ISSN 1563 – 0277
eISSN 2617 – 4871

ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰТТЫҚ УНИВЕРСИТЕТІ

ХАБАРШЫ

Математика, механика, информатика сериясы

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени АЛЬ-ФАРАБИ

ВЕСТНИК

Серия математика, механика, информатика

AL-FARABI KAZAKH NATIONAL UNIVERSITY

Journal of Mathematics, Mechanics and Computer Science

№3 (107)

Алматы
«Қазақ университеті»
2020

Зарегистрирован в Министерстве информации и коммуникаций Республики Казахстан, свидетельство №16508-Ж от 04.05.2017 г. (Время и номер первичной постановки на учет №766 от 22.04.1992 г.). Язык издания: казахский, русский, английский. Выходит 4 раза в год. Тематическая направленность: теоретическая и прикладная математика, механика, информатика.

Научное издание

Вестник. Серия математика, механика, информатика, № 3(107) 2020.
Редактор – С.М. Темешева. Компьютерная верстка – С.М. Темешева

ИБ N 13829

Формат 60 × 84 1/8. Бумага офсетная. Печать цифровая. Объем 7,3 п.л.
Заказ N 11618. Издательский дом "Қазақ университеті"
Казахского национального университета им. аль-Фараби. 050040, г. Алматы, пр.аль-Фараби, 71, КазНУ.
Отпечатано в типографии издательского дома "Қазақ университеті".

1-бөлім **Раздел 1** **Section 1**

Математика **Математика** **Mathematics**

МРНТИ 27.31.15 DOI: https://doi.org/10.26577/JMMCS.2020.v107.i3.01

З.Ю. Фазуллин
Башкирский государственный университет, г. Уфа, Россия
e-mail: fazullinzu@mail.ru

ПРЕДСТАВЛЕНИЕ ФУНКЦИИ ГРИНА ДВУМЕРНОГО ГАРМОНИЧЕСКОГО ОСЦИЛЛЯТОРА

В 1933 году Курант Р. и Гильберт Д. рассмотрели формальное разложение функции источника по собственным функциям задачи Дирихле оператора Лапласа на прямоугольнике. Оказалось, что указанный ряд не может сходиться абсолютно ни для какой пары внутренних точек прямоугольника. Следовательно, сходимость ряда может быть только условной. Тогда для условной сходимости важен порядок суммирования. Системно подобные разложения изучены в работах В.А.Ильина. В данной работе исследована сходимость разложения функции источника по собственным функциям двумерного гармонического осциллятора. Получено представление функции Грина двумерного гармонического осциллятора. Выделены особенности функции Грина. В результате вытекает, что функция Грина двумерного гармонического осциллятора имеет две особые точки. Особенности расположены симметрично относительно начала координат. Подобного эффекта не наблюдалось в исследованиях В.А.Ильина. Ядра дробного порядка, изученные В.А.Ильиным, имели только одну особую точку. Еще одно обстоятельство отличает функцию Грина двумерного гармонического осциллятора от функции Грина краевых задач в ограниченной области. Функция Грина краевой задачи на плоской ограниченной области имеет логарифмическую особенность. В то же время функция Грина двумерного гармонического осциллятора имеет степенные особенности. Однако степень указанной особенности гораздо меньше, чем степенная особенность функции Грина трехмерной краевой задачи в ограниченной области.

Ключевые слова: функция Грина, функция источника, собственные функции, двумерный гармонический осциллятор.

З.Ю. Фазуллин
Башқұрт мемлекеттік университеті, Уфа қ., Ресей
e-mail: fazullinzu@mail.ru

Екі өлшемді гармоникалық осциллятордың Грин функциясының кескінделуі

1933 жылы Курант Р. мен Гильберт Д. тіктөртбұрышта Лаплас операторы үшін Дирихле есебінің меншікті функциялары бойынша қайнар көз функциясының формалды жіктелуін қарастырды. Көрсетілген қатар тіктөртбұрыштың ішкі нүктелерінің кез-келген жұбы үшін жинақтала алмайтыны белгілі болды. Сондықтан қатардың жинақтылығы тек шартты болуы мүмкін. Онда шартты жинақтылық үшін қосындылау тәртібі маңызды. Мұндай жіктелулер В.А. Ильиннің еңбектерінде жүйелі түрде зерттелген. Бұл жұмыста екі өлшемді гармоникалық осциллятордың меншікті функциялары бойынша қайнар көз функциясының жіктелуінің жинақталуы зерттелген. Екі өлшемді гармоникалық осциллятордың Грин функциясының түрі алынды. Грин функциясының ерекшеліктері көрсетілген. Нәтижесінде екі өлшемді гармоникалық осциллятор үшін Грин функциясының екі ерекше нүктесі бар

екені анықталды. Ерекшеліктер координаттар басына қарағанда симметриялы орналасқан. Мұндай әсер В.А. Ильиннің зерттеулерінде байқалған емес. В.А. Ильин зерттеген бөлшек ретті ядролардың бір ғана ерекше нүктесі болды. Тағы бір жағдай екі өлшемді гармоникалық осциллятордың Грин функциясын шенелген облыста шеттік есептердің Грин функциясынан ажыратады: жазық шенелген облыста шеттік есептің Грин функциясының логарифмдік ерекшелігі, ал екі өлшемді гармоникалық осциллятордың Грин функциясының дірежелік ерекшеліктері бар. Алайда, бұл ерекшеліктің дәрежесі шенелген облыстағы үш өлшемді шеттік есептің Грин функциясының дәрежелік ерекшелігінен әлдеқайда аз.

Түйін сөздер: Грин функциясы, қайнар көз функциясы, меншікті функциялар, екі өлшемді гармоникалық осциллятор.

Z.Yu. Fazullin
Bashkir State University, Ufa, Russia
e-mail: fazullinzu@mail.ru

Representation of the Green function of a two-dimensional harmonic oscillator

In 1933, Courant R. and Hilbert D. considered a formal decomposition of the source function by eigenfunctions of the Dirichlet problem of the Laplace operator on a rectangle. It turned out that the specified series cannot converge absolutely for any pair of internal points of the rectangle. Therefore, the convergence of a series can only be conditional. Then the summation order is important for conditional convergence. Systemically similar decompositions are studied in the works of V. A. Ilyin. In this paper, we investigate the convergence of the source function decomposition with respect to the eigenfunctions of a two-dimensional harmonic oscillator. A representation of the green function of a two-dimensional harmonic oscillator is obtained. The features of the green function are highlighted. As a result, it follows that the green function of a two-dimensional harmonic oscillator has two singular points. The features are located symmetrically relative to the origin. This effect was not observed in the studies of V. A. Ilyin. Fractional order kernels studied By V. A. Ilyin had only one singular point. Another circumstance distinguishes the green function of a two-dimensional harmonic oscillator from the green function of boundary-value problems in a bounded domain. The green function of a boundary value problem on a flat bounded domain has a logarithmic singularity. At the same time, the green function of a two-dimensional harmonic oscillator has power-law features. However, the degree of this singularity is much less than the power-law singularity of the green function of a three-dimensional boundary value problem in a bounded domain.

Key words: Green's function, source function, eigenfunctions, two-dimensional harmonic oscillator.

1 Введение

Часто линейные дифференциальные операторы на конечном отрезке удобно интерпретировать как конечномерные возмущения вольтерровых операторов. Подобная трактовка позволила получить ряд выдающихся результатов [1–6]. В то же время линейные уравнения с частными производными редко поддаются такой трактовке. Поскольку их фундаментальные решения редко выписываются в явном виде. Однако иногда все же удается получить полезные представления для фундаментальных решений многомерных дифференциальных уравнений с переменными коэффициентами. В предлагаемой работе найдено представление функции Грина для двумерного гармонического осциллятора.

2 Вспомогательные факты о двумерном гармоническом осцилляторе

В функциональном пространстве $L_2(\mathbb{R}^2)$ двумерный гармонический осциллятор B_0 задается по формуле

$$B_0 = -\triangle + x^2, \quad x^2 = x_1^2 + x_2^2, \quad \triangle = \frac{\partial^2}{\partial x_1^2} + \frac{\partial^2}{\partial x_2^2}.$$

Спектр оператора B_0 хорошо известен и состоит из собственных значений $\lambda_n = 2n + 2$, $n \geq 0$. Соответствующие проекторы на собственные подпространства размерности $n+1$ имеют вид

$$P_n h = \sum_{l=0}^{n} \left\langle h \;\middle|\; \varphi_l^{(n)} \right\rangle \varphi_l^{(n)}$$

где $\langle \cdot \mid \cdot \rangle$ скалярное произведение в $L_2(\mathbb{R}^2)$,

$$\varphi_l^{(n)}(x) = f_l(x_1) f_{n-l}(x_2),$$

$f_l(t)$ – нормированная собственная функция одномерного гармонического осциллятора, соответствующая собственному значению $2l+1$, $l \geq 0$.

Хорошо известно, что

$$f_l(t) = \left(2^l l! \sqrt{\pi}\right)^{\frac{1}{2}} e^{-\frac{t^2}{2}} H_l(t),$$

где $H_l(t)$ многочлены Эрмита, причем на любом компакте $K \subset \mathbb{R}^2$ имеет место глобальная оценка [7]

$$|f_l(t)| \leq \frac{C_0}{\sqrt[4]{2l+1}}.$$

Здесь C_0 зависит только от K.

Из асимптотической формулы для многочлена $H_l(t)$ [8] и формулы Стирлинга [7] следует, что при $l \gg 1$, $t \in K$

$$f_l(t) = \alpha_l \left\{ \cos\left[t\sqrt{2l+1} - \frac{l\pi}{2} \right] \left[u_0(t) - \frac{u_2(t)}{4(2l+1)} + O\left(\frac{1}{l^2}\right) \right] \right\} +$$

$$+\frac{\alpha_l}{2\sqrt{2l+1}}\left\{\sin\left[t\sqrt{2l+1}-\frac{l\pi}{2}\right]\left[u_1(t)-\frac{u_3(t)}{4(2l+1)}+O\left(\frac{1}{l^2}\right)\right]\right\},$$

где $u_0(t)\equiv 1$, $u_l(t)=\int_0^t Lu_{l-1}(t)\,dt$,$L=-\frac{d^2}{dt^2}+t^2$,

$$\alpha_l=\sqrt{\frac{\pi}{2}}\,\frac{1}{\sqrt[4]{2l+1}}\left\{1-\frac{1}{32(2l+1)^2}+O\left(\frac{1}{l^3}\right)\right\}.$$

3 Функция Грина двумерного гармонического осциллятора

Оператор B_0 самосопряженный в $L_2(\mathbb{R}^2)$ и обратим, причем

$$B_0{}^{-1}F(x)=\int_{\mathbb{R}^2}\varepsilon(x,t)\,F(t)\,dt$$

Функция $\varepsilon(x,t)$ представляет функцию Грина оператора B_0 и имеет представление

$$\varepsilon(x,t)=\sum_{n=1}^{\infty}\frac{1}{2n+2}\sum_{l=0}^{n}f_l(x_1)f_{n-l}(x_2)f_l(t_1)f_{n-l}(t_2).$$

Детально исследуем правую часть последнего ряда. Подобного рода ряды встречаются довольно часто в математической физике. Согласно терминологии В.А.Ильина подобные представления являются разложениями функции источника в виде билинейного ряда по собственным функциям [9]. Систематические исследования подобных рядов и их различных обобщений можно найти в работах [10, 11]. В случае ограниченных областей с гладкими границами для разложений по собственным функциям оператора Лапласа В.А.Ильин показал, что такие ряды не могут сходиться абсолютно. Возможно только условная сходимость подобных рядов. При условной сходимости рядов важную роль играет порядок суммирования отдельных слагаемых. В.А.Ильин в своих исследованиях указал такой порядок слагаемых, что сумма ряда может иметь особенности специального вида.

С другой стороны, обычно функция Грина представляет сумму фундаментального решения и компенсирующей (гладкой) функции. Таким образом, методы суммирования В.А.Ильина позволяют исследовать возможные особенности фундаментального решения.

Оказывается, что в случае двумерного гармонического осциллятора особенности фундаментального решения удается определить классическими методами. Не привлекая аппарат формулы среднего значения, которым пользовался В.А.Ильин.

Также отметим, двумерный гармонический осциллятор исследуется на всей плоскости, а не в ограниченной области.

В работе [12] доказано, что на любом компакте $K\subset\mathbb{R}^2$ и при $n\to\infty$ верна асимптотическая формула

$$\sum_{l=0}^{n}f_l(x_1)f_{n-l}(x_2)f_l(t_1)f_{n-l}(t_2)=\frac{1}{2\pi}J_0\left(\sqrt{2n+2}\,|x-t|\right)+$$

$$+\frac{(-1)^n}{2\pi}J_0\left(\sqrt{2n+2}\,|x+t|\right)+r_n(x,t),\ x\in K,\ t\in K$$

где $J_0(\cdot)$ – функция Бесселя первого рода, $r_n(x,t)$ при каждом $\sigma\in\left(0,\frac{1}{2}\right)$ допускает оценку

$$|r_n(x,t)|\le\frac{C_1}{n^{\frac{1}{2}+\frac{\sigma}{2}}}+\frac{C_2}{n^{1-\frac{3\sigma}{2}}}$$

причем $C_1,\ C_2>0$ и зависят только от σ и K.

Поскольку при больших $\beta\to\infty$ верна асимптотика

$$J_0(\beta)=\sqrt{\frac{2}{\pi}}\cos(\beta-\frac{\pi}{4})\,[1+o(1)]$$

То ряд, определяющий функцию $\varepsilon(x,t)$, сходится при $x\neq\pm t$. В точках $x=\pm t$ функция $\varepsilon(x,t)$ может иметь особенности. Действительно, для функции Грина справедливо представление

$$\varepsilon(x,t)=\sqrt{\frac{2}{|x-t|\,\pi}}\varepsilon_-(x,t)+\sqrt{\frac{2}{|x+t|\,\pi}}\varepsilon_+(x,t)+k(x,t),$$

где $\varepsilon_-(x,t)$, $\varepsilon_+(x,t)$, $k(x,t)$ – непрерывные функций двух переменных (x,t).

Заметим, что

$$\varepsilon_-(x,t)=\sum_{n=1}^{\infty}\frac{\cos(\sqrt{2n+2}\,|x-t|)}{(2n+2)^{5/4}}\,(1+O(1)),$$

$$\varepsilon_+(x,t)=\sum_{n=1}^{\infty}\frac{\cos(\sqrt{2n+2}\,|x+t|)}{(2n+2)^{5/4}}\,(1+O(1)).$$

Таким образом, нами доказана теорема.

Теорема 1 *Функция Грина $\varepsilon(x,t)$ двумерного гармонического осциллятора определена при всех $x\neq\pm t$ и является непрерывной функцией от (x,t) на области определения. Больше того, для функций Грина $\varepsilon(x,t)$ справедливо представление*

$$\varepsilon(x,t)=\sqrt{\frac{2}{|x-t|\,\pi}}\varepsilon_-(x,t)+\sqrt{\frac{2}{|x+t|\,\pi}}\varepsilon_+(x,t)+k(x,t).$$

Замечание 1 *Более детальный анализ позволяет утверждать, что функций $\varepsilon_-(x,t)$, $\varepsilon_+(x,t)$, $k(x,t)$ имеют дробные производные по t_1 и t_2, порядок которых меньше* 0.5.

Список литературы

[1] Birkhoff G.D., "On the asymptotic characters of the solution of certain linear differential equations containing a parameter *Trans. Amer. Math. Soc.* **9** (1908): 219-231.

[2] Birkhoff G.D., "Boundary value and expansion problems of ordinary linear differential equations *Trans. Amer. Math. Soc.* **9** (1908): 373-395.

[3] Тамаркин Я.Д., *О некоторых общих задачах теории обыкновенных дифференциальных уравнений* (Петроград, 1917).

[4] Stone M.H., "A comparision of the series of Fourier and Birkhoff *Trans. Amer. Math. Soc.* **28** (1926): 695-761.

[5] Келдыш М.В., "О собственных значениях и собственных функциях некоторых кассов несамосопряженных линейных уравнений *Докл. АН СССР* **77**:1 (1951): 11-14.

[6] Хромов А.П., "Конечномерные возмущения вольтерровых операторов *Современная математика. Фундаментальные направления* **10** (2004): 3-162.

[7] Никифоров А.Ф., Уваров В.Б., *Специальные функций математической физики* (М.: Наука, 1984).

[8] Сеге Г., *Ортогональные многочлены* (М.: ГИФМЛ, 1962).

[9] Ильин В.А., "Представление функции источника для прямоугольника в виде билинейного ряда по собственным функциям *Докл. АН СССР* **74**:3 (1950): 413-416.

[10] Ильин В.А., "Ядра дробного порядка *Матем. сборник* **41(83)**:4 (1957): 459-480.

[11] Ильин В.А., "О разложимости функций, обладающих особенностями, в условно сходящийся ряд по собственным функциям *Изв. АН СССР, сер. матем.* **22**:1 (1958): 49-80.

[12] Fazullin Z.Yu. and Murtazin Kh.Kh., "Regularized trace of a two-dimensional harmonic oscillator *Sb. Math.* **192**:5 (2001): 725–761.

