тем за заг. ред. д.т.н., професора І. Д. Горбенко. Харків: Видавництво «Форт», 2016. 960 с.
2. Горбенко І. Д., Гріненко Т. О., Нарєжній О. П. Методика вимірювання спектральної щільності потужності шума квантової радіооптичної системи генератора випадкових чисел. *Радиотехника: всеукр. межвед. науч.-техн. сб.* Харьков: ХТУРЕ, 2016. Вып. 186. С. 172-183.
3. Gorbenko Y., Grinenko T. A pseudorandom sequences generator based on the multimodulo transformation. Computer science and cybersecurity. International electronic scientific journal. 2016 Issue. 1(1). P. 5-19, [Електронний ресурс]. Режим доступу: http://periodicals.karazin.ua/cscs/article/view/6194/5739.

In general form it is stated and solved the task of synthesis and analysis of extractor algorithm on the multi-module transformation with alphabet basis greater than two for prospective quantum random numbers generator (QRNG). The work was lead within a framework of complex theoretical and experimental researches for creation of QRNG prototype based on double radio-optic resonance in alkaline metal pairs.

Key words: *quantum random numbers generator; physical quantum noise; extractor of quantum random numbers generator; computation complexity of the algorithm.*

Одержано 05.03.2017

УДК 519.6

М. О. Недашковський*, д-р фіз.-мат. наук, професор,
Т. І. Крошка,** старший викладач

*Університет Казимира Великого, м. Бидгощ, Польща,
**Буковинський державний фінансово-економічний університет, м. Чернівці

РОЗВ'ЯЗУВАННЯ МАТРИЧНИХ ПОЛІНОМІАЛЬНИХ РІВНЯНЬ ІЗ ВЕКТОРНИМИ НЕВІДОМИМИ

Пропонуються нові обчислювальні схеми розв'язання поліноміальних матричних рівнянь з векторними невідомими за допомогою ланцюгових дробів.

Ключові слова: *поліноміальні матричні рівняння, ланцюгові дроби.*

Вступ. У роботах В. С. Григорківа [1–4] було розглянуто пряму нелінійну балансову модель міжгалузевої еколого-економічної взаємодії а також двоїсту до неї модель відносно цін. Аторами показано [5], що ця нелінійна модель зводиться до поліноміального матричного рівняння із векторними невідомими вигляду

$$A_n diag(X)^{n-1} X + A_{n-1} diag(X)^{n-2} X + ... + A_1 X + B = 0\,. \qquad (1)$$

Тут A_i $(i = 1, 2, ..., n)$ — квадратні матриці розмірністю $m \times m$, а X — вектори розміру m. Однак, до останнього часу ефективних методів для подібних рівнянь не було відомо.

Пропонуються дві схем розв'язання рівнянь виду (1).

СХЕМА 1. Розлядається рівняння 3-го порядку

$$A_3\left(diag(X)\right)^2 X + A_2\left(diag(X)\right)X + A_1X + B = 0\ . \qquad (2)$$

На його основі після нескладного перетворення

$$\left(A_3(diag(X))^2 + A_3diag(X) + (A_2 - A_3)\cdot diag(X) + A_1\right)X + B = 0\ . \quad (3)$$

Введемо тепер позначення

$$Y = A_3\left(E\cdot diag(X)\right)^2 + A_3\left(E\cdot diag(X)\right)^{-1}.$$

Тоді $\left(Y^{-1} + (A_2 - A_3)diag(X) + A_1\right)X + B = 0$.

Звідки отримуємо рекурентне співвідношення для X

$$X = -\left(A_1 + (A_2 - A_3)diag(X) + Y^{-1}\right)^{-1}B\ .$$

А для обчислення Y у свою чергу можна записати

$$Y = \left(A_3(diag(X))^2 + A_3\cdot diag(X)\right)^{-1} = \left(A_3\left(diag(X) + E\right)\left(diag(X)\right)\right)^{-1}.$$

Далі

$$\left(A_3(diag(X) + E)(diag(X))\right)^{-1} = \left(diag(X)\right)^{-1}\left(diag(X) + E\right)^{-1}A_3^{-1}.$$

Звідки $Y = [diag(X)]^{-1}[diag(X) + E]^{-1}A_3^{-1}$.

