambruno M.* Trekhmernaya (3D) grafika i animatsiya [3D Graphics &Animation]. Moscow: Vil'yams, 2002, 640 p.
15. *Dzwonkowski M., Rykaczewski R.* Secure quaternion Feistel cipher (S-QFC) for DICOM images, *IEEE Transactions on Image Processing*, 2019, Vol. 28, No. 1, pp. 371-380.
16. *Dzwonkowski M., Papaj M., Rykac R.* A new quaternion-based encryption method for DICOM Images, *IEEE Transactions on Image Processing*, 2015, Vol. 24, No. 11, pp. 4614-4522.
17. *Gantmakher F.R.* Teoriya matrits [The theory of matrices]. Moscow: Glavnaya redaktsiya fiziko-matematicheskoy literatury izdatel'stva "Nauka", 1966.

18. *Blair Jeffrey S.* The Biomedical Engineering handbook. CRC Press Taylor & Francis Group, New York, 2006, pp. 42-4–42-5.
19. *Deng Y., Guo M., Ramos A.F., et al.* Optimal low-latency network topologies for cluster performance enhancement, *J. Supercomput. Published online 02 March 2020*. Available at: https://doi.org/10.1007/s11227-020-03216-y.
20. *Hayes J.P., Mudge T.* Hypercube supercomputers, *Proceedings of the IEEE,* 1989, Vol. 77 (12), pp. 1829-1841.

Статью рекомендовал к опубликованию д.т.н., профессор Ю.М. Вишняков.

Духнич Евгений Иванович – Государственный Морской университет имени адмирала Ф.Ф. Ушакова; e-mail: evgenydukhnich@gmail.com; г. Новороссийск, Россия; тел.: +79184907411; кафедра радиоэлектроники и информационных технологий; д.т.н.; профессор.

Чефранов Александр Гергиевич – Восточный Средиземноморский университет; e-mail: alexander.chefranov@emu.edu.tr; г. Фамагуста, С. Кипр; тел.: +05338673790; кафедра компьютерных технологий; д.т.н.; профессор.

Dukhnich Evgeny Ivanovich – Novorossiysk State Maritime University; e-mail: evgenydukhnich@gmail.com; Novorossiysk, Russia; phone: +79184907411; the department of radio-electronics and information technologies; dr. of eng. sc.; professor.

Chefranov Alexander Georgievich – Eastern Mediterranean University, e-mail: alexander.chefranov@emu.edu.tr; t. Famagusta, N. Cyprus; phone: +05338673790; the department of computer engineering; dr. of eng. sc.; professor.

УДК 519.224.22 DOI 10.18522/2311-3103-2020-7-52-67

А.К. Мельников

АЛГОРИТМИЧЕСКАЯ СЛОЖНОСТЬ РАСЧЕТА ТОЧНЫХ ПРИБЛИЖЕНИЙ РАСПРЕДЕЛЕНИЙ ВЕРОЯТНОСТЕЙ ЗНАЧЕНИЙ СТАТИСТИК МЕТОДОМ РЕШЕНИЯ УРАВНЕНИЯ ПЕРВОЙ КРАТНОСТИ ТИПОВ

Рассматривается алгоритмическая сложность расчета точных распределений вероятностей значений статистик и их точных приближений методом решения уравнения первой кратности. В качестве точных приближений распределений вероятностей значений статистик рассматриваются их Δ–точные распределения, отличающиеся от точных распределений не более чем на заранее заданную, сколь угодно малую величину Δ. Показывается, что основой метода расчета точных распределений вероятностей значений статистик является перечисление элементов области поиска решений линейного уравнения кратности типов, составленной из векторов кратности типов, каждый элемент которого представляет собой число вхождений элементов определенного типа (какого-либо знака алфавита) в рассматриваемую выборку. Одновременно показывается, что для расчета точных приближений распределения вероятностей значений статистик применяется метод ограничения области поиска решений. Приводится выражение определяющее алгоритмическую сложность вычисления точных распределений методом решения уравнения первой кратности. Приведенное выражение является конечным и позволяет для каждого значения мощности алфавита определить максимальный объем выборки, для которой при использовании ограниченного вычислительного ресурса методом решения уравнения первой кратности могут быть рассчитаны точные распределения. Определена область параметров, представляемых объемом выборок и мощностью алфавита, для которых при ограниченном вычислительном ресурсе могут быть рассчитаны точные распределения. Для оценки алгоритмической сложности расчета точных приближений распределений приводится, впервые полученное, выражение для числа решений уравнения первой кратности с ограничением на значения координат векторов решений. Приводится выражение