References

[1] Birkhoff G.D., "On the asymptotic characters of the solution of certain linear differential equations containing a parameter *Trans. Amer. Math. Soc.* **9** (1908): 219-231.

[2] Birkhoff G.D., "Boundary value and expansion problems of ordinary linear differential equations *Trans. Amer. Math. Soc.* **9** (1908): 373-395.

[3] Tamarkin Ya.D., *O nekotoryh obshchih zadachah teorii obyknovennyh differencial'nyh uravnenij [On some General problems of the theory of ordinary differential equations]* (Petrograd, 1917).

[4] Stone M.H., "A comparision of the series of Fourier and Birkhoff *Trans. Amer. Math. Soc.* **28** (1926): 695-761.

[5] Keldysh M.V., "O sobstvennyh znacheniyah i sobstvennyh funkciyah nekotoryh kassov nesamosopryazhennyh linejnyh uravnenij [On eigenvalues and eigenfunctions of certain casses of non-self-adjoint linear equations] *Doklady Akad. Nauk SSSR* **77**:1 (1951): 11-14.

[6] Khromov A.P., "Konechnomernye vozmushcheniya vol'terrovyh operatorov [Finite-dimensional perturbations of Voltaire operators] *Modern mathematics. Fundamental direction* **10** (2004): 3-162.

[7] Nikiforov A.F., Uvarov V.B., *Special'nye funkcij matematicheskoj fiziki [Special functions of mathematical physics]* (M: Science, 1984).

[8] Sege G., *Ortogonal'nye mnogochleny [Orthogonal polynomials]* (M.: GIFML, 1962).

[9] Ильин В.А., "Представление функции источника для прямоугольника в виде билинейного ряда по собственным функциям *Doklady Akad. Nauk SSSR* **74**:3 (1950): 413-416.

[10] Il'in V.A., "Уфdra drobnogo poryadka [The kernel of fractional order] *Sb. Math.* **41(83)**:4 (1957): 459-480.

[11] Il'in V.A., "O razlozhimosti funkcij, obladayushchih osobennostyami, v uslovno skhodyashchijsya ryad po sobstvennym funkciyam [On the decomposability of functions with singularities into a conditionally convergent series by eigenfunctions] *Izvestia of the USSR Academy of Sciences* **22**:1 (1958): 49-80.

[12] Fazullin Z.Yu. and Murtazin Kh.Kh., "Regularized trace of a two-dimensional harmonic oscillator *Sb. Math.* **192**:5 (2001): 725–761.

МРНТИ 27.39.21 DOI: https://doi.org/10.26577/JMMCS.2020.v107.i3.02

Б.Н. Даулетбай
Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан
Назарбаев Интеллектуальная школа физико-математического направления,
г. Алматы, Казахстан
e-mail: dauletbay_b@fmalm.nis.edu.kz

СПЕКТРАЛЬНАЯ ТЕОРЕМА В ФОРМЕ М.В. КЕЛДЫША ДЛЯ ПРОИЗВОЛЬНОГО ЛИНЕЙНОГО ОПЕРАТОРА В КОНЕЧНОМЕРНОМ ПРОСТРАНСТВЕ

Одной из главных проблем спектральной теории линейных операторов является вопрос о спектральном разложении операторов. Из курса "Функциональный анализ" нам известно, что самосопряженный оператор в гильбертовом пространстве допускает единственное спектральное разложение. В 1971 году М.В. Келдыш в своей работе определил коэффициенты главной части разложений Лорана для резольвенты вполне непрерывного оператора в гильбертовом пространстве (при этом про сходимость ряда ничего не сказано). Данные коэффициенты он определил методом решения систем дифференциальных уравнений. П. Ланкастер в своей монографии сформулировал теорию спектрального разложения для квадратичных матриц, но определил коэффициенты разложения только для специальных (симметричных) матриц. Данная работа посвящена вопросу спектрального разложения произвольного линейного оператора в конечномерном пространстве. Целью работы является определить коэффициенты разложения Лорана для произвольного линейного оператора в конечномерном пространстве через базисные элементы данного и сопряженного ему оператора. В ходе исследования были доказаны некоторые свойства компонентов линейного оператора, а также была доказана спектральная теорема в форме М.В. Келдыша для произвольного линейного оператора в конечномерном пространстве. Все коэффициенты разложения совпадали с найденными коэффициентами главной части разложения Лорана для резольвенты вполне непрерывного оператора в гильбертовом пространстве, вычисленных в работе М.В. Келдыша, но в этой работе они вычислены уже функциональным методом. Доказанная теорема имеет огромную значимость в исследовании спектральных свойств возмущенных линейных операторов в конечномерном пространстве.

Ключевые слова: спектральная теорема, спектральное разложение, базисные элементы, компонентные операторы, резольвента, собственные значения, собственные проекторы.

Б.Н. Даулетбай
Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
Физика-математика бағытындағы Назарбаев Зияткерлік мектебі, Алматы қ., Қазақстан
e-mail: dauletbay_b@fmalm.nis.edu.kz

Ақырлы өлшемді кеңістікте анықталған кез келген сызықтық оператор үшін М.В. Келдыш түріндегі спектралды теорема

Сызықтық операторлардың спектралды теориясының басты мәселелерінің бірі операторлардың спектралды жіктелу сұрағы болып табылады. Гильберт кеңістігінде анықталған өзіне-өзі түйіндес операторлардың спектралды жіктелетіндігі туралы бізге "Функционалдық анализ" курсынан белгілі. 1971 жылы М.В. Келдыш өзінің жұмысында Гильберт кеңістігінде анықталған толық үзіліссіз операторлардың резольвентасы үшін Лоран қатарларының

бас бөліктерінің коэффициенттерін анықтап шықты (бірақ қатардың жинақтылығы туралы ештеңе айтылмаған). Бұл коэффициенттерді ол дифференциалдық теңдеулер жүйесін шешу әдісімен анықтады. П. Ланкастер өзінің монографиясында матрицалар үшін спектралды жіктелу теориясын құрды, бірақ жіктелу коэффициенттерін тек арнайы (симметриялы) матрицалар үшін ғана анықтады. Бұл жұмыс ақырлы өлшемді кеңістікте анықталған кез келген сызықтық операторлардың спектралды жіктелу сұрағына арналған. Жұмыстың мақсаты - ақырлы өлшемді кеңістікте анықталған сызықтық операторлардың резольвентасы үшін Лоран қатарының коэффициенттерін осы оператор мен оған түйіндес операторлардың базистік элементтері арқылы анықтау. Зерттеу барысында сызықтық операторлардың компоненттерінің кейбір қасиеттері және ақырлы өлшемді кеңістікте анықталған кез келген сызықтық оператор үшін М.В. Келдыш түріндегі спектралды теорема дәлелденді. Жіктелу коэффициенттері М.В. Келдыштың жұмысында келтірілген Гильберт кеңістігінде анықталған толық үзіліссіз операторлардың резольвентасы үшін Лоран қатарларының бас бөліктері коэффициенттерімен сәйкес келді, бірақ бұл жұмыста олар функционалдық әдіспен анықталды. Дәлелденген теореманың ақырлы өлшемді кеңістікте анықталған сызықтық операторлардың ауытқуларының спектралды қасиеттерін зерттеуде маңызы зор.

Түйін сөздер: спектралды теорема, спектралды жіктелу, базистік элементтер, компоненттік операторлар, резольвента, меншікті мәндер, меншікті проекторлар.

B.N. Dauletbay
Al-Farabi Kazakh National University, Almaty, Kazakhstan
Nazarbayev Intellectual school of Physics and Mathematics, Almaty, Kazakhstan
e-mail: dauletbay_b@fmalm.nis.edu.kz

Spectral theorem in the form of M. V. Keldysh for an arbitrary linear operator in a finite-dimensional space

One of the main problems of the spectral theory of linear operators is the question of the spectral decomposition of operators. We know from the course "Functional analysis"that a self-adjoint operator in a Hilbert space admits a unique spectral decomposition. In 1971, M.V. Keldysh in his work determined the coefficients of the main part of the Laurent expansions for the resolvent of a completely continuous operator in a Hilbert space (while nothing is said about the convergence of the series). He determined these coefficients by solving systems of differential equations. P. Lancaster in his monograph formulated the theory of spectral expansion for quadratic matrices, but determined the expansion coefficients only for special (symmetric) matrices. This paper is devoted to the spectral decomposition of an arbitrary linear operator in a finite-dimensional space. The aim of this work is to determine the coefficients of the Laurent expansion for an arbitrary linear operator in a finite-dimensional space through the basis elements of this and its adjoint operator. In the course of the research, some properties of the components of the linear operator were proved, and a spectral theorem in the form of M.V. Keldysh was proved for an arbitrary linear operator in a finite-dimensional space. All the coefficients of the expansion coincided with the coefficients of the main part of the Laurent expansion found for the resolvent of a completely continuous operator in Hilbert space, calculated in the work of M.V. Keldysh,but in this work they are calculated by the functional method. The proved theorem is of great importance in the study of the spectral properties of perturbed linear operators in a finite-dimensional space.

Key words: spectral theorem, spectral decomposition, basic elements, component operators, resolvent, eigenvalues, eigenprojectors.

1 Введение. Постановка задачи

Пусть X – конечномерное пространство размерности n.

Известно, что оператор $X \to X$ в некотором базисе, состоящем из его собственных элементов, имеет так называемую диагональную форму. Следовательно, если оператор T имеет n линейно независимых собственных элементов, то приводится к диагональному виду. Однако количество линейно независимых собственных элементов у линейного оператора T может оказаться меньше, чем n. В таком случае выбирается некоторый базис пространства X и линейный оператор T приводится к так называемой жордановой нормальной форме. К примеру, в книге [1, с. 200] приведено следующее утверждение.

Утверждение 1 *Пусть $T-$ произвольный линейный оператор в комплексном пространстве X размерности $n < \infty$. Предположим, что у оператора T имеется $s\,(s \le n)$ линейно независимых собственных элементов x_1, x_2, ..., x_s, соответствующих собственным значениям λ_1, λ_2, ..., λ_s.*

Тогда существует базис, состоящий из $s\,(s \le n)$ групп элементов

$$x_1, x_{11}, ..., x_{1,m_1}; x_2, x_{21}, ..., x_{2,m_2}; ...; x_s, x_{s1}, ..., x_{s,m_s},$$

в котором оператор T имеет следующий вид:

$$\begin{array}{llll} Tx_1 = \lambda_1 x_1, & Tx_{11} = \lambda_1 x_{11} + x_1, & \ldots, & Tx_{1,m_1} = \lambda_1 x_{1,m_1} + x_{1,m_1-1}; \\ Tx_2 = \lambda_2 x_2, & Tx_{21} = \lambda_2 x_{21} + x_2, & \ldots, & Tx_{2,m_2} = \lambda_2 x_{2,m_2} + x_{2,m_2-1}; \\ \ldots & \ldots & \ldots & \ldots \\ Tx_s = \lambda_s x_s, & Tx_{s1} = \lambda_s x_{s1} + x_s, & \ldots, & Tx_{s,m_s} = \lambda_s x_{s,m_s} + x_{s,m_s-1}. \end{array}$$

Утверждение 1 можно применить к сопряженному оператору T^*. Следовательно, у оператора T^* имеется $s\,(s \le n)$ линейно независимых собственных элементов y_1, y_2, ..., y_s, соответствующих собственным значениям $\overline{\lambda_1}$, $\overline{\lambda_2}$, ..., $\overline{\lambda_s}$. Тогда существует базис, состоящий из $s\,(s \le n)$ групп элементов

$$y_1, y_{11}, \ldots, y_{1,m_1}; \quad y_2, y_{21}, \ldots, y_{2,m_2}; \quad \ldots; \quad y_s, y_{s1}, \ldots, y_{s,m_s},$$

в котором оператор T^* имеет следующий вид:

$$\begin{array}{llll} T^*y_1 = \overline{\lambda_1} y_1, & T^*y_{11} = \overline{\lambda_1} y_{11} + y_1, & \ldots, & T^*y_{1,m_1} = \overline{\lambda_1} y_{1,m_1} + y_{1,m_1-1}; \\ T^*y_2 = \overline{\lambda_2} y_2, & T^*y_{21} = \overline{\lambda_2} y_{21} + y_2, & \ldots, & T^*y_{2,m_2} = \overline{\lambda_2} y_{2,m_2} + y_{2,m_2-1}; \\ \ldots & \ldots & \ldots & \ldots \\ T^*y_s = \overline{\lambda_s} y_s, & T^*y_{s1} = \overline{\lambda_s} y_{s1} + y_s, & \ldots, & T^*y_{s,s} = \overline{\lambda_s} y_{s,m_s} + y_{s,m_s-1}. \end{array}$$

В монографии [2, с. 163] приведено следующее

Утверждение 2 *Пусть T – произвольный линейный оператор в комплексном пространстве X размерности $n < \infty$, а скалярная функция f определена на спектре T. Тогда существуют такие независимые от f операторы Z_{kj}, что*

$$f(T) = \sum_{k=1}^{s} \sum_{j=1}^{m_k+1} f^{(j-1)}(\lambda_k) Z_{kj}. \tag{1}$$

Операторы Z_{kj} называются компонентами оператора T.

Поставлена следующая задача: определить компоненты Z_{kj}, используя базисные элементы операторов T и T^*.

2 Основные результаты

Пусть $f(T) = \mathcal{R}(\lambda; T) = (T - \lambda I)^{-1}$. Тогда для $k = 1, 2, ..., s$ функция f принимает значения $f(\lambda_k) = \dfrac{1}{\lambda_k - \lambda}$, а

$$f^{(j-1)}(\lambda_k) = \frac{(-1)^{j-1}(j-1)!}{(\lambda_k - \lambda)^j} = \frac{(-1)^{j-1}(j-1)!}{(-1)^j(\lambda - \lambda_k)^j} = -\frac{(j-1)!}{(\lambda - \lambda_k)^j}.$$

Следовательно,

$$\mathcal{R}(\lambda; T) = -\sum_{k=1}^{s}\sum_{j=1}^{m_k+1}\frac{(j-1)!}{(\lambda - \lambda_k)^j}Z_{kj}. \tag{2}$$

Так как операторы Z_{kj} не зависят от f, мы сможем определить их значения, используя свойства резольвенты оператора T.

Проинтегрируем обе части равенства (2) по контуру $|\lambda - \lambda_p| = \varepsilon$ $(1 \le p \le s)$. Оператор вычетов резольвенты $\mathcal{R}(\lambda; T)$ справа равен Z_{k1}. Таким образом, из теоремы о вычетах получаем равенство

$$\oint_{|\lambda-\lambda_p|=\varepsilon}\mathcal{R}(\lambda; T)\,d\lambda = -2\pi i Z_{p1}.$$

И для всех $k = 1, 2, ..., s$ получаем

$$Z_{k1} = -\frac{1}{2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon}\mathcal{R}(\lambda; T)\,d\lambda.$$

Проведенное рассуждение может быть легко обобщено до получения формул всех компонент в виде контурных интегралов. Умножим сначала обе части равенства (2) на $(\lambda - \lambda_p)^q$ $(0 \le q \le m_p)$ и затем проинтегрируем их по контуру $|\lambda - \lambda_p| = \varepsilon$ $(1 \le p \le s)$. Таким образом,

$$\oint_{|\lambda-\lambda_k|=\varepsilon}(\lambda - \lambda_p)^q\mathcal{R}(\lambda; T)\,d\lambda = -\sum_{k=1}^{s}\sum_{j=1}^{m_k+1}(j-1)!Z_{kj}\oint_{|\lambda-\lambda_k|=\varepsilon}\frac{(\lambda - \lambda_p)^q}{(\lambda - \lambda_k)^j}d\lambda.$$

Ненулевые интегралы справа – это те, для которых $k = p, j = q + 1$, и этот интеграл имеет значение $2\pi i$, то есть

$$\oint_{|\lambda-\lambda_k|=\varepsilon}\frac{(\lambda - \lambda_p)^q}{(\lambda - \lambda_k)^j}d\lambda = \begin{cases} 2\pi i, & \text{если} \quad k = p, \quad j = q+1 \\ 0, & \text{если} \quad k \ne p, \quad j \ne q+1 \end{cases}$$

Следовательно,

$$\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_p)^q \mathcal{R}(\lambda;T)\, d\lambda = -(2\pi i)\, q! Z_{p,q+1}.$$

В общем виде, для $k=1,2,...,s;\ j=1,2,...,m_k+1$ получаем

$$Z_{kj} = -\frac{1}{(j-1)!2\pi i} \oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j-1} \mathcal{R}(\lambda;T)\, d\lambda. \tag{3}$$

Вышеизложенные вычисления есть в монографии [2, с. 176-177].

Из данных вычислений мы получаем следующие теоремы.