З іншого боку

$$[diag(X)]^{-1} - [diag(X) + E]^{-1} = \left[diag(X)\right]^{-1}\left[diag(X) + E - diag(X)\right]\times$$

$$\times\left[diag(X) + E - diag(X)\right]^{-1} = [E\cdot diag(X)]^{-1}E[diag(X)] + E]^{-1}.$$

Звідки негайно випливає, що

$$Y = \left(\left(diag(X)\right)^{-1} - \left(diag(X) + E\right)^{-1}\right)A_3^{-1}.$$

Отже, ітераційний процес можна проводити за співвідношеннями

$$Y^{k+1} = \left(\left(diag(X^k)\right)^{-1} - \left(diag(X^k) + E\right)^{-1}\right)A_3^{-1},$$

$$X^{k+1} = -\left(A_1 + (A_2 - A_3)diag(X^k) + (Y^k)^{-1}\right)^{-1}B\ .$$

Звідки $(Y^{k+1})^{-1} = A_3\left(\left(diag(X^k)\right)^{-1} - \left(diag(X^k) + E\right)^{-1}\right)^{-1}$.

Об'єднуючи разом рекурентні формули для обчислення X^{k+1} та Y^{k+1} можна записати наступну ітераційну схему:

$$X^{k+1}=\left(A_1+(A_2-A_3)diag(X^k)+A_3\left(\left(diag(X^k)\right)^{-1}-\left(diag(X^k)+E\right)^{-1}\right)^{-1}\right)^{-1}B.$$

Послідовне застосування закону композиції для X^{k+1} дає наступне розвинення X в одно періодичний гіллястий ланцюговий дріб з двома вітками розгалуження.

$$X=-\Big(A_1+(A_2-A_3)diag((-(A_1+...)^{-1}B)^k)+$$

$$+A_3((diag((-(A_1+...)^{-1}B)^k))^{-1}-(diag((-(A_1+...)^{-1}B)^k)+E)^{-1})^{-1}\Big)^{-1}$$

Приклад 1. Розглянемо як ілюстрацію ефективності даної схеми матричне рівняння 3-го порядку

$$A_3\left(diag(X)\right)^2X+A_2\left(diag(X)\right)X+A_1X+B=0\,, \tag{4}$$

де

$$A_3=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix};\ A_2=\begin{pmatrix}2.012&-3.4&-5.03\\2.2&2.51&0.25\\2&-2.34&-0.13\end{pmatrix};\ A_1=\begin{pmatrix}0.979&5.968&-5.0\\0.245&2.2&0.251\\2.34&-1.3&0.212\end{pmatrix};$$

$$B=\begin{pmatrix}33.0099&-7.1837&-8.9359\end{pmatrix}^T.$$

За допомогою пакету MatLab це матричне рівняння розв’язувалося з використанням рекурентної формули

$$X^{k+1}=\left(A_1+(A_2-A_3)diag(X^k)+A_3\left(\left(diag(X^k)\right)^{-1}-\left(diag(X^k)+E\right)^{-1}\right)^{-1}\right)^{-1}B.$$

В результаті обчисленнь при початковому наближенні

$$X_0=\begin{pmatrix}-1.21&0.61&2.2\end{pmatrix}^T$$

отримано наближений розв'язок

$$X_k=\begin{pmatrix}0.3689&0.9258&2.2352\end{pmatrix}^T.$$

Результати експерименту наведені в табл. 1.

Таблиця 1

$\lVert X_k-X_{k-1}\rVert/\lVert X_k\rVert$	Кількість ітерацій	Величина нев'язки
1.000000e-004	48	8.153217e-004
1.000000e-005	56	8.351903e-005
1.000000e-006	64	8.560547e-006
1.000000e-007	72	8.767670e-007
1.000000e-008	80	8.983232e-008
1.000000e-009	88	9.202762e-009
1.000000e-010	97	7.091406e-010
1.000000e-011	105	7.266972e-011

На жаль, дану схему поки що не вдається узагальнити на випадок рівняння n -го порядку.

СХЕМА 2. Для рівняння (1) 3-го порядку можна також записати

$$\left(A_3 diag(X)^2 + A_2 diag(X) + A_1\right)X + B = 0 .$$

І далі $\left(\left(A_3 diag(X) + A_2\right) diag(X) + A_1\right)X + B = 0$.

Якщо тепер ввести позначення $Y = \left(A_2 + A_3 diag(X)\right)^{-1}$, то для обчислення X можна записати $\left(Y^{-1} \cdot diag(X) + A_1\right)X + B = 0$.

Звідки $X = -\left(A_1 + Y^{-1} \cdot diag(X)\right)^{-1} B$.