Теорема 1 *Для всех $k=1,2,...,s;\ j=1,2,...,m_k$ имеет место равенство*

$$Z_{k,j+1} = \frac{1}{j}(T-\lambda_k I) Z_{kj}. \tag{4}$$

Доказательство. Вычислим значение $(T-\lambda_k I) Z_{kj}$ для всех $k=1,2,...,s;\ j=1,2,...,m_k$.

$$(T-\lambda_k I) Z_{kj} = (T-\lambda_k I)\left[-\frac{1}{(j-1)!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j-1}\mathcal{R}(\lambda;T)\, d\lambda\right] =$$
$$= -\frac{1}{(j-1)!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j-1}(T-\lambda_k I)\mathcal{R}(\lambda;T)\, d\lambda =$$
$$= -\frac{1}{(j-1)!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j-1}(T-\lambda I+\lambda I-\lambda_k I)\mathcal{R}(\lambda;T)\, d\lambda =$$
$$= -\frac{1}{(j-1)!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j-1}(T-\lambda I)\mathcal{R}(\lambda;T)\, d\lambda -$$
$$-\frac{1}{(j-1)!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j-1}(\lambda-\lambda_k) I\mathcal{R}(\lambda;T)\, d\lambda =$$
$$= -\frac{1}{(j-1)!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j-1} d\lambda - \frac{1}{(j-1)!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j}\mathcal{R}(\lambda;T)\, d\lambda =$$
$$= 0 - \frac{1}{(j-1)!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j}\mathcal{R}(\lambda;T)\, d\lambda =$$
$$= -\frac{j}{j!2\pi i}\oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda-\lambda_k)^{j}\mathcal{R}(\lambda;T)\, d\lambda = jZ_{k,j+1}.$$

Следовательно, $Z_{k,j+1} = \frac{1}{j}(T-\lambda_k I) Z_{kj}$. Теорема доказана.

Приведем следующее следствие, полученной из теоремы 1.

Следствие 1 *Для $k=1,2,...,s,\ \ j=1,2,...,m_k+1$ выполняется равенство*

$$Z_{kj} = \frac{1}{(j-1)!}(T-\lambda_k I)^{j-1} Z_{k1}. \tag{5}$$

Для Z_{k1} равенство (5) очевидно. Для $j = 2, ..., m_k + 1$ получаем

$$Z_{k,j} = \frac{1}{j-1}(T - \lambda_k I) Z_{k,j-1} = \frac{1}{j-1}(T - \lambda_k I) \frac{1}{(j-1)-1}(T - \lambda_k I) Z_{k,(j-1)-1} =$$
$$= \frac{1}{(j-1)(j-2)}(T - \lambda_k I)^2 \frac{1}{(j-1)-2}(T - \lambda_k I) \dots \frac{1}{(j-1)-(j-2)} Z_{k,j-1-(j-2)} =$$
$$= \dots = \frac{1}{(j-1)!}(T - \lambda_k I)^{j-1} Z_{k1}.$$

Значит, $Z_{kj} = \frac{1}{(j-1)!}(T - \lambda_k I)^{j-1} Z_{k1},\ k = 1, 2, ..., s,\ \ j = 1, 2, ..., m_k + 1.$

Теорема 2 *Для всех $k = 1, 2, ..., s$ имеет место равенство*

$$(T - \lambda_k I) m_k! Z_{k,m_k+1} = 0. \tag{6}$$

Доказательство. Для Z_{k,m_k+1} имеем

$$(T - \lambda_k I) Z_{k,m_k+1} = -\frac{1}{m_k! 2\pi i} \oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda - \lambda_k)^{m_k} (T - \lambda_k I) \mathcal{R}(\lambda; T)\, d\lambda =$$
$$= -\frac{1}{m_k! 2\pi i} \oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda - \lambda_k)^{m_k+1} \mathcal{R}(\lambda; T)\, d\lambda.$$

$$(T - \lambda_k I) m_k! Z_{k,m_k+1} = -\frac{1}{2\pi i} \oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda - \lambda_k)^{m_k+1} \mathcal{R}(\lambda; T)\, d\lambda.$$

Так как функция $(\lambda - \lambda_k)^{m_k+1} \mathcal{R}(\lambda; T)$ аналитична внутри $|\lambda - \lambda_k| = \varepsilon$, для всех $k = 1, 2, ..., s$

$$-\frac{1}{2\pi i} \oint_{|\lambda-\lambda_k|=\varepsilon} (\lambda - \lambda_k)^{m_k+1} \mathcal{R}(\lambda; T)\, d\lambda = 0.$$

Отсюда $(T - \lambda_k I) m_k! Z_{k,m_k+1} = 0$. Теорема доказана.

По данной теореме, компонента $m_k! Z_{k,m_k+1}$ есть собственный проектор оператора T, соответствующий собственному значению λ_k.

Из следствия 1 и теоремы 2 получаем следующее следствие.

Следствие 2 *Для $k = 1, 2, ..., s$ выполняется равенство*

$$(T - \lambda_k I)^{m_k+1} Z_{k1} = 0.$$

Действительно, $(T - \lambda_k I)^{m_k+1} Z_{k1} = m_k! (T - \lambda_k I) Z_{k,m_k+1} = 0.$

Для резольвенты $\mathcal{R}(\lambda; T)$ оператора T имеем

$$\mathcal{R}(\lambda; T) = -\sum_{k=1}^{s} \sum_{j=1}^{m_k+1} \frac{(j-1)!}{(\lambda - \lambda_k)^j} Z_{kj},$$

отсюда

$$(\mathcal{R}(\lambda;T))^* = \left(-\sum_{k=1}^{s}\sum_{j=1}^{m_k+1}\frac{(j-1)!}{(\lambda-\lambda_k)^j}Z_{kj}\right)^* = -\sum_{k=1}^{s}\sum_{j=1}^{m_k+1}\frac{(j-1)!}{\left(\overline{\lambda}-\overline{\lambda_k}\right)^j}Z_{kj}^*.$$

Так как, $(\mathcal{R}(\lambda;T))^* = \mathcal{R}\left(\overline{\lambda};T^*\right)$,то

$$\mathcal{R}\left(\overline{\lambda};T^*\right) = -\sum_{k=1}^{s}\sum_{j=1}^{m_k+1}\frac{(j-1)!}{\left(\overline{\lambda}-\overline{\lambda_k}\right)^j}Z_{kj}^*.$$

Итак, мы пришли к следующему выводу: если Z_{kj} есть компонента оператора T, то Z_{kj}^* есть компонента оператора T^*.

Лемма 1 $\left(T^*-\overline{\lambda_k}I\right)Z_{kj}^* = Z_{kj}^*\left(T^*-\overline{\lambda_k}I\right).$

Доказательство. Применяя для $\mathcal{R}\left(\overline{\lambda};T^*\right)$ лемму 1, получаем

$$Z_{k,j+1}^* = \frac{1}{j}\left(T^*-\overline{\lambda_k}I\right)Z_{kj}^*. \tag{7}$$

С другой стороны,

$$(Z_{k,j+1})^* = \left(\frac{1}{j}(T-\lambda_k I)Z_{kj}\right)^*;$$

$$Z_{k,j+1}^* = \frac{1}{j}Z_{kj}^*\left(T^*-\overline{\lambda_k}I\right).$$

Тогда $\frac{1}{j}\left(T^*-\overline{\lambda_k}I\right)Z_{kj}^* = \frac{1}{j}Z_{kj}^*\left(T^*-\overline{\lambda_k}I\right)$. Следовательно,

$$\left(T^*-\overline{\lambda_k}I\right)Z_{kj}^* = Z_{kj}^*\left(T^*-\overline{\lambda_k}I\right).$$

Итак, мы собрали все нужные данные о компонентах Z_{kj} для доказательства следующей важной теоремы.

Теорема 3 *Пусть оператор $T: X \to X$ такой, что выполнено утверждение 1 и сохранены его обозначения. Тогда для произвольной скалярной функции f, у которой определены значения*

$$\begin{array}{l} f(\lambda_1), f'(\lambda_1), ..., f^{(m_1)}(\lambda_1) \\ f(\lambda_2), f'(\lambda_2), ..., f^{(m_2)}(\lambda_2) \\ \ldots \\ f(\lambda_s), f'(\lambda_s), ..., f^{(m_s)}(\lambda_s), \end{array}$$

выполнено следующее операторное соотношение

$$f(T) = \sum_{k=1}^{s}\sum_{j=1}^{m_k+1} f^{(j-1)}(\lambda_k)Z_{kj}, \tag{8}$$

где

$$Z_{k1} = x_{k,m_k} y_k^* + x_{k,m_k-1} y_{k,1}^* + ... + x_k y_{k,m_k}^*,$$

$$Z_{k2} = \frac{1}{1!}\left(x_{k,m_k-1} y_k^* + x_{k,m_k-2} y_{k,1}^* + ... + x_k y_{k,m_k-1}^*\right),$$

$$Z_{k3} = \frac{1}{2!}\left(x_{k,m_k-2} y_k^* + x_{k,m_k-3} y_{k,1}^* + ... + x_k y_{k,m_k-2}^*\right),$$

$\dots$

$$Z_{k,m_k-1} = \frac{1}{(m_k-2)!}\left(x_{k,2} y_k^* + x_{k,1} y_{k,1}^* + x_k y_{k,2}^*\right),$$

$$Z_{k,m_k} = \frac{1}{(m_k-1)!}\left(x_{k,1} y_k^* + x_k y_{k,1}^*\right),$$

$$Z_{k,m_k+1} = \frac{1}{m_k!} x_k y_k^*.$$

Здесь и в дальнейшем принято следующее обозначение, введенное М.В. Келдышом [3]: через xy^* обозначим оператор

$$(xy^*)\, a = \langle a, y\rangle\, x,$$

где $\langle a, y\rangle$ – линейный непрерывный функционал относительно элемента $a \in X$.

Доказательство. Так как компонента $m_k! Z_{k,m_k}$ есть собственный проектор оператора T, соотсветствующий собственному значению λ_k, а компонента $m_k! Z_{k,\underline{m_k}}^*$ есть собственнный проектор опертора T^*, соответствующий собственному значению $\overline{\lambda_k}$, спарведливо равенство

$$m_k! Z_{k,m_k} = x_k y_k^*$$

Отсюда компонента Z_{k,m_k+1} принимает значение

$$Z_{k,m_k+1} = \frac{1}{m_k!} x_k y_k^*.$$

Из равенства (4) получаем

$$Z_{k,m_k+1} = \frac{1}{m_k}\left(T - \lambda_k I\right) Z_{k,m_k}.$$

Тогда

$$\frac{1}{m_k}\left(T - \lambda_k I\right) Z_{k,m_k} = \frac{1}{m_k!} x_k y_k^*;$$

$$\left(T - \lambda_k I\right) Z_{k,m_k} = \frac{1}{(m_k-1)!} x_k y_k^*. \tag{9}$$

А из равенства (7)

$$(T^* - \lambda_k I)\, Z^*_{k,m_k} = \frac{1}{(m_k-1)!} y_k x^*_k. \tag{10}$$

Принимая во внимание равенства (9) и (10), получаем

$$Z_{k,m_k} = \frac{1}{(m_k-1)!}\left(x_{k,1} y^*_k + x_k y^*_{k,1}\right)$$

Далее, по индукционному предположению находим значения остальных компонент $Z_{k,m_k-1}, Z_{k,m_k-2}, ..., Z_{k,1}$.
Для компоненты Z_{k,m_k-1}

$$Z_{k,m_k} = \frac{1}{m_k-1}(T-\lambda_k I)\, Z_{k,m_k-1} = \frac{1}{(m_k-1)!}\left(x_{k,1} y^*_k + x_k y^*_{k,1}\right);$$

$$(T-\lambda_k I)\, Z_{k,m_k-1} = \frac{1}{(m_k-2)!}\left(x_{k,1} y^*_k + x_k y^*_{k,1}\right);$$

$$Z_{k,m_k-1} = \frac{1}{(m_k-2)!}\left(x_{k,2} y^*_k + x_{k,1} y^*_{k,1} + x_k y^*_{k,2}\right).$$

И так далее, для компоненты $Z_{k,2}$ получаем

$$Z_{k,3} = \frac{1}{2}(T-\lambda_k I)\, Z_{k,2} = \frac{1}{2!}\left(x_{k,m_k-2} y^*_k + x_{k,m_k-3} y^*_{k,1} + ... + x_k y^*_{k,m_k-2}\right)$$

$$(T-\lambda_k I)\, Z_{k,2} = \frac{1}{1!}\left(x_{k,m_k-2} y^*_k + x_{k,m_k-3} y^*_{k,1} + ... + x_k y^*_{k,m_k-2}\right),$$

$$Z_{k2} = \frac{1}{1!}\left(x_{k,m_k-1} y^*_k + x_{k,m_k-2} y^*_{k,1} + ... + x_k y^*_{k,m_k-1}\right).$$

Для компоненты $Z_{k,1}$ получаем

$$Z_{k,2} = (T-\lambda_k I)\, Z_{k,1} = \frac{1}{1!}\left(x_{k,m_k-1} y^*_k + x_{k,m_k-2} y^*_{k,1} + ... + x_k y^*_{k,m_k-1}\right),$$

$$Z_{k1} = x_{k,m_k} y^*_k + x_{k,m_k-1} y^*_{k,1} + ... + x_k y^*_{k,m_k}.$$

Теорема доказана.

Теорема 3 называется спектральной теоремы в форме М.В. Келдыша для произвольного линейного оператора в конечномерном пространстве.

Приведем одно полезное следствие данной теоремы.

Следствие 3 *Пусть оператор $T : X \to X$ такой, что выполнено утверждение 1 и сохранены его обозначения. Тогда для функции $f(t) = \frac{1}{t-\lambda}$ выполнено следующее операторное соотношение*

$$\mathcal{R}(\lambda; T) = -\sum_{k=1}^{s} \sum_{j=1}^{m_k+1} \frac{(j-1)!}{(\lambda-\lambda_k)^j} Z_{kj},$$

где

$$Z_{k1} = x_{k,m_k} y^*_k + x_{k,m_k-1} y^*_{k,1} + ... + x_k y^*_{k,m_k},$$

$$Z_{k2} = \frac{1}{1!}\left(x_{k,m_k-1}y_k^* + x_{k,m_k-2}y_{k,1}^* + ... + x_k y_{k,m_k-1}^*\right),$$

$$Z_{k3} = \frac{1}{2!}\left(x_{k,m_k-2}y_k^* + x_{k,m_k-3}y_{k,1}^* + ... + x_k y_{k,m_k-2}^*\right),$$

$$\ldots$$

$$Z_{k,m_k-1} = \frac{1}{(m_k-2)!}\left(x_{k,2}y_k^* + x_{k,1}y_{k,1}^* + x_k y_{k,2}^*\right),$$

$$Z_{k,m_k} = \frac{1}{(m_k-1)!}\left(x_{k,1}y_k^* + x_k y_{k,1}^*\right),$$

Замечание 1 *В случае $s = n$ в монографии [2] отмечено, что все $m_k = 0$ и $Z_{k1} = x_k y_k^*$.*

Новым моментом теоремы 3 является то, что операторы Z_{kj} выписаны через базисные элементы $x_k, x_{k1}, ..., x_{k,m_k}$ оператора T и базисные элементы $y_k, y_{k1}, ..., y_{k,m_k}$ оператора T^* при произвольных m_k.

Замечание 2 *Для вполне непрерывных операторов в Гильбертовом пространстве в работе М.В. Келдыша [3] получено представление главной части разложения Лорана резольвенты в окрестности полюса λ_k :*

$$\textit{главная часть } \mathcal{R}(\lambda;T) = \sum_{j=1}^{m_k+1} \frac{(j-1)!}{(\lambda-\lambda_k)^j} Z_{kj}.$$

Результат М.В. Келдыша следует из представления (8). Однако в работе М.В. Келдыша нет представления резольвенты на всем резольвентном множестве.

Список литературы

[1] Ланкастер П., *Теория матриц* (Москва: Наука, 1977), 277.

[2] Гельфанд И.М. *Лекции по линейной алгебре* (Москва: Добросвет, МЦНМО, 1998), 320.

[3] Келдыш М.В., "О полноте собственных функций некоторых классов несамосопряжённых линейных операторов *УМН* **51**:2 (1971): 15-41.

References

[1] Lancaster P., *Matrix Theory* (Moscow: Nauka, 1977), 277.

[2] Gelfand I.M. *Lectures on linear algebra* (Moscow: Dobrosvet, icnmo, 1998), 320.

[3] Keldysh M. V., "On the completeness of eigenfunctions of certain classes of non-self-adjoint linear operators *Advances in mathematical Sciences* **51**:2 (1971): 15-41.

IRSTI 27.39.25 DOI: https://doi.org/10.26577/JMMCS.2020.v107.i3.03

R.K. Kerimbaev, K.A. Dosmagulova, Zh.Kh. Zhunussova*
Al-Farabi Kazakh National University, Almaty, Kazakhstan
*e-mail: zhunussova777@gmail.com

ALGORITHMIC COMPLEXITY OF LINEAR NONASSOCIATIVE ALGEBRA

One of the central problems of algebraic complexity theory is the complexity of multiplication in algebras. For this, first, the concept of algebra is defined and the class of algebras under study is fixed. Then the concept of the algorithm and its complexity are clarified. in the most general sense, an algebra is a set with operations. An operation is defined, as a rule, as a function of one or more elements of a set, the set of values of which is the original set or some of its subset. Usually, a set of elementary operations is fixed, for example, a Boolean operation on two bits, addition or multiplication of two numbers, after which a computation model is fixed, for example, a sequential algorithm, at each step of which one elementary operation is performed on some inputs and the results of intermediate calculations, the result of which can be used to enter an elementary operation at subsequent steps of the algorithm. The most significant ones are the column-by-column multiplication algorithm, which has quadratic complexity (along the input length) and the row-by-column matrix multiplication algorithm, which has $O(mnp)$ complexity for multiplying $m \times n$ by $n \times p$ matrices. Estimation of the complexity of algebras from other more complex classes is relevant. in this paper, we derive an estimate for the complexity of a nondegenerate symmetric bilinear form over an algebraic closed field for a simple Jordan algebra, as well as an estimate for a Cayley-Dixon body and for a simple Lie algebra over a characteristic field.

Key words: algebra complexity, optimal algorithm, simple algebra, Cayley-Dixon body, Lie algebra, characteristic field.

Р.К. Керимбаев, Қ.А. Досмағұлова, Ж.Х. Жунусова*
Әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы қ., Қазақстан
*e-mail: zhunussova777@gmail.com

Кейбір сызықты ассоциативтік емес алгебраның алгоритмдік күрделілігі

Алгебралық күрделілік теориясының негізгі мәселелерінің бірі - алгебралардағы көбейтудің күрделілігі. Ол үшін, біріншіден, алгебра ұғымы анықталып, зерттелетін алгебралар класы бекітіледі. Содан кейін алгоритм түсінігі және оның күрделілігі нақтыланады. Жалпы мағынада алгебра - амалдардан тұратын жиынтық. Операция, ереже бойынша, жиынның бір немесе бірнеше элементтерінің функциясы ретінде анықталады, оның мәндері жиынтығы бастапқы жиын немесе оның кейбір бөлігі болып табылады. Әдетте, қарапайым операциялардың жиынтығы, мысалы, екі битке логикалық операция, екі санды қосу немесе көбейту, содан кейін есептеу моделі бекітілген, оған мысал - кезекті алгоритм, оның әр сатысында бір элементар амал орындалады. Кейбір кірістер мен аралық есептеулердің нәтижелері, олардың нәтижесі алгоритмнің келесі кезеңдерінде элементар әрекетті енгізу үшін қолданыла алады. Ең маңыздыларына баған бойынша көбейту алгоритмі, және $m \times n$ өлшемді матрицаны $n \times p$ өлшемді матрицаға көбейтетін квадраттық $O(mnp)$ күрделілігі бар (кіріс ұзындығы бойынша) көбейту алгоритмі болып табылады. Басқа күрделі кластардан алгебралардың күрделігін бағалау өте маңызды. Бұл жұмыста қарапайым йордан алгебрасы үшін алгебралық жабық өрістен азайтылмайтын симметриялы билинарлы форманың күрделілігінің бағасы, сонымен қатар Кейли-Диксон денесі мен қарапайым өріс үшін Ли алгебрасы үшін баға алынған.

Түйін сөздер: алгебраның күрделілігі, оңтайлы алгоритм, қарапайым алгебра, Кейли-Диксон денесі, Ли алгебрасы, характеристикалық өріс.

Р.К. Керимбаев, Қ.А. Досмағұлова, Ж.Х. Жунусова*
Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан
*e-mail: zhunussova777@gmail.com

Алгоритмическая сложность некоторых линейных неассоциативных алгебр

Одной из центральных задач алгебраической теории сложности является сложность умножения в алгебрах. Для этого сначала определяется понятие алгебры и фиксируется класс изучаемых алгебр. Затем уточняется понятие алгоритма и его сложности. В наиболее общем смысле алгеброй называется множество с операциями. Операция определяется, как правило, как функция одного или нескольких элементов множества, множеством значений которой является исходное множество или некоторое его подмножество. Обычно фиксируется некоторое множество элементарных операций, например, булева операция над двумя битами, сложение или умножение двух чисел, после чего фиксируется модель вычислений, например, последовательный алгоритм, на каждом из шагов которого выполняется одна элементарная операция над некоторыми входами и результатами промежуточных вычислений, результат которой может быть использован для входа элементарной операции на последующих шагах алгоритма. К наиболее значимым следует отнести алгоритм умножения чисел "в столбик имеющий квадратичную сложность (по длине входа) и алгоритм умножения матриц "строка на столбец имеющий сложность $O(mnp)$ для умножения матриц размера $m \times n$ на $n \times p$. Оценка сложности алгебр из других более сложных классов актуальна. В данной статье мы выводим оценку сложности невырожденной симметрической билинейной формы над алгебраическим замкнутым полем для простой йордановой алгебры, а также оценку для тела Кэли-Диксона и простой алгебры Ли над характеристическим полем.

Ключевые слова: сложность алгебры, оптимальный алгоритм, простая алгебра, тело Кэли-Диксона, алгебра Ли, характеристическое поле.

1 Introduction

The complexity $L(A)$ of a finite-dimensional algebra A is a multiplication number (non-scalar:), divisions of the optimal algorithm, computing the production of two elements of algebra.

In the work [1] for associated algebra the results are obtained:

1)$L(A) \geq L(A/radA) + 2 * dim(radA)$,

where $radA$ is a radical of algebra.

2)$L(A) \geq 2 * dimA - 1$,

where A is a simple algebra. More general: for simple algebra A and arbitrary algebra B it is proved, that

$$L(A \oplus B) \geq 2 * dimA - 1 + L(B)$$

As a result, for arbitrary finite-dimensional associative algebra A the final estimation is obtained:

3)$L(A) \geq 2 * dimA - t$,

where t is a number of maximal two-sided ideal of algebra A. Naturally, the issue about complexity of algebra from other classes is arisen.

We note, that the 1-st result, as a sequence of structural theorems [2], are true for jordan alternative algebra.

The 2-nd result for jordan algebra, in general, is not true. We show in §2 of this work, that for simple jordan algebra $B(f) = K * 1 + V$ nondegenerate symmetric bilinear form f over algebraic closed field K the complexity

$$L(B(f)) = 2 * dimB(f) - 2.$$

In §3 we show for keli-Dixon body C, that

$$15 \leq Z(C) \leq 30$$

In §4 we show for simple Li algebra $sl(2,K)$ over filed K the characteristics $\neq 2$, that

$$L(sl(2,K)) = 5.$$

2 The main definitions

We present some definitions from [1] below. Let K be infinite filed, $x_1, \ldots, x_n$ are variables over K.

Definition 1 *The sequence of rational functions $g_1, ..., g_r \in K(x_1, ..., x_n)$ are called by computing sequence, if for any number $\rho \leq r$ there exist*

$$u_\rho, v_\rho \in K + Kx_1 + ... + Kx_n + Kg_1 + ...Kg_{\rho-1},$$

such, that

$$g_\rho = u_\rho * v_\rho$$

or

$$g_\rho = u_\rho / v_\rho, v_\rho \neq 0.$$

Definition 2 *Let $f_1, ..., f_q \in K(x_1, ..., x_n)$. The complexity $L(f_1, ..., f_q)$ of set $f_1, ..., f_q$ is a least r with property: there exists a computing sequence $g_1, ..., g_r$ such, that for all $i \leq q$*

$$f_i \in K + Kx_1 + ... + Kx_n + Kg_1 + ...Kg_r$$

Let E, W be finite-dimensional vector K - spaces with basis, accordingly $e_1, ..., e_r$ and $\hat{e}_1, ...\hat{e}_q$.

Definition 3 *Mapping $f : E \to W$ is called by quadratic, if there exist quadratic forms $f_1, ..., f_q$ of $K[x_1, ..., x_n]$ such that for all $\xi_1, ..., \xi_n \in K$*

$$f(\sum_{i=1}^{n} \xi_i e_i) = \sum_{j=1}^{q} f_j(\xi_1, ..., \xi_n)\hat{e}_j$$

$L(f) = L(f_1, ..., f_q)$ is called by complexity f, where $f_1, ..., f_q$ are considered as elements $K(x_1, ..., x_n)$.

Let A is a finite-dimensional algebra with unit, $e_1, ..., e_n$ is a basis of vector space.

$$e_i * e_j = \sum_{m=1}^{n} \tau_{ijm} e_m,$$

where $\tau_{ijm} \in K, i, j, = 1, ..., n$. Then we get

$$(\sum_{i=1}^{n} \xi_i e_i) * (\sum_{j=1}^{n} \eta_j e_j) = \sum_{m=1}^{n} (\sum_{i,j=1}^{n} \tau_{ijm} \xi_i \eta_j) e_m$$

The elements $x, y \in A$ are considered as vector-columns with coordinates $x_1, ..., x_n$ and $y_1, ..., y_n$ accordingly. Then for $\sum_{i,j=1}^{n} \tau_{ijm} x_i y_j$ we get the following:

$$\sum_{i,j=1}^{n} \tau_{ijm} x_i y_j = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}^t \begin{pmatrix} \tau_{11m} & \tau_{12m} & \tau_{1nm} \\ \tau_{21m} & \tau_{22m} & \tau_{2nm} \\ \tau_{n1m} & \tau_{n2m} & \tau_{nnm} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = x^t T_m y,$$

where x^t is a vector-line, $T_m \in M_n(K), m = 1, \ldots, n$. For any $x, y \in A$ we get

$$xy = \sum_{m=1}^{n} (x^t T_m y) e_m$$

Let $T = \{T_1, \ldots, T_n\}$. We consider $M \subseteq M_n(K)$ - subset, for which power $|M| = r, r > 0, linM$ is a linear membrane M.

Definition 4 *M is called by the algorithm of the length r of algebra A, if the conditions are held:*
1) M consists of linearly independent matrixes,
2) for any $m \in M, rang = 1$,
3) $T \leq linM$.

Algorithm M is called by optimal, if its length does not exceed of the length of any algorithm of algebra A.

Multiplication in algebra A is a bilinear mapping $f : A \oplus A \to A$. For any $x, y \in A$ we get

$$f(x + y) = xy = \sum_{m=1}^{n} x^t T_m y e_m = \sum_{m=1}^{n} f_m(x_1, ..., x_n, y_1, ..., y_n) e_m = \sum_{m=1}^{n} f_m(x, y) e_m,$$

where $x^t T_m y = f_m(x_1, ..., x_n, y_1, ..., y_n) = f_m(x, y) \in k[x_1, ..., x_n, y_1, ..., y_n]$- are quadratic forms, $m = 1, ..., n$. In fact, $f : A \bigoplus A \to A$ is quadratic mapping.

Definition 5 *Complexity of algebra A is called complexity of quadratic mapping $f : A \bigoplus A \to A$, defined by the rule:*

$$f(x + y) = xy.$$

We denote the complexity of algebra A by $L(A)$.

Proposal 1 *$L(A)$ is equal to the optimal algorithm of algebra A.*

Proof. If M is optimal algorithm of the length r of algebra A, then

$$f_m(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{j=1}^{r} d_{m_j} x^t M_j y,$$

where $M_j \in M, j = 1, \ldots, r$. Any matrix C of rang 1 is represented in the form

$$C = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} (b_1, \ldots, b_n).$$

Therefore for each matrix M_j there exist such vector-lines u_j, v_j that $M_j = u_j^t v_j$; moreover

$$x^t M_j y = x^t u_j^t v_j y = u_j(x) v_j(y), j = 1, \ldots, r,$$

where $u_j(x) = (x^t, u_j), v_j(y) = (y^t, v_j)$ are linear forms.

As a result we get

$$f_m(x, y) = \sum_{j=1}^{r} d_{mj} u_j(x) v_j(y)$$

hence, that $L(A) = L(f) \leq r$.

Let $L(f) = L(f_1, \ldots, f_n) = k$. In the work [1] is proved, that the set of quadratic forms is optimally calculated without division. There exists

$$u_\rho \in K + Kx_1 + \cdots + Kx_n,$$

$$v_\rho \in K + Ky_1 + \cdots + Ky_n,$$

$\rho = 1, \ldots, k$, such that

$$f_m(x, y) = \sum_{\rho=1}^{k} d_{m\rho} u_\rho(x) v_\rho(y).$$

If $u_\rho, v_\rho, \rho = 1, \ldots, k$, are linear dependent, then the number k can be decreased, consequently u_ρ, v_ρ are linear independent.

Let $u_\rho(x) = (u_\rho, x^t), v_\rho(y) = (v_\rho, y^t)$, for some vectors u_ρ, v_ρ.

Then the matrix $M_\rho = u_\rho^t v_\rho$ has a rang 1, and we get

$$u_\rho(x) v_\rho(y) = x^t M_\rho y.$$

Then $f_m(x, y) = \sum_{j=1}^{k} d_{mj} x^t M_j y = x^t (\sum_{j=1}^{k} d_{mj} M_j) y$, on the other hand $f_m(x, y) = x^t T_m y$, hence $T_m \in lin(M_1, \ldots, M_k)$. We have constructed the algorithm, the length of which is equal to $L(A)$ Now it is clear, that $L(A) \geq r$ and finally, we get, that $L(A) = r$.

Example 1 *Let C are field of complex numbers. For any $x, y \in C$ we get*

$$xy = (x_1 y_1 - x_2 y_2) + (x_1 y_2 - x_2 y_2) i,$$

i.e. $xy = x^t \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} y + x^t \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} yi,$

For C $T = \left\{ T_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, T_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$. *We take*

$$M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

Then $L(C) \leq 3$. We suppose, that $M = \{M_1, M_2\}$ is an algorithm of the length 2 for C. Then there exist $d_1, d_2, d_3, d_4 \in R$ such that $d_1 d_4 - d_2 d_3 \neq 0$ and

$$\begin{cases} d_1 M_1 + d_2 M_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \\ d_3 M_1 + d_4 M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{cases}$$

Let $d_1 \neq 0$, *then* $M_1 = \frac{1}{d_1 d_4 - d_2 d_3} \begin{pmatrix} -d_3 & d_1 \\ d_1 & d_3 \end{pmatrix}$ *and* $d_1^2 + d_3^2 = 0$, *i.e.* $d_1 = 0$, *contradiction,* $L(C) = 3$.

3 Complexity of $B(f)$-jordan algebra of nondegenerated symmetric bilinear form

$B(f) = K1 + V$ is jordan algebra [2] of symmetric nondegenerated bilinear form $f : V \times V \to K$, where K is a field, V is the vector space over K dimensionality n. Multiplication in $B(f)$ is defined:

$$(x_0 * 1 + x)(y_0 * 1 + y) = (x_0 y_0 + f(x, y))(x_0 y_0 + y_0 x).$$

Theorem 1 *a) If* K *is algebraic closed field, then*

$$L(B(f)) = 2n.$$

b) If $K = \Re$ *is a field of the real numbers, then*

$$L(B(f)) = \begin{cases} 2n+1, if \quad f \quad is \quad negative \quad defined; \\ 2n, in \quad the \quad other \quad case. \end{cases}$$

Proof. By choosing the canonical basis $l_1, \ldots, l_n$ in V with respect to f for any $a, b \in B(f)$ we obtain, that

$$ab = (x_0 1 + x)(y_0 1 + y) = (x_0 y_0 + x_1 y_1 + \cdots + x_k y_k -$$

$$-x_{k+1} y_{k+1} - \cdots - x_n y_n)1 + (x_0 y_1 + x_0 y_1) l_1 + \cdots + (x_0 y_n + x_n y_0) l_n,$$

where $K = 0, 1, \ldots, n$ for $K = \Re$ and $k = n$, if the field K is algebraic closed. If $K = 0$, then we take

$$f_0 = x_0 y_0, f_i = \Big(\sqrt{\frac{1}{n}} x_0 + x_i\Big)\Big(\sqrt{\frac{1}{n}} y_0 + y_i\Big),$$

$$g_i = \Big(\sqrt{\frac{1}{n}} x_0 + x_i\Big)\Big(\sqrt{\frac{1}{n}} y_0 - y_i\Big), i = 1, \ldots, n.$$

Then

$$ab = \Big(2f_0 - \sum_{i=1}^{n} \frac{f_i + g_i}{2}\Big)1 + \sum_{i=1}^{n} \frac{f_i - g_i}{2} l_i.$$

If $0 < k < n$, then we take

$$f_i = \Big(\sqrt{\frac{2}{k}} x_0 + x_i\Big)\Big(\sqrt{\frac{2}{k}} y_0 + y_i\Big), g_i = \Big(\sqrt{\frac{2}{k}} x_0 - x_i\Big)\Big(\sqrt{\frac{2}{k}} y_0 - y_i\Big), i = 1, \ldots, k,$$

$$f_i = \Big(\sqrt{\frac{2}{n-k}} x_0 + x_i\Big)\Big(\sqrt{\frac{2}{n-k}} y_0 + y_i\Big), i = k+1, \ldots, n,$$

$$g_i = \Big(\sqrt{\frac{2}{n-k}} x_0 - x_i\Big)\Big(\sqrt{\frac{2}{n-k}} y_0 - y_i\Big), i = k+1, \ldots, n.$$

Then

$$ab = \Big(\sum_{i=1}^{k} \frac{f_i + g_i}{2} - \sum_{i=k+1}^{n} \frac{f_i + g_i}{2}\Big)1 + \sum_{i=1}^{k} \sqrt{\frac{k}{2}} \frac{f_i - g_i}{2} l_i + \sum_{i=k+1}^{k} \sqrt{n-k} \frac{f_i - g_i}{2} l_i.$$

If $k = n$, then

$$f_i = \Big(\sqrt{\frac{1}{n}} x_0 + x_i\Big)\Big(\sqrt{\frac{1}{n}} y_0 + y_i\Big),$$

$$g_i = \Big(\sqrt{\frac{1}{n}} x_0 - x_i\Big)\Big(\sqrt{\frac{1}{n}} y_0 - y_i\Big), i = 1, \ldots, n$$

and we get

$$ab = \sum_{i=1}^{k} \frac{f_i + g_i}{2} 1 + \sum_{i=1}^{n} \sqrt{n} \frac{f_i - g_i}{2} l_i.$$

Thus, we obtain, that

$$L(B(f)) \leq 2n, \tag{1}$$

Under $0 < K < n$ or algebraic closed K,

$$L(B(f)) \leq 2n + 1, \quad K = 0. \tag{2}$$

Now the elements $a, b \in B(f)$ are considered as vector-columns.