Отже, підрахунок значення X може бути проведений за рекурентними співвідношеннями

$$Y^{k+1} = \left(A_2 + A_3 diag(X^k)\right)^{-1} , \tag{5}$$

$$X^{k+1} = -\left(A_1 + (Y^k)^{-1} \cdot diag(X^k)\right)^{-1} B . \tag{6}$$

Приклад 2. Розглянемо тепер матричне рівняння (5) з коефіцієнтами

$$A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \; A_2 = \begin{pmatrix} 1.991 & -3.2 & -5.02 \\ 2.2 & 2.51 & 0.25 \\ 2.0 & -2.34 & -0.132 \end{pmatrix};$$

$$A_1 = \begin{pmatrix} 0.979 & 5.968 & -5.0 \\ 0.245 & 2.2 & 0.251 \\ 2.34 & -1.3 & 0.212 \end{pmatrix};$$

$$B = \begin{pmatrix} 32.8882 & -7.1897 & -8.9086 \end{pmatrix}^T .$$

За допомогою пакету MatLab це матричне рівняння розв’язувалося з використанням рекурентних формул

$$Y^{k+1} = \left(A_2 + A_3 diag(X^k)\right)^{-1} ,$$

$$X^{k+1} = -\left(A_1 + (Y^k)^{-1} \cdot diag(X^k)\right)^{-1} B .$$

У результаті обчислень при початковому наближенні

$$X_1^0 = \begin{pmatrix} -1.21 & 0.61 & 2.2 \end{pmatrix}^T$$

обчислено такі значення наближеного розв'язку

$$X_k = \begin{pmatrix} 0.3614 & 0.9277 & 2.2379 \end{pmatrix}^T$$

Результати експерименту наведені в табл. 2.

Таблиця 2

$\left\|X_k - X_{k-1}\right\| / \left\|X_k\right\|$	Кількість ітерацій	Величина нев'язка
1.000000e-004	60	7.378027e-004
1.000000e-005	68	7.645293e-005
1.000000e-006	76	7.776666e-006
1.000000e-007	84	7.943752e-007
1.000000e-008	92	8.107417e-008
1.000000e-009	100	8.275652e-009
1.000000e-010	108	8.447562e-010
1.000000e-011	116	8.624885e-011

Дана схема, на відміну від попередньої, може бути узагальнена і на випадок матричних поліноміальних рівнянь вищого порядку.

Поліноміальне матричне рівняння n-го порядку. Для поліноміального матричного рівняння (1) можна записати

$$\left(A_n diag(X)^{n-1} + A_{n-1} diag(X)^{n-2} + \ldots + A_2 diag(X) + A_1\right)\cdot X + B = 0\,. \quad (7)$$

Введемо тепер до розгляду Y_1 вигляду

$$Y_1 = \left(A_n diag(X)^{n-1} + A_{n-1} diag(X)^{n-2} + \ldots + A_2 diag(X) + A_1\right)^{-1}. \quad (8)$$

Тоді з урахуванням (7) і (8) можна записати

$$X = -\left(A_1 + Y_1^{-1}\right)\cdot B\,.$$

А далі

$$Y_1 = \left(\left(A_n diag(X)^{n-1} + A_{n-1} diag(X)^{n-2} + \ldots + A_2\right) diag(X) + A_1\right)^{-1}. \quad (9)$$

І використовуючи позначення

$$Y_2 = \left(A_n diag(X)^{n-2} + A_{n-1} diag(X)^{n-3} + \ldots A_3 diag(X) + A_2\right)^{-1}. \quad (10)$$

Для Y_1 можна записати

$$Y_1 = \left(A_1 + Y_2^{-1} diag(X)\right)^{-1}. \quad (11)$$

За аналогією ввівши для (7) позначення

$$Y_3 = \left(A_n diag(X)^{n-3} + A_{n-1} diag(X)^{n-4} + \ldots + A_4 diag(X) + A_3\right)^{-1},$$

для Y_2 отримуємо

$$Y_2 = \left(A_2 + Y_3^{-1} diag(X)\right)^{-1}.$$

Продовжуючи далі цей ступінчатий процес, для Y_{n-1} отримуємо

$$Y_{n-2} = \left(A_{n-2} + Y_{n-1}^{-1} diag(X)\right)^{-1}, \quad (12)$$

де в свою чергу

$$Y_{n-1} = \left(A_{n-1} + A_n diag(X)\right)^{-1} . \qquad (13)$$

Таким чином, вдається записати ітераційну схему для обчислення розв'язків матричного поліноміального рівняння із застосуванням апарату матричних ланцюгових дробів.