Then we get

$$ab = a^t \begin{pmatrix} E_{k+1} & 0 \\ 0 & -E_{n-k} \end{pmatrix} b \cdot 1 + \sum_{i=2}^{n+1} a^t (E_{1i} + E_{2i}) b \cdot l_{i-1} =$$

$$= a^t C_0 b + \sum_{i=2}^{n+1} a^t C_{i-1} b \cdot l_{i-1},$$

where $C_0, C_1, \ldots, C_n \in M_{n+1}(K)$. Let $M \subseteq M_{n+1}(K)$ is the algorithm of the length r for $B(f)$. Then we get

$$C_i = \sum_{j=0}^{r} d_{ij} x_j,$$

where $i = 0, 1, \ldots, n, x_j \in M, d_{ij} \in K$. We consider a matrix of order $n \times r$,

$$\begin{pmatrix} d_{11} & \cdots & d_{1n} & \cdots & d_{1r} \\ d_{21} & \cdots & d_{2n} & \cdots & d_{2r} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ d_{n1} & \cdots & d_{nn} & \cdots & d_{nr} \end{pmatrix}.$$

Since $C_1, \ldots, C_n$ are linear independent, that there exists a minor M_1 of order $n \times n$, that $|M_1| \neq 0$. Without limitation of generality, we can assume, that

$$M_1 = \begin{pmatrix} d_{11} & \cdots & d_{1n} \\ \cdots & \cdots & \cdots \\ d_{n1} & \cdots & d_{nn} \end{pmatrix}.$$

Then from the system of equations

$$\begin{cases} d_{11}x_1 + \cdots + d_{1n}x_n = C_1 - \sum_{j=n+1}^{r} d_{1j}x_j = B_1 \\ d_{n1}x_2 + \cdots + d_{nn}x_n = C_n - \sum_{j=n+1}^{r} d_{nj}x_j = B_n \end{cases}$$

We find x_i;

$$x_i = \frac{1}{|M_i|}\sum_{j=1}^{n}(-1)^{i+j}M_1^{ij}B_j, i = 1, \ldots, n.$$

where M_1^{ij} is a minor of the element d_{ij} of the matrix M_1. By substituting $x_i, i = 1, \ldots, n$ to $C_0 = \sum_{j=1}^{r} d_{0j}x_i$ we obtain

$$C_0 = \frac{1}{|M_1|}(\gamma_1 B_1 - \gamma_2 B_2 + \cdots + (-1)^{n+1}\gamma_n B_n) + \sum_{j=n+1}^{r} d_{0j}x_j,$$

where

$$\gamma_1 = \begin{vmatrix} d_{01} & \cdots & d_{0n} \\ d_{21} & \cdots & d_{2n} \\ \cdots & \cdots & \cdots \\ d_{n1} & \cdots & d_{nn} \end{vmatrix}, \ldots, \gamma_n = \begin{vmatrix} d_{01} & \cdots & d_{0n} \\ d_{21} & \cdots & d_{2n} \\ \cdots & \cdots & \cdots \\ d_{n-11} & \cdots & d_{n-1n} \end{vmatrix}.$$

Hence

$$\Delta = C_0 + \sum_{i=1}^{n}\frac{(-1)^i\gamma_i}{|M_1|}C_i = \sum_{j=n+1}^{r}\frac{d_j}{|M_1|}x_i, \tag{3}$$

where

$$d_j = \begin{vmatrix} d_{01} & \cdots & d_{0n} & d_{0j} \\ d_{21} & \cdots & d_{2n} & d_{1j} \\ \cdots & \cdots & \cdots & \cdots \\ d_{n-11} & \cdots & d_{n-1n} & d_{nj} \end{vmatrix}, j = n+1, ..., r. \tag{4}$$

We assume $\delta_1 = \frac{(-1)^i\gamma_i}{|M_1|}, i = 1, \ldots, n$. Then in (3) for Δ we get

$$\Delta = \begin{pmatrix} 1 & \delta_1 & \cdots & \delta_k & \delta_{k+1} & \cdots & \delta_n \\ \delta_1 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \delta_k & 0 & \cdots & 1 & 0 & \cdots & 0 \\ \delta_{k+1} & 0 & \cdots & 0 & -1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \delta_n & 0 & \cdots & 0 & 0 & \cdots & -1 \end{pmatrix}. \tag{5}$$

Let $T_{12}(-\delta_1), \ldots, T_{1k+1}(-\delta_k), T_{1k+2}(\delta_{k+1}), \ldots, T_{1n+1}(\delta_n) \in M_{n+1}(K)$ be transfection. We assume

$$U = T_{1n+1}(\delta_n)\ldots T_{12}(-\delta_1). \tag{6}$$

Then

$$U\Delta U^t = \begin{pmatrix} 1-\delta_1^2-\cdots-\delta_k^2+\cdots+\delta_n^2 & 0 & 0 \\ 0 & E_k & 0 \\ 0 & 0 & -E_{n-k} \end{pmatrix}$$

hence we get, that $rang\Delta \geq n$. It is shown, that in (3) $r \geq 2n$. Together with (1) we obtain

$$L(B(f)) = 2n,$$

if $0 < k < n$ or K is algebraic closed. If $k = 0$ and $K = R$ is a field of the real numbers, then $rang\Delta = n + 1$.

Consequently $r \geq 2n + 1$. Together with (2) it leads, that

$$L(B(f)) = 2n + 1.$$

The theorem is proved.

4 Complexity of the Keli-Dixon body

Let C be a Keli-Dixon body, $1, l_1, \ldots, l_7$ is a basis C of the multiplication table: Let $x, y \in C$.

Table 1 – The multiplication table

0	l_1	l_2	l_3	l_4	l_5	l_6	l_7
l_1	-1	l_3	$-l_2$	l_5	$-l_4$	$-l_7$	l_6
l_2	$-l_3$	-1	l_1	l_6	l_7	$-l_4$	$-l_5$
l_3	l_2	$-l_1$	-1	l_7	$-l_6$	l_5	$-l_4$
l_4	$-l_5$	$-l_6$	$-l_7$	-1	l_1	l_2	l_3
l_5	l_4	$-l_7$	l_6	$-l_1$	-1	$-l_3$	l_2
l_6	l_7	l_4	$-l_5$	$-l_2$	l_3	-1	$-l_1$
l_7	$-l_6$	l_5	l_4	$-l_3$	$-l_2$	l_1	-1

Using the table, we compute the production x, y by its coordinates.

$$\begin{aligned} xy = {} & (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8) \cdot 1 \\ & +(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 - x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7) \cdot e_1 \\ & +(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6) \cdot e_2 \\ & +(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_6) \cdot e_3 \\ & +(x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4) \cdot e_4 \\ & +(x_1y_6 + x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3) \cdot e_5 \\ & +(x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2) \cdot e_6 \\ & +(x_1y_8 - x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1) \cdot e_7 \end{aligned}$$

$$= C_1 \cdot 1 + C_2 \cdot e_1 + C_3 \cdot e_2 + C_4 \cdot e_3 + C_5 \cdot e_4 + C_6 \cdot e_5 + C_7 \cdot e_6 + C_8 \cdot e_7.$$

Now we assume

$$f_1 = (x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8)(y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8),$$

$$f_2 = (x_1 + x_2 + x_3 + x_4 - x_5 - x_6 - x_7 - x_8)(y_1 + y_2 + y_3 + y_4 - y_5 - y_6 - y_7 - y_8),$$

$$f_3 = (x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8)(y_1 - y_2 + y_3 - y_4 + y_5 - y_6 + y_7 - y_8),$$

$$f_4 = (x_1 - x_2 + x_3 - x_4 - x_5 + x_6 - x_7 + x_8)(y_1 - y_2 + y_3 - y_4 - y_5 + y_6 - y_7 + y_8),$$

$$f_5 = (x_1 + x_2 - x_3 - x_4 + x_5 + x_6 - x_7 - x_8)(y_1 + y_2 - y_3 - y_4 + y_5 + y_6 - y_7 - y_8),$$

$$f_6 = (x_1 + x_2 - x_3 - x_4 - x_5 - x_6 + x_7 + x_8)(y_1 + y_2 - y_3 - y_4 - y_5 - y_6 + y_7 + y_8),$$

$$f_7 = (x_1 - x_2 - x_3 + x_4 + x_5 - x_6 - x_7 + x_8)(y_1 - y_2 - y_3 + y_4 + y_5 - y_6 - y_7 + y_8),$$

$$f_8 = (x_1 - x_2 - x_3 + x_4 - x_5 + x_6 + x_7 - x_8)(y_1 - y_2 - y_3 + y_4 - y_5 + y_6 + y_7 - y_8),$$

$$f_9 = x_1y_1, f_{10} = x_4y_3, f_{11} = x_6y_5, f_{12} = x_7y_8, f_{13} = x_2y_4,$$

$$f_{14} = x_7y_5, f_{15} = x_8y_6, f_{16} = x_3y_2, f_{17} = x_6y_7,$$

$$f_{18} = x_8y_5, f_{19} = x_2y_6, f_{20} = x_3y_7, f_{21} = x_4y_8,$$

$$f_{22} = x_3y_8, f_{23} = x_5y_2, f_{24} = x_7y_4,$$

$$f_{25} = x_4y_6, f_{26} = x_5y_3, f_{27} = x_8y_2, f_{28} = x_2y_7, f_{29} = x_6y_3, f_{30} = x_5y_4$$

Then

$$C_1 = \frac{1}{8}(16f_9 - f_1 - f_2 - f_3 - f_4 - f_5 - f_6 - f_7 - f_8),$$

$$C_2 = \frac{1}{8}(f_1 + f_2 + f_5 + f_6 - f_3 - f_4 - f_7 - f_8) - 2(f_{10} + f_{11} + f_{12}),$$

$$C_3 = \frac{1}{8}(f_1 + f_2 + f_3 + f_4 - f_5 - f_6 - f_7 - f_8) - 2(f_{13} + f_{14} + f_{15}),$$

$$C_4 = \frac{1}{8}(f_1 + f_2 + f_7 + f_8 - f_3 - f_4 - f_5 - f_6) - 2(f_{16} + f_{17} + f_{18}),$$

$$C_5 = \frac{1}{8}(f_1 - f_4 + f_5 - f_8 - f_2 + f_3 - f_6 + f_7) - 2(f_{19} + f_{20} + f_{21}),$$

$$C_6 = \frac{1}{8}(f_1 + f_4 + f_5 + f_8 - f_2 - f_3 - f_6 - f_7) - 2(f_{22} + f_{23} + f_{24}),$$

$$C_7 = \frac{1}{8}(f_1 + f_4 + f_5 + f_8 - f_2 - f_4 - f_5 - f_7) - 2(f_{25} + f_{26} + f_{27}),$$

$$C_8 = \frac{1}{8}(f_1 + f_4 + f_6 + f_7 - f_2 - f_3 - f_5 - f_8) - 2(f_{28} + f_{29} + f_{30}),$$

Hence we get, that $L(C) \leq 30$. Let $L(C) = r$ and the elements $x, y \in C$ are considered as vector-columns, then $C_i = x^t C_i y, i = 1, \ldots, 8$ where $C_i \in M_8(K)$ and there exists an algorithm M of the length r for which

$$C_i = \sum_{j=1}^{r} d_{ij} x_i, i = 1, \ldots, 8,$$

where $x_j \in M \subseteq M_8(K), i = 1, \ldots, r, d_{ij} \in K$. For Keli-Dixon body C the matrix Δ has the form

$$\Delta = \begin{pmatrix} 1 & \delta_1 & \delta_2 & \delta_3 & \delta_4 & \delta_5 & \delta_6 & \delta_7 \\ \delta_1 & -1 & \delta_3 & -\delta_2 & \delta_5 & -\delta_4 & -\delta_7 & \delta_6 \\ \delta_2 & -\delta_3 & -1 & \delta_1 & \delta_6 & \delta_7 & -\delta_4 & -\delta_5 \\ \delta_3 & \delta_2 & -\delta_1 & -1 & \delta_7 & -\delta_6 & \delta_5 & -\delta_4 \\ \delta_4 & -\delta_5 & -\delta_6 & -\delta_7 & -1 & \delta_4 & \delta_2 & \delta_3 \\ \delta_5 & \delta_4 & -\delta_7 & \delta_6 & -\delta_1 & -1 & -\delta_3 & \delta_2 \\ \delta_6 & \delta_7 & \delta_4 & -\delta_5 & -\delta_2 & \delta_3 & -1 & -\delta_1 \\ \delta_7 & -\delta_6 & \delta_5 & \delta_4 & -\delta_3 & -\delta_2 & \delta_1 & -1 \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}.$$

Then $detA_{11} \cdot det(A_{22} - A_{21}A_{11}^{-1}A_{12}) = d_1^4(1 + d_1d_2) \neq 0$, where $d_1 = (1 + d_1^2 + d_2^2 + d_3^2 + d_4^2)$, $d_2 = d_4^2 + d_5^2 + d_6^2 + d_7^2$. On the other hand $\Delta = \sum_{j=8}^{r} \frac{d_j}{|M_1|}x_j$, consequently $r - 7 \geq 8$, i.e. $L(C) \geq 15$. By this way it is proved the following theorem.

Theorem 2 *C is a Keli-Dixon body. Then* $15 \leq L(C) \leq 30$.

5 Complexity of Li algebra

In this section we calculate the complexity of the least simple Li algebra $sl(2, K)$ over field K of characteristics $\neq 2$. We mention, that $sl(2, K)$ consists of 2×2 matrixes over K with zero trace: as its basis the elements can be taken $l_1 = l_{11} - l_{22}, l_2 = l_{12}, l_3 = l_{21}$ where l_{ij} are ordinary matrix units. For any $x = \sum_{i=1}^{3} x_i l_i = \sum_{i=1}^{3} y_i l_i$ we have

$$[x, y] = 2(x_1y_2 - x_2y_1)l_2 - 2(x_1y_3 - x_3y_1)l_3 + (x_2y_3 - x_2y_3)l_1 =$$

$$= C_1l_1 + 2C_2l_2 + 2C_3l_3,$$

where

$$C_1(x, y) = x_2y_3 - x_3y_2, C_2(x, y) = x_1y_2 - x_2y_1, C_3(x, y) = x_3y_1 - x_1y_2.$$

We assume

$$f_1 = (x_1 - x_2 - x_3)(y_1 - y_2 + y_3),$$

$$f_2 = (x_1 + x_2 + x_3)(y_1 + y_2 - y_3),$$

$$f_3 = (x_1 + x_2 - x_3)(y_1 + y_2 + y_3),$$

$$f_4 = (x_1 - x_2 + x_3)(y_1 - y_2 - y_3),$$

$$f_5 = x_1y_2.$$

Then

$$C_1 = -\frac{1}{4}(f_1 + f_2 - f_3 - f_4),$$

$$C_3 = \frac{1}{2}(f_2 - f_1) + C_1$$

$$C_2 = \frac{1}{2}(f_2 - f_1) - C_3 - 2f_5.$$

Therefore

$$sl(2,K) \leq 5.$$

Let $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$; then we get

$$C_i = xC_iy^t, i = 1, 2, 3,$$

where

$$C_1 = l_{23} - l_{32}, C_2 = l_{12} - l_{21}, C_3 = l_{31} - l_{13}.$$

Let $L(sl(2,K)) = r$ then there exists an algorithm of the length r for $sl(2,K)$ i.e. there exist the matrixes $X_1, \ldots, X_r$ of $M_3(K)$ rang 1 such that

$$C_i = \sum_{i=1}^{r} \alpha_{ij} X_j, i = 1, 2, 3. \tag{7}$$

The procedure is repeated for $B(f)$, and we get

$$\Delta = C_2 + \delta_1 C_3 + \delta_2 C_1 = \sum_{j=2}^{r} \frac{\alpha_j}{|M_1|} X_j, \tag{8}$$

where

$$|M_1| = \begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{31} & \alpha_{32} \end{vmatrix}, \alpha_j = \begin{vmatrix} \alpha_{21} & \alpha_{22} & \alpha_{2j} \\ \alpha_{11} & \alpha_{12} & \alpha_{1j} \\ \alpha_{31} & \alpha_{32} & \alpha_{3j} \end{vmatrix}. j = 3, \ldots, r.$$

Since $det\Delta = \delta_1\delta_2 - \delta_1\delta_2 = 0$, then $rang\Delta = 2$, i.e. $r \geq 4$. Let $r = 4, C_i = \sum_{j=1}^{4} \alpha_{ij} X_j, i = 1, 2, 3$. Since C_1, C_2, C_3 are linear independent, we can suppose, that

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix} \neq 0.$$

Let $|M_{23}| = \alpha_{11}\alpha_{32} - \alpha_{12}\alpha_{31} \neq 0$. Then under $i = 1, 3$ we find X_1 из (7).

$$X_1 = \frac{1}{|M_{23}|}(\alpha_{32}C_3 - \alpha_{12}C_1 + \gamma_3^1 X_3 + \gamma_4^1 X_4) = \gamma_1 C_3 + \gamma_2 C_1 + \gamma_3 X_3 + \gamma_4 X_4$$

Let

$$R = \begin{pmatrix} 1 & 0 & \delta_2 \\ 0 & 1 & \delta_1 \\ 0 & 0 & 1 \end{pmatrix}, L = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ \delta_2 & \delta_1 & 1 \end{pmatrix},$$

then from (8) we obtain

$$L\Delta R = d_3' L X_3 R + d_4' L X_4 R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, d_3 \neq 0, d_4 \neq 0.$$

Now we show, that if X, Y is a matrix of rang 1 and

$$X + Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tag{9}$$

then X, Y have the form

$$\begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Let

$$X = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} (x_1, x_2, x_3), Y = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} (y_1, y_2, y_3).$$

Then from (9) we get

$$\begin{cases} a_1x_1 + b_1y_1 = 1 \\ a_2x_1 + b_2y_1 = 0 \\ a_3x_1 + b_3y_1 = 0 \end{cases}, \begin{cases} a_1x_1 + b_1y_1 = 0 \\ a_2x_1 + b_2y_1 = 1 \\ a_3x_1 + b_3y_1 = 0 \end{cases}, \begin{cases} a_1x_1 + b_1y_1 = 0 \\ a_2x_1 + b_2y_1 = 0 \\ a_3x_1 + b_3y_1 = 0 \end{cases}.$$

It leads us,

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \neq 0, \begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix} = 0, \begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} = 0.$$

Hence we get, that $x_3 = y_3 = 0$. If $a_3 \neq 0 \neq b_3$, then $a_1b_2 - b_1a_2 = b_1b_2\frac{a_3}{b_3} - b_1b_2\frac{a_3}{b_3} = 0$, consequently $a_3 = b_3 = 0$. Now, let

$$d_3'LX_3R = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 0 \end{pmatrix}_1, d_4'LX_4R = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 0 \end{pmatrix}_2.$$

Then

$$Y_1 = LX_1R = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ \delta_2 & \delta_1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & -\gamma_1 \\ 0 & 0 & \gamma_2 \\ \gamma_1 & -\gamma_2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & \delta_2 \\ 0 & 1 & \delta_1 \\ 0 & 0 & 1 \end{pmatrix} + \frac{\gamma_3}{d_3'}(d_3'LX_3R) +$$

$$+\frac{\gamma_4}{d_4'}(d_4'LX_4R) = \begin{pmatrix} 0 & 0 & \gamma_2 \\ 0 & 0 & -\gamma_1 \\ \gamma_1 & -\gamma_2 & 0 \end{pmatrix} + \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} * & * & \gamma_2 \\ * & * & -\gamma_1 \\ \gamma_1 & -\gamma_2 & 0 \end{pmatrix}.$$

Since $rang Y_1 = 1$ we obtain, that $\gamma_1 = \gamma_2 = 0$, i.e. $|M_{23}| = 0$, is the contradiction. By this way the following theorem is proved.

Theorem 3 *Let $sl(2, K)$ is Li algebra 2×2 with zero trace over the field K of characteristics $\neq 2$. Then $L(sl(2, K)) = 5$.*

6 Conclusion

A dependence on the field of the complexity algebra is presented in the paper. For example, there is a difference between the complexity of nondegenerate bilinear form of algebra in the field of the real numbers and complex numbers.

References

[1] A. Alder, Shtrassen F. "Algorithmic complexity of linear algebra. Algorithms in the modern mathematics and its applications **2** (1978): 124.

[2] K.A. Zhevlakov, A.M. Slinko, I.P. Shestakov, A.I. Shirshov, "Rings, closed to associative *M.: Science.* (1978).

[3] V. Strassen, "Vermeidung Von Divissionen *I. fur reine und angew. Mathematik.* **264** (1973): 184–202.

2-бөлім **Раздел 2** **Section 2**

Механика **Механика** **Mechanics**

МРНТИ 30.19.31 DOI: https://doi.org/10.26577/JMMCS.2020.v107.i3.04

Ш.А. Алтынбеков*, А.Д. Ниязымбетов
Южно-Казахстанский государственный педагогический университет, г. Шымкент, Казахстан
*e-mail: sh.altynbekov@mail.ru

МЕТОДЫ ПРИКЛАДНОЙ МАТЕМАТИКИ В РЕШЕНИЯХ ЗАДАЧИ ТЕОРИИ КОНСОЛИДАЦИИ НЕОДНОРОДНЫХ НАСЛЕДСТВЕННО-СТАРЕЮЩИХ ГРУНТОВ

Вопросы совершенствования существующих методов прогноза осадки оснований сооружений, алгоритмизация решения их задачи ещё не сняты с повестки дня научных исследований. Подтверждением этому служат ежегодно проводимые международные конференции, симпозиумы и конгрессы в сфере промышленного, нефтепромышленного, гражданского и гидротехнического строительства. Основной целью исследования явилось совершенствование существующих методов фильтрационной теорий консолидации применительно к неоднородным грунтам и применение её для решения задачи. Сформулирована математическая постановка пространственной квазилинейной краевой задачи консолидации неоднородного наследственно-стареющего грунта. Здесь, неоднородность грунта обусловлена изменением его модуля деформации, мера ползучести и коэффициента бокового давления в процессе консолидации согласно экспоненциальному закону по глубине. Квазилинейность краевой задачи определена через коэффициент фильтрации. В работе принято, что коэффициент фильтрации зависит от коэффициента пористости. При учете неоднородности грунта не всегда удается получить аналитические решения задачи. Применение метода Фурье оставляет нас на полпути. Чтобы выйти из этой ситуации предложена функция аппроксимации. Исследована его погрешность. При малых значениях параметров неоднородности точность аппроксимации высока. Для решения задачи применены: метод итерации, метод наименьших квадратов, метод введения новой неизвестной функции, метод преобразования неоднородных граничных условий в однородные, метод Фурье, метод аппроксимации, метод введение новых переменных, метод разложение по собственным функциям, а для расчета осадок основании сооружений - метод В.А. Флорина.

Ключевые слова: консолидация, грунт, коэффициент фильтрации, уплотнения, аппроксимация.

Ш.А. Алтынбеков*, А.Д. Ниязымбетов
Оңтүстік Қазақстан мемлекеттік педагогикалық университеті, Шымкент қ., Қазақстан
*e-mail: sh.altynbekov@mail.ru

Біртекті емес тұқым қуалайтын-қартайған топырақтар консолидация теориясының есептерін шешудегі қолданбалы математика әдістері

Құрылыс іргетастарының шөгу процесін болжаудың қолданыстағы әдістерін жетілдіру, олардың есептерін шешуді алгоритмдеу мәселелері ғылыми зерттеулердің күн тәртібінен алынған жоқ. Мұны өнеркәсіптік, мұнай, азаматтық және гидротехникалық құрылыс саласындағы жыл сайынғы халықаралық конференциялар, симпозиумдар мен конгрестер

растайды. Зерттеудің негізгі мақсаты бір текті емес топырақтарға қолданылатын консолидациясының фильтрациялау теорияларының бар әдістерін жетілдіру және оны есепті шешу үшін қолдану болып табылады. Бір текті тұқым қуалайтын-қартайған топырақты біріктірудің кеңістіктік квазисызықты шеттік есебінің математикалық қойылымы қалыптастырылды. Мұнда топырақтың біртектілігі оның деформация Модулінің өзгеруімен, тереңдігі бойынша экспоненциалды заңға сәйкес консолидация процесіндегі бүйірлік қысым коэффициентінің және сырғу өлшемімен байланысты. Квазисызықты шеттік есеп фильтрация коэффициенті арқылы анықталған. Жұмыста фильтрациялық коэффициенті кеуектілік коэффициентіне тәуелді болған . Топырақтың біркелкі еместігін есепке алу кезінде есептің аналитикалық шешімдерін алу әрдайым мүмкін емес. Фурье әдісін қолдану бізді жолда қалдырады. Осы жағдайдан шығу үшін аппроксимация функциясы ұсынылады. Оның қателігі зерттелді. Параметрлердің аз мәндерінде аппроксимация дәлдігі жоғары. Есепті шешу үшін: Итерация әдісі, ең кіші квадраттар әдісі, жаңа белгісіз функцияны енгізу әдісі, біртекті емес шекаралық шарттарды біртекті етіп түрлендіру әдісі, Фурье әдісі, аппроксимация әдісі, жаңа айнымалыларды енгізу әдісі, өз функциялары бойынша жіктеу әдісі, ал құрылыстар негізінде шөгінділерді есептеу үшін В. А. Флорин әдісі қолданылды.Мақалада әр текті топырақтар консолидация теориясының жасына және уақытқа қатысты шекаралық бейсызықты есебін шешудің жуық әдістері ұсынылады.

Түйін сөздер: консолидация, топырақ, фильтрация коэффициенті, нығыздалу, аппроксимация.

S.A. Altynbekov*, A.D. Niyazymbetov
South Kazakhstan state pedagogical university, Shymkent city, Kazakhstan
*e-mail: sh.altynbekov@mail.ru

Methods of applied mathematics in solving the problem of the theory of consolidation of inhomogeneous hereditary-aging soils

The issues of improving the existing methods of forecasting the precipitation of the foundations of structures, algorithmization of the solution of their problems have not yet been removed from the agenda of scientific research. This is confirmed by the annual international conferences, symposiums and congresses in the field of industrial, oil, civil and hydraulic engineering construction. The main goal of the study was to improve the existing methods of filtration theory of consolidation in relation to inhomogeneous soils and use it to solve the problem. A mathematical formulation of the spatial quasi-linear boundary value problem of consolidation of heterogeneous hereditary-aging soil is formulated. Here, the heterogeneity of the soil is due to changes in its deformation modulus, a measure of creep and lateral pressure coefficient during consolidation according to the exponential depth law. The quasilinearity boundary value problem is defined via the filtration coefficient. It is assumed that the filtration coefficient depends on the porosity coefficient. When taking into account the heterogeneity of the soil, it is not always possible to obtain analytical solutions to the problem. The application of the Fourier method leaves us on the way. To get out of this situation, the approximation function is proposed. Its error is investigated. For small values of inhomogeneity parameters, the approximation accuracy is high. To solve the problem, we used the iteration Method, the least squares method, the method of introducing a new unknown function, the method of converting inhomogeneous boundary conditions into homogeneous ones,the Fourier method, the approximation method, the method of introducing new variables, the method of decomposition by eigenfunctions, and the method of V. A. Florin for calculating the sedimentation of structures.

Key words: consolidation, soil, filtration coefficient, compaction, approximation.

1 Введение

Введение состоит из следующих элементов: •Обоснование выбора темы и его актуальность; В обосновании выбора темы связано применение методов прикладной математики к задачам теории консолидации. Актуальность темы определяется общим интересом к изучению процесса консолидации грунтов с учетом их физико-механических свойств. •Определение оъекта исследование, целей, задач, методов. Целью исследования явилась совершенствование существующих методов теории консолидации применительно к неоднородным грунтам и применение её для решения задачи.

2 Обзор литературы

Методом решение задачи теории консолидации грунтов посвящены множество работ [1–13]. Однако, в этих работах недостаточно исследовано вопросы применение этих методов для изучения уплотнении наследственно стареющих неоднородных грунтов. А ведь, область применение методов определяется в зависимости от физико-механических свойств и параметров изучаемого процесса. В данной работе эти вопросы находит свои ответ. Они относятся в большой степени к решению краевых задач консолидации неоднородных грунтов с учетом их нелинейной наследственной ползучести, переменности коэффициентов фильтрации, бокового давления, объемной сжатия и мгновенного уплотнения.

Решения краевых задач консолидации этих перечисленных условиях весьма сложны. Поэтому точное аналитическое и полуаналитическое решение удалось получить в настоящее время для весьма ограниченного круга задач. В этой связи первостепенной задачей, стоящей перед аналитической и полуаналитической теорией консолидации, являются разработка и обоснование методов решения нелинейной теории консолидации наследственно стареющих неоднородных грунтов.

3 Материал и методы

Материалы исследование и обоснованные методы позволяет качественные и количественные изучения процесса консолидации неоднородных грунтов. В работе [16] не дано универсальный алгоритм решение проблемой. При учете неоднородность грунта не всегда удается получить аналитическое решения краевых задач консолидации неоднородных грунтов. Применение метода Фурье оставляет нас на пол пути. Чтобы выйти из этой ситуации предлагется метод аппроксимации. Этот метод способствует развитию методов и алгоритмизацию задачи теории консолидации грунтов.

4 Результаты и обсуждение

С целью теоретического исследования данного вопроса рассмотрим следующую задачу.

4.1 Постановка задачи

Рассмотрим методику решения трехмерного интегро-дифференциального уравнения процесса консолидации наследственно-стареющих неоднородных грунтов

$$\frac{\partial H}{\partial t} = C^*_{vn}(x,t,H)L^*(H) - C_{1n}(x,t,H)\times$$

$$\times\left\{\int_{\tau_1}^{t} f(\tau,H)K_1(t,\tau)dt + f(t,H)K_2(t,t)\right\} + C_{2n}(x,t,H) \tag{1}$$

при следующих краевых условиях

$$H(x,\tau_1) = \frac{\theta_0^*}{n\gamma} + H_0^*, \tag{2}$$

$$\left.\begin{array}{l} h_1^{(1)}\frac{\partial H}{\partial x_1} - h_1^{(2)}H\Big|_{x_1=-1} = \psi_1(x_2,x_3,t), \\ h_1^{(3)}\frac{\partial H}{\partial x_1} + h_1^{(4)}H\Big|_{x_1=+1} = \psi_2(x_2,x_3,t); \end{array}\right\}, \tag{3}$$

$$\left.\begin{array}{l} h_2^{(1)}\frac{\partial H}{\partial x_2} - h_2^{(2)}H\Big|_{x_2=-1} = \psi_3(x_1,x_3,t), \\ h_2^{(3)}\frac{\partial H}{\partial x_2} + h_2^{(4)}H\Big|_{x_2=+1} = \psi_4(x_1,x_3,t); \end{array}\right\} \tag{4}$$

$$\left.\begin{array}{l} h_3^{(1)}\frac{\partial H}{\partial x_3} - h_3^{(2)}H\Big|_{x_3=0} = \psi_5(x_1,x_2,t), \\ h_3^{(3)}\frac{\partial H}{\partial x_3} + h_3^{(4)}H\Big|_{x_3=1} = \psi_6(x_1,x_2,t), \end{array}\right\} \tag{5}$$

где:

$$L^* = \sum_{s=1}^{n}\frac{\partial}{\partial x_s}\left(K_{\Phi S}\frac{\partial}{\partial x_s}\right), K_1(t,\tau) = \frac{\partial}{\partial t}\left(\frac{\partial C(t,\tau)}{\partial \tau}\right), K_2(t,t) = \left(\frac{\partial C(t,\tau)}{\partial \tau}\right)\Big|_{\tau=t}.$$

Здесь уравнение состояния скелета наследственно-стареющих неоднородных грунтов представлено в следующем виде:

$$\varepsilon(t) = \varepsilon(\tau_1) - \frac{1}{1+(n-1)\xi(x)}\times$$

$$\times\left\{(\alpha_1+\alpha_2\eta_1(x))\ a_0(t)\theta(t) - \int_{\tau_1}^{t}\theta(\tau)K(t,\tau,x,\theta(\tau))d\tau\right\}, \tag{6}$$

$$K(t,\tau,x,\theta(\tau)) =$$

$$= (\alpha_1 + \alpha_2\eta_1(x))\frac{\partial a_0(\tau)}{\partial t} + (\alpha_3 + \alpha_4\eta_2(x))\frac{f(\tau,\theta(\tau))}{\theta(\tau)} \cdot \frac{\partial C(t,\tau)}{\partial \tau}, \tag{7}$$

$$a_0(t) = \frac{1}{E_0(1-\beta_E e^{-a_E t})}, E_0 > 0, \tag{8}$$

$$C(t,\tau) = t^{\alpha_5-\alpha_6}\frac{C_0(t,\tau)}{(t-\tau+\alpha_7)^{1-\alpha_6}}. \tag{9}$$

Причем функция $C_0(t,\tau)$, входящая в (9), определяется одним из нижеуказанных соотношений [1-3]:

$$C_0(t,\tau) = \varphi(\tau)\sum_{k=1}^{\infty} a_k(1-e^{-\gamma_k(t-\tau)}), \tag{10}$$

$$C_0(t,\tau) = \psi(\tau)(1-e^{-\gamma_1(t-\tau)}) + (\varphi(\tau)-\psi(\tau))\cdot(1-e^{-\gamma_2(t-\tau)}), \tag{11}$$

$$C_0(t,\tau) = A_c\varphi(\tau)(t-\tau)^{m_c}, \tag{12}$$

$$C_0(t-\tau) = A_c\varphi(\tau)(t-\tau)^{m_c}(Ba^{n_c}+1). \tag{13}$$

Старение среды описывается одним из следующих выражений:

$$\varphi(\tau) = C_0 + \frac{A_0}{\tau^k + B_0}, \psi(\tau) = C_1 + \frac{A_1}{\tau^k + B_1}, k > 0, \tag{14}$$

$$\varphi(\tau) = C_0 + \sum_{k=1}^{\infty}\frac{A_k}{\tau^k}, \varphi(\tau) = C_0 + \sum_{k=1}^{\infty} A_k e^{-\tilde{\gamma}_{k(t-\tau)}}. \tag{15}$$

Функция $f(\tau,\theta(\tau))$, входящая в (7), представлена в следующем виде:

$$f(\tau,\theta(\tau)) = \beta_1(\tau)\theta(\tau) + \beta_2(\tau)\theta^m(\tau), m > 0, \tag{16}$$

$$\beta_1(\tau) = \beta_{10} + \frac{\beta_{11}}{\tau^k + \beta_{12}}, \beta_2(\tau) = \beta_{20} + \frac{\beta_{21}}{\tau^k + \beta_{22}}, k > 0.$$

Вид функций $C^*_{vn}(x,t,H)$, $C_{1n}(x,t,H)$, $C_{2n}(x,t,H)$ в (1) обусловлен зависимостями (6)-(16), приведенными в данной работе. При этом коэффициент фильтрации, характеризующий сопротивление пористой среды движущейся жидкости согласно [4] аппроксимирован выражением:

$$K_{\Phi s}(\varepsilon(t)) = K_{\Phi s0}\left(\frac{\varepsilon(t)-\varepsilon_k}{\varepsilon_0-\varepsilon_k}\right)^{n_s}, n_s \geq 1.$$

Опишем принятые здесь обозначения: H– напор поровой жидкости; $\hat{P}_0 = \gamma\hat{H}_0$ – величина атмосферного давления; $\varepsilon(t)$ – коэффициент пористости; $\theta(t)$– сумма главных тотальных напряжений; θ^* и H^*– соответственно сумма нормальных напряжений и напор поровой жидкости, соответствующие полной стабилизации; $n = 1, 2, 3$ в зависимости от мерности рассматриваемой задачи: $x = (x_1, x_2, x_3)$– пространственные координаты; $\eta_1(E)$ и $\eta_2(E)$ – функции, характеризующие неоднородности грунтов; $\xi(E)$– функция, характеризующая изменения коэффициента бокового давления грунта в процессе его деформации; γ – удельный вес воды; $h_n^{(\alpha)}$ и $h_n^{(\alpha+1)}$ $(\alpha = 1, 2, 3;\ \ n = 1, 2, 3)$ – коэффициенты водоотдачи; $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ – параметры неоднородности; $\alpha_5, \alpha_6, \alpha_7, \alpha_k, \gamma_k, A_c$ и m_c– параметры ползучести; $a,\ B$ – амплитуда и параметр колебаний; C_0 и C_1– предельные значения меры ползучести; $k, A_0, B_0, A_1, B_1, A_k, \gamma_k$ – некоторые параметры, зависящие от свойства и условий старения среды; $E_0, \beta_E, \alpha_E,\ k, m, \beta_{10}, \beta_{11}, \beta_{12}, \beta_{20}, \beta_{21}, \beta_{22}$– опытные данные; $K_{\Phi S0}$– начальный коэффициент фильтрации; ϵ_0 и ε_k – соответственно начальный и конечный коэффициент пористости.

4.2 Метод введения новой неизвестной функции. Метод преобразования неоднородных граничных условий в однородное

Задача может быть решена различными методами численного анализа и уравнений математической физики. Здесь предпочтение отдается методу введения новой неизвестной функции, методу преобразования неоднородных граничных условий в неоднородные, методу итерации, методу наименьших квадратов, методу аппроксимации, методу введения новых переменных и теореме разложения для собственных функций.

Введем новую неизвестную функцию $W(x, t)$

$$H(x, t) = \psi(x, t) + W(x, t), \tag{17}$$

представляющее собой отклонение от известной функции $\psi(x, t)$, характеризующей напор некоторого водоносного слоя, примыкающего к рассматриваемому участку. Эта функция $W(x, t)$ будет определяться как решение уравнения

$$\frac{\partial W}{\partial t} = C_{vn}^*(x, t, W)L^*(W) - C_{1n}(x, t, W)\times$$

$$\times\left\{\int_{\tau_1}^{t} f(\tau, W)K_1(t, \tau)d\tau + f(t, W)K_2(t, t)\right\} + C_{2n}(x, t, W) + D_n(x, t) \tag{18}$$

с нулевыми граничными условиями:

$$\left.\begin{aligned} h_1^{(1)}\frac{\partial W}{\partial x_1} - h_1^{(2)}W\Big|_{x_1=-1} &= 0, \\ h_1^{(3)}\frac{\partial W}{\partial x_2} + h_1^{(4)}W\Big|_{x_1=+1} &= 0; \end{aligned}\right\}, \tag{19}$$

$$\left.\begin{aligned} h_2^{(1)}\frac{\partial W}{\partial x_2} - h_2^{(2)}W\Big|_{x_2=-1} &= 0, \\ h_2^{(3)}\frac{\partial W}{\partial x_2} + h_2^{(4)}W\Big|_{x_2=+1} &= 0; \end{aligned}\right\}, \tag{20}$$

$$\left.\begin{array}{l} h_3^{(1)}\frac{\partial W}{\partial x_3} - h_3^{(2)}W\Big|_{x_3=0} = 0, \\ h_3^{(3)}\frac{\partial W}{\partial x_3} + h_3^{(4)}W\Big|_{x_3=1} = 0. \end{array}\right\}, \tag{21}$$

При этом начальное условие (2) будет выглядеть следующим образом:

$$W(x,\tau_1) = \frac{\theta_0^*}{n\gamma} + H_0^* - \psi(x,\tau_1). \tag{22}$$

Представив функцию $\psi(x,t)$ в виде

$$\psi(x_1,x_2,x_3,t) = (\alpha_1^{(1)}x_1 + \beta_1^{(1)})\psi_1(x_2,x_3,t) + (\alpha_2^{(1)}x_1 + \beta_2^{(1)})\psi_2(x_2,x_3,t) +$$
$$+(\alpha_1^{(2)}x_2 + \beta_1^{(2)})\psi_3(x_1,x_3,t) + (\alpha_2^{(2)}x_2 + \beta_2^{(2)})\psi_4(x_1,x_3,t) +$$

$$+(\alpha_1^{(3)}x_3 + \beta_1^{(3)})\psi_5(x_1,x_2,t) + (\alpha_2^{(3)}x_3 + \beta_2^{(3)})\psi_6(x_1,x_2,t), \tag{23}$$

потребуем, чтобы она удовлетворяла условиям видов (19)-(21). Тогда коэффициенты $\alpha_1^{(1)}, \alpha_1^{(2)}, \alpha_1^{(3)}, \alpha_2^{(1)}, \alpha_2^{(2)}, \alpha_2^{(3)}, \beta_1^{(1)}, \beta_1^{(2)}, \beta_1^{(3)}, \beta_2^{(1)}, \beta_2^{(2)}, \beta_2^{(3)}$ в (23) определяются однозначно

$$\alpha_1^{(1)} = \frac{h_1^{(4)}}{h_1^*}, \beta_1^{(1)} = -\frac{h_1^{(3)} + h_1^{(4)}}{h_1^*}, \alpha_2^{(1)} = \frac{h_1^{(2)}}{h_1^*}, \beta_2^{(1)} = \frac{h_1^{(1)} - h_1^{(2)}}{h_1^*},$$
$$\alpha_1^{(2)} = \frac{h_2^{(4)}}{h_2^*}, \beta_1^{(2)} = -\frac{h_2^{(3)} + h_2^{(4)}}{h_2^*}, \alpha_2^{(2)} = \frac{h_2^{(2)}}{h_2^*}, \beta_2^{(2)} = \frac{h_2^{(1)} + h_2^{(2)}}{h_2^*},$$
$$\alpha_1^{(3)} = \frac{h_3^{(4)}}{h_3^*}, \beta_1^{(3)} = -\frac{h_3^{(3)} + h_3^{(4)}}{h_3^*}, \alpha_2^{(3)} = \frac{h_3^{(2)}}{h_3^*}, \beta_2^{(3)} = \frac{h_3^{(1)}}{h_3^*},$$

где

$$h_1^* = h_1^{(1)}h_1^{(3)} + 2h_1^{(2)}h_1^{(4)} + h_1^{(1)}h_1^{(4)},$$
$$h_2^* = h_2^{(2)}h_2^{(3)} + 2h_2^{(2)}h_2^{(4)} + h_2^{(1)}h_2^{(4)},$$
$$h_3^* = h_3^{(1)}h_3^{(3)} + h_3^{(2)}h_3^{(4)} + h_3^{(1)}h_3^{(4)}.$$

В дальнейшем в качестве функций $\psi_1(x_2,x_3,t)$, $\psi_2(x_2,x_3,t)$,$\psi_3(x_1,x_3,t)$, $\psi_4(x_1,x_2,t)$, $\psi_5(x_1,x_2,t)$, $\psi_6(x_1,x_2,t)$ берем следующие зависимости:

$$\psi_1(x_2,x_3,t) = \tilde{\varphi}_1(t)(1-x_2^2)^{n_1}f_1(x_2)x_3^{m_1}(1-x_3)^{k_1}f_1^*(x_3),$$
$$\psi_2(x_2,x_3,t) = \tilde{\varphi}_2(t)(1-x_2^2)^{n_2}f_2(x_2)x_3^{m_2}(1-x_3)^{k_2}f_2^*(x_3),$$
$$\psi_3(x_1,x_2,t) = \tilde{\varphi}_3(t)(1-x_1^2)^{n_3}f_3(x_1)x_3^{m_3}(1-x_3)^{k_3}f_3^*(x_3),$$
$$\psi_4(x_1,x_3,t) = \tilde{\varphi}_4(t)(1-x_1^2)^{n_4}f_4(x_1)x_3^{m_4}(1-x_3)^{k_4}f_4^*(x_3),$$
$$\psi_5(x_1,x_2,t) = \tilde{\varphi}_5(t)(1-x_1^2)^{n_5}f_5(x_1)(1-x_2^2)^{m_5}f_5^*(x_2),$$
$$\psi_6(x_1,x_2,t) = \tilde{\varphi}_6(t)(1-x_1^2)^{n_6}f_6(x_1)(1-x_2^2)^{m_6}f_6^*(x_2),$$

где: $n_i \geq 2$, $m_i \geq 2$, $k_j \geq 2$, $\tilde{\varphi}_i(t)$, $f_i(x)$, $f_i^*(x)$ $(i = 1,2,3,\ldots,6;\ j = 1,2,3,4)$ – заданные параметры и функции.

4.3 Метод итерации. Метод наименьших квадратов. Метод аппроксимации. Метод новых переменных

Задача (18)-(22) может быть решена методом итерации, обоснованным в работе [5]. Согласно этому методу перепишем задачу (18)-(22) в виде

$$\frac{\partial W_k}{\partial t} = C_{vn}(t)\frac{1+(n-1)\xi(x)}{\alpha_1+\alpha_2\eta_1(x)}L(W_k) + \Phi(x,t,W_{k-1}), \tag{24}$$

$$\left.\begin{array}{l} h_1^{(1)}\frac{\partial W_k}{\partial x_1} - h_1^{(2)}W_k\Big|_{x_1=-1} = 0, \\ h_1^{(3)}\frac{\partial W_k}{\partial x_1} + h_1^{(4)}W_k\Big|_{x_1=+1} = 0; \end{array}\right\}, \tag{25}$$

$$\left.\begin{array}{l} h_2^{(1)}\frac{\partial W_k}{\partial x_2} - h_2^{(2)}W_k\Big|_{x_2=-1} = 0, \\ h_2^{(3)}\frac{\partial W_k}{\partial x_2} + h_2^{(4)}W_k\Big|_{x_2=+1} = 0; \end{array}\right\}, \tag{26}$$

$$\left.\begin{array}{l} h_3^{(1)}\frac{\partial W_k}{\partial x_3} - h_3^{(2)}W_k\Big|_{x_3=0} = 0, \\ h_3^{(3)}\frac{\partial W_k}{\partial x_3} + h_3^{(4)}W_k\Big|_{x_3=1} = 0. \end{array}\right\}, \tag{27}$$

$$W_k(x,\tau_1) = \frac{\theta_0^*}{n\gamma} + H_0^* - \psi(x,\tau_1). \tag{28}$$

$$L = \sum_{s=1}^{n} K_{\Phi S0}\frac{\partial^2}{\partial x_3^2}, C_{vn}(t) = \frac{1}{n\gamma a_0(t)}.$$

Здесь коэффициент фильтрации $K_{\Phi S}(\varepsilon(t))$ согласно методу наименьших квадратов заменен линейной функцией

$$K_{\Phi S}(\varepsilon(t)) = K_{\Phi S0}\left(\frac{\varepsilon(t)-\varepsilon_k}{\varepsilon_0-\varepsilon_k}\right)^{n_s} \approx K_{\Phi S}(A+B\varepsilon(t)),$$

где A и B – известные константы, определяемые из условия

$$f_m = \int_{\varepsilon_0}^{\varepsilon_k}\left\{\left[\frac{\varepsilon_k}{\varepsilon_k-\varepsilon_0}+\frac{1}{\varepsilon_0-\varepsilon_k}\varepsilon(t)\right]^{n_s} - -(A+B\varepsilon(t))\right\}^2 d\varepsilon = \min.$$

Затем выбрав в качестве функций $\xi(x)$ и $\eta_1(x)$ соответственно следующие зависимости:

$$\xi(x) = \xi_0 e^{\alpha_8 x_n}, \eta_1(x) = e^{-\alpha_8 x_n}$$

согласно методу аппроксимации, обоснованной в работе [6], функцию $1+(n-1)\xi_0\exp(\alpha_8 x_n)$ приближенно заменяем функцией $\bar{\xi}(x_n)$, а функцию $\alpha_1+\alpha_2\eta_1(x) = \alpha_1+\alpha_2\exp(-\alpha_9 x_n)$ функцией $\tilde{\eta}_1(x_n)$, т.е.

$$1+(n-1)\xi_0 e^{\alpha_8 x_n} \approx (1+(n-1)\xi_0)\exp\left(\left(\ln\frac{1+(n-1)\xi_0 e^{\alpha_8}}{1+(n-1)\xi_0}\right)\ x_n\right), \tag{29}$$

$$\alpha_1 + \alpha_2 e^{-\alpha_9 x_n} \approx (\alpha_1 + \alpha_2) \exp\left(\left(\ln \frac{\alpha_1 + \alpha_2 e^{-\alpha_9}}{\alpha_1 + \alpha_2}\right) x_n\right). \tag{30}$$

Имея в виду (29) и (30), функцию $f_1(x_n) = \frac{1+(n-1)\xi_0 e^{\alpha_8 x_n}}{\alpha_1+\alpha_2 e^{-\alpha_9 x_n}}$ приближенно заменяем функцией $\tilde{f}_1(x_n)$:

$$\frac{1 + (n-1)\xi_0 e^{\alpha_8 x_n}}{\alpha_1 + \alpha_2 e^{-\alpha_9 x_n}} \approx \frac{(1 + (n-1)\xi_0}{\alpha_1 + \alpha_2} e^{\alpha x_n}. \tag{31}$$

Здесь $\alpha = \ln \frac{(1-(n-1)\xi_0 e^{\alpha_8})(\alpha_1+\alpha_2)}{(1-(n-1)\xi_0)\left(\alpha_1+\alpha_2 e^{-\alpha_8}\right)}$

Нетрудно заметить, что при$x_n = 0$ и $x_n = 1$ аппроксимация вида (31) абсолютно точная. Внутри точек интервала (0;1) сравним исходные значения $f_1(x_n)$ с соответствующими значениями $\tilde{f}_1(x_n)$, полученными из приближенной формулы (31). Соответствующие результаты, вычисленные на ПЭВМ при различных значениях параметров $\xi_0, \alpha_8, \alpha_1, \alpha_2$ и α_9, показывают, что функция $f_1(x_n)$ с высокой точностью $(10^{--2}...10^{--3})$ точностью аппроксимирована функцией $\tilde{f}_1(x_n)$.(См. Табл. 1 - Табл. 3)Следовательно, аппроксимация вида (31) для малых значений α_8 и α_9 вполне приемлема в практических расчетах.

Таблица 1 – $\boldsymbol{\alpha_3 = 1527 \cdot 10^{-1}}$

$\mathbf{F}_1\ (\mathbf{x}_3)$	$\mathbf{F}_2\ (\mathbf{x}_3)$	$\lvert\mathbf{F}_1 - \mathbf{F}_2\rvert$
6.7185243000E-03	6.7185243000E-03	0.0000000000E+00
6.3544726410E-03	6.4342890858E-03	7.9816444767E-05
6.0273268951E-03	6.1620787826E-03	1.3475188754E-04
5.7333457074E-03	5.9013846622E-03	1.6803895482E-04
5.4691670048E-03	5.6517195187E-03	1.8255751387E-04
5.2317695460E-03	5.4126167579E-03	1.8084721196E-04
5.0184383694E-03	5.1836295258E-03	1.6519115636E-04
4.8267337440E-03	4.9643298726E-03	1.3759612858E-04
4.6544632578E-03	4.7543079538E-03	9.9844686019E-05
4.4996567944E-03	4.5531712638E-03	5.3514469336E-05
4.3605439022E-03	4.3605489022E-03	0.0000000000E+00

4.4 Метод разложении по собственным функциям к решение задачи

Далее с учетом (31), вводим последовательно новые переменные

$y = -\frac{\alpha}{2} x_8 + \frac{1}{2}\ell n \frac{4\lambda^2}{\alpha^2 K_{\$S}}$ и $z = e^y$ тогда дифференциальное уравнение $Z^{//}(x_3) + (\lambda^2 e^{-\alpha x_3} - (\nu^2 + \rho^2))\, Z(x_3) = 0$легко сводится к уравнению Бесселя [14, 15], общее решение которого известно.

Таблица 2 – $\boldsymbol{\alpha_3 = 0,1527 \cdot 10^{-3}}$

$\mathbf{F}_1\ (\mathbf{x}_3)$	$\mathbf{F}_2\ (\mathbf{x}_3)$	$\lvert\mathbf{F}_1 - \mathbf{F}_2\rvert$
6.7185243000E-03	6.7185243000E-03	0.0000000000E+00
6.7146878012E-03	6.7146963932E-03	8.5920035531E-08
6.7108554011E-03	6.7108706674E-03	1.5766316211E-08
6.7070270952E-03	6.7070471213E-03	2.0026106995E-08
6.7032028792E-03	6.7032257537E-03	2.2874480976E-08
6.6993827488E-03	6.6994065634E-03	2.3814564543E-08
6.6955666995E-03	6.6955895490E-03	2.7849498293E-08
6.6917547270E-03	6.6917747094E-03	1.9982394406E-08
6.6879468269E-03	6.6879620433E-03	1.5216372162E-08
6.9841929949E-03	6.6841515495E-03	8.5545366346E-09
6.7181404656E-03	6.7181404656E-03	0.0000000000E+00

Таблица 3 – $\boldsymbol{\alpha_3 = 0,1527 \cdot 10^{-5}}$

$\mathbf{F}_1\ (\mathbf{x}_3)$	$\mathbf{F}_2\ (\mathbf{x}_3)$	$\lvert\mathbf{F}_1 - \mathbf{F}_2\rvert$
6.7185243000E-03	6.7185243000E-03	0.0000000000E+00
6.7184859147E-03	6.7184859156E-03	8.5265128291E-13
6.7184475298E-03	6.7184475314E-03	1.5347723092E-12
6.7184091454E-03	6.7184091474E-03	2.0108359422E-12
6.7183707613E-03	6.7183707636E-03	2.2879476091E-12
6.7183323772E-03	6.7183323800E-03	2.3945290195E-12
6.7182939944E-03	6.7182939967E-03	2.2879476091E-12
6.7182556116E-03	6.7182556136E-03	2.0108359422E-12
6.7182172292E-03	6.7182172307E-03	1.5347723092E-12
6.1781788472E-03	6.7181788480E-03	8.6686213763E-13
6.7181404656E-03	6.7181404656E-03	0.0000000000E+00

Пользуясь предложенным методом [5, 6] и аппроксимацией вида (31), будем искать решение задачи (24)-(28) в виде

$$W_k(x,t) = \sum_{i_1}^{\infty}\sum_{i_2}^{\infty}\sum_{i_3}^{\infty} T_{k_{i_1 i_2 i_3}}(t)\cdot(\cos\mu_{i_1}x_1 + A^*_{i_1}\sin\mu_{i_1}x_1)\times$$

$$\times(\cos\mu_{i_2}x_2 + C^*_{i2}\sin\mu_{i_2}x_2)\cdot V_{vi_1i_2}\left(\frac{2\lambda_{i_1i_2i_3}}{\alpha_{10}\sqrt{K_{\Phi S0}}}e^{-\frac{\alpha_{10}}{2}x_n}\right). \qquad (32)$$

Здесь $T_{k_{i_1i_2i_3}}(t)$ $(k = 1,2,3,\ldots)$ – некоторые неизвестные функции от t подлежащие определению; $V_{v_{i_1i_2}}\left(\frac{2\lambda_{i_1i_2i_3}}{\alpha_{10}\sqrt{K_{\Phi S0}}}e^{-\frac{\alpha_{10}}{2}x_n}\right)$ – функция из комбинации функции Бесселя первого и

второго рода индекса; $v_{i_1 i_2}$, $\lambda_{i_1 i_2 i_3}$– положительные корни уравнения, составленного из комбинаций функций Бесселя; μ_{i_1} и μ_{i_2}– положительные корни уравнения, составленного из комбинаций тригонометрических функций; $A^*_{i_1}, C^*_{i_1}, \alpha_{10}$ – известные коэффициенты.

Предположим, что функция $\Phi(x,t,W_{k-1})$ может быть разложена в ряд Фурье-Бесселя

$$\Phi(x,t,W_{k-1}) = \sum_{i_1}^{\infty}\sum_{i_2}^{\infty}\sum_{i_3}^{\infty} \tilde{\Phi}^{(k-1)}_{i_1 i_2 i_3}(t)\cdot(\cos\mu_{i_1}x_1 + A^*_{i_1}\sin\mu_{i_1}x_1)\times$$

$$\times(\cos\mu_{i_2}x_2 + C^*_{i_2}\sin\mu_{i_2}x_2)\cdot V_{v_{i_1 i_2}}\left(\frac{2\lambda_{i_1 i_2 i_3}}{\alpha_{10}\sqrt{K_{\Phi S0}}}e^{-\frac{\alpha_{10}}{2}x_n}\right), \tag{33}$$

где $\tilde{\Phi}^{(k-1)}_{i_1 i_2 i_3}(t)$– известная функция.

Подставляя ряд (32) в уравнение (24) и принимая во внимание (33), получим

$$T'_{k_{i_1 i_2 i_3}}(t) + \lambda^2_{i_1 i_2 i_3}!_{vn}(t)T_{k_{i_1 i_2 i_3}}(t) = \tilde{\Phi}^{(k-1)}_{i_1 i_2 i_3}(t). \tag{34}$$

Решая обыкновенное дифференциальное уравнение (34) с начальным условием (28), находим

$$T_{k_{i_1 i_2 i_3}}(t) = \left\{\int_0^t \tilde{\Phi}^{(k-1)}_{i_1 i_2 i_3}(\tau)e^{\lambda_{i_1 i_2 i_3}\int C_{vn}(\tau)d\tau}d\tau + C_{i_1 i_2 i_3}\right\}\cdot e^{\lambda^2_{i_1 i_2 i_3}\int C_{vn}(t)dt},$$

$$k = 1,2,3,\ldots \tag{35}$$

Подставив (35) в (32), получим решение задачи (24)-(28).

Полученный ряд вида (32) сходится. Значение функции $T_{k_{i_1 i_2 i_3}}(t)(k=1,2,3)$, определяемое по формуле (35), уменьшается как с увеличением i_1, i_2 и $\lambda_{i_1 i_2 i_3}$, так и с течением времени. Следовательно, последовательность $\{W_k\}$ $(k=1,2,3,\ldots)$ сходится к решению задачи (18)-(21) при$k\to\infty$.

Подставив функцию $W(x,t)$ в (17), получим решение поставленной задачи (1)-(5).

4.5 Расчет осадок грунтового основания

Расчет осадок грунтового основания согласно методу описанному в [1] и полученным результатам легко определить осадок грунтовых основания вызванной нагрузки q:

$$S(t) = \frac{s\gamma a_0}{1+\varepsilon_0}\int_0^h \frac{\alpha_1 + \alpha_2 e^{-\alpha_8 x_3}}{1+2\xi e^{-\alpha_9 x_3}}\left(\frac{\theta^*}{n\gamma} + H^*_0 - H_k(x,t)\right)dx_3 \tag{36}$$

Предварительные расчеты по формуле (36) показали:

1. Нагрузка приложенная на верхней поверхности слоя земной массы, со временем переносится на его каркас.
2. При больших значениях параметра α_8 и малых значениях параметровα_1, α_2 уплотнение грунта не зависят от времени

3. С увеличением коэффициента бокового давления осадок грунтовых оснований уменьшается.

4. Слой отложений неоднородных грунтовых оснований с увеличением параметра α_3увеличивается, а затем постоянно уменьшается.

5. Возраст скелета достаточно заметно влияет на характер уплотнения грунтовых оснований. Это влияние может быть незначительным только дляA_0, A_1, A_k, β_{10}, β_{11}, β_{20}, $\beta_{21} \to 0$

6. Деформация неоднородных грунтов обусловленных их консолидацией, от типа краевых условий. В зависимости от краевых условий может происходит набухания грунта, что вызывает после некоторых времени незначительный осадок.

5 Заключение

Разработанная модель и обоснованные методы дают возможность анализа количественного и качественного влияния коэффициентов водонасыщенности грунта и растворимости соли и жидкости, параметров упругомгновенной деформации, линейной и нелинейной ползучести, функции, характеризующей изменение возраста скелета грунта в зависимости от пространственных координат, параметров линейной и нелинейной зависимости и между начальным градиентом напора и коэффициентом пористости, а также краевых условий на процесс осадки грунтовых оснований сооружений.

Статья посвящена одному из недостаточно изученных вопросов уплотнения неоднородных наследственно стареющих грунтов. Метод аппроксимации является вкладом в прикладную механику грунтов.

Полученные результаты и расчетная формула (36) дают нам возможность количественного и качественного анализа осадки грунтовых оснований.

Список литературы

[1] Флорин В.А. Основы механики грунтов.– М.:Стройиздат,1959, 1961.–Т.1-2.

[2] Месчян С.Р. Ползучесть глинистых грунтов.– Ереван: Изд-во АН АрмССР, 1967.– 318 с.

[3] Гольдин А.Л., Месчян С.Р., Рустамян Г.Ф. //ДАН Арм.ССР. – 1985, №2.– С.78-81.

[4] Цытович Н.А., Зарецкий Ю.К., Малышев М.В., Абелев М.Ю., Тер-Мартиросян З.Г. Прогноз скорости осадок оснований сооружений. – М.: Строй издат, 1967. – 238 с.

[5] Алтынбеков Ш., Ширинкулов Т.Ш. //ДАН РУз. Математика. Технические науки. Естествознание.– 1996, №1-2.– С.25-27.

[6] Алтынбеков Ш. //Проблемы механики.– 1995, №3-4.– С.5-7.

[7] Дасибеков А., Юнусов А.А., Айменов Ж.Т., Алибекова Ж.Д. //Успехи современного Естествознания. 2014, №4. – С.87 -95.

[8] Дасибеков А., Юнусов А.А., Сайдуллаева Н.С., Юнусова А. А. //Международный журнал экспериментального образования.-М.,2012.-№8.-С. 67-72.

[9] Парамонов В.Н. //Интернет –журнал «Реконструкция городов и геотехнического строительства» 1999.-№1.-1-8.

[10] Парамонов В.Н. Метод конечных элементов при решении нелинейных задач геотехники. Санкт-Петербург; Группа компаний Георекнструкция. 2012. – 264 с.

[11] Давыдов О.П. /Российский государственный университет НЕФТИ и ГАЗА. М.:- 2012. – С.33-40.

[12] Князева С.А. //Геотехника.DOI 10.23968/1999-5571-2018-15-3-77-83.

[13] Алтынбеков Ш.,Ниязымбетов А.Д. //Наука и жизнь Казахстана.2019.-№5/2.-С. 104-109.

[14] Коренов Б.Г. Некоторые задачи упругости и теплопроводности, решаемые в Бесселевых функциях. М.: Физматгиз. 1960.-438 с.

[15] Коренев Б.Г. Введение в теорию бесселевых функции – М. Наука, 1961.- 287с.

[16] Баршевский Б.Н. Одномерная задача консолидации для грунтов с переменными по глубине модулем деформации //В сб.: Некоторые вопросы машиностроения и строительной механикй. – Ленинград, 1967 Вып.68. ч.III. –С.55-61.

References

[1] Florin V.A. "Osnovy mehaniki gruntov. [Fundamentals of soil mechanics]".- Moscow: Stroizdat,1959, 1961.- Vol. 1-2.

[2] Meschyan S.R. "Polzuchest glinistyh gruntov.[Creep of clay soils]". – Yerevan: Publishing house of the Armenian Academy of Sciences, 1967.– 318 p.

[3] Gol'din A.L., Meschyan S.R., Armen Rustamyan, G.F. //DOKLADY Arm.SSR. - 1985, No. 2.– Pp. 78-81.

[4] Tsytovich N.A., Zaretsky Yu.K., Malyshev M.V., Abelev M.Yu., Ter-Marti-Rosen Z.G. "Prognoz skorosti osadok osnovanii soorujenii[Prediction of sediment speed of construction bases.]". - M.: Stroypublications, 1967. – 238 p.

[5] Altynbekov S., Shirinkulov T.S. //DOKLADY of the Republic of Uzbekistan. Mathematics.Technical sciences. Natural science.- 1996, no. 1-2.- Pp. 25-27.

[6] Altynbekov Sh. //Problems of mechanics.- 1995, no. 3-4.- P. 5-7.

[7] Tasibekov A., Yunusov A.A., Iminov J.T., Alibekova J.D. //Progress in modern Natural science. 2014, no. 4. - C. 87 -95.

[8] Tasibekov A., Yunusov A.A., Saidullaeva N. With., Yunusov A.A. //Internationaljournal of experimental education.- Moscow, 2012.- No. 8.- Pp. 67-72.

[9] Paramonov V.N. // Online magazine "Reconstruction of cities and geotechnical construction"1999.- No. 1.- 1-8.

[10] Paramonov V.N. "Metod konechnyh elementov pri reshenii nelineinyh zadach geotehniki.[finite element Method for solving nonlinear problems geotechnics.]"// Saint Petersburg; Georeconstruction Group of companies. 2012. – 264 PP.

[11] Davydov O.P. / Russian state University of OIL and GAS. Moscow: - 2012. - P. 33-40.

[12] Knyazeva S.A. /Geotechnical Engineering.DOI 10.23968/1999-5571-2018-15-3-77-83.

[13] Altynbekov Sh., Niyazymbetov A.D. / Science and life of Kazakhstan.2019.- No. 5/2.-Pp. 104-109.

[14] Korenov B.G. "Nekotorye zadachi uprugosti i teploprovodnosti, reshaemye v Besselevyh funkciyah. [Some problems of elasticity and thermal conductivity solved in Bessel functions.] "Moscow: Fizmatgiz. 1960.-438 p.

[15] Korenev B.G. "Vvedenie v teoriyu besselevyh funkcii. [Introduction to the theory of Bessel functions.] M. Nauka, 1961.- 287c.

[16] Баршевский Б.Н. "Odnomernaya zadacha konsolidacii dlya gruntov s peremennymi po glubine modulem deformacii [One-Dimensional problem of consolidation for soils with variable depth modulus of deformation] "//in SB.: Some questions of mechanical engineering and construction mechanics. - Leningrad, 1967 Issue 68. CH. III. - P. 55-61.

3-бөлім **Раздел 3** **Section 3**

Информатика **Информатика** **Computer Science**

МРНТИ 50.05.13 DOI: https://doi.org/10.26577/JMMCS.2020.v107.i3.05

Б.С. Дарибаев[1,2*], **Д.В. Лебедев**[1], **Д.Ж. Ахмед-Заки**[2]
[1]Казахский национальный университет имени аль-Фараби, г.Алматы, Казахстан
[2]Университет международного бизнеса (UIB), г. Алматы, Казахстан
*e-mail: beimbet.daribayev@gmail.com

РЕАЛИЗАЦИЯ ПАРАЛЛЕЛЬНОГО АЛГОРИТМА ИЗВЛЕЧЕНИЯ N-GRAM ИЗ ТЕКСТА НА ФУНКЦИОНАЛЬНОМ ЯЗЫКЕ

В данной статье рассматривается реализация параллельного алгоритма извлечения N-gram из слабоструктурированного текста на функциональном языке системы LuNA реализующий технологию фрагментированного программирования. Алгоритм извлечения N-gram относится к задачам NLP. Проведен анализ других реализаций рассматриваемого параллельного алгоритма с использованием технологий MPJ Express, Apache Spark и Apache Hadoop. На основе анализа предлагается выбрать систему LuNA из-за того, что она умеет автоматически настраивать алгоритм на конкретную вычислительную систему за счёт используемой модели алгоритма в виде множества последовательных информационно зависимых задач, которые динамически распределяются по процессорам и ядрам вычислителя. В работе описывается схема реализации данного алгоритма, с применением технологии фрагментированного программирования. В статье была описана схема разделения на фрагменты данных и фрагменты вычислений. Приведена схема реализации алгоритма извлечения N-gram. Проведено тестирование на различном количестве процессоров для извлечения N-gram по словам. При извлечении токенов были удалены все стоп слова, которые задаются заранее в отдельном текстовом хранилище. Тестирование показало хорошую эффективность предлагаемого подхода по реализации алгоритмов с использованием системы LuNA.

Ключевые слова: параллельный алгоритм, функциональный язык, LuNA, N-gram, фрагментированное программирование.

Б.С. Дарибаев[1,2*], Д.В. Лебедев[1], Д.Ж. Ахмед-Заки[2]
[1]Әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы қ., Қазақстан
[2]Халықаралық