$$\left.\begin{array}{ll} Y_{n-1}^{k+1} & = \left(A_{n-1} + A_n diag(X^k)\right)^{-1} \\ Y_i^{k+1} & = \left(A_i + (Y_{i+1}^k)^{-1} diag(X^k)\right)^{-1} \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Y_1^{k+1} & = \left(A_1 + (Y_2^k)^{-1} diag(X^k)\right)^{-1} \\ X^{k+1} & = -\left(A_1 + (Y_1^k)^{-1}\right)\cdot B \end{array}\right\} . \qquad (14)$$

Послідовне застосування отриманих формул надає можливість обчислити X^m із заданою точністю ε на основі перевірки нерівності

$$\left\|X^m - X^{m-1}\right\| \le \varepsilon .$$

З іншого боку, на основі (14) можна записати X у вигляді розвинення розв'язку у неперервний матричний ланцюговий дріб.

Дослідження збіжності наведених обчислювальних схем пов'язано зі збіжністю матричних гіллястих дробів вигляду [6]

$$D = \mathop{D}_{i=1}^{\infty} \sum_{k(i)=1}^{n} a_{k_{(i)}} \frac{c_{k_{(i)}}}{b_{k_{(i)}}} . \qquad (15)$$

Тут V — банахів простір квадратних матриць порядку $p \times p$ над полем дійсних чисел; $k_{(i)} = k_1 k_2 ... k_i$ — скорочені позначення для мультиіндексів; $a_{k_{(i)}}, b_{k_{(i)}}, c_{k_{(i)}} \in V$ — матриці розмірності $p \times p$.

Твердження 1. Якщо розв'язок поліноміального матричного рівняння існує і належить інтервалу $[-n, n]$, то розвинення за деякою ітераційною процедурою у МГЛД з елементами, що задовольняють умови

$$\left\|b_{k_{(s)}}\right\| \le \frac{1}{\left\|a_{k_{(s)}}\right\| \left\|c_{k_{(s)}}\right\| + n} \qquad (1 \le k_s \le n; s = 1,2,3...)$$

збігається до цього розв'язку.

Твердження 2. Якщо розв'язок поліноміального матричного рівняння існує і належить інтервалу $[-\sum_{k_1=1}^{n} \left\|a_{k_1}\right\| \left\|c_{k_1}\right\|, \sum_{k_1=1}^{n} \left\|a_{k_1}\right\| \left\|c_{k_1}\right\|]$ то розвинення за деякою ітераційною процедурою у МГЛД з елементами, що задовольняють умови

$$\left\| b_{k(s)}^{-1} \right\| \leq \frac{1}{1 + \sum\limits_{k_{s+1}=1}^{n} \left\| a_{k(s+1)} \right\| \left\| c_{k(s+1)} \right\|} \qquad (s = 1, 2, 3...)$$

збігається до цього розв'язку.

Висновки. Таким чином, побудовано ефективний метод для аналітичного запису розв'язку матричного поліноміального рівняння *n*-го порядку або обчислення його наближеного значення із заданою точністю.

Список використаних джерел:

1. Григорків В. С. Моделювання еколого-економічної взаємодії: Навчальний посібник. Чернівці: Рута, 2007. 84 с.
2. Григорків В. С. Моделювання економіки. Частина 2: Навчальний посібник. Чернівці: Рута, 2006. 100 с.
3. Икрамов. Х. Д. Численное решение матричных уравнений. М: Наука, 1984. 192 с.
4. Недашковський М. О. Ознаки збіжності матричних гіллястих ланцюгових дробів. Математичні методи та фізико-механічні поля. Львів. 2003. Том 46, № 4. С. 50–56.
5. Недашковський М. О., Крошка Т. І. Збіжність наближених розв\`язків нелінійної задачі для моделі Леотьєва-Форда. *Фізико-математичне моделювання та інформаційні технології.* Центр математичного моделювання ІППММ ім. Я. С. Підстригача НАН України. 2013. Вип. 18. С. 126–135.
6. Скоробогатько В. Я. Теория ветвящихся цепных дробей и ее применение в вычислительной математике. М.: Наука, 1983. 311 с.

A new method for solving polynomial matrix equations with vector unknowns using continued fractions.

Key words: *Matrix polynomial equations, continued fractions.*

Одержано 01.03.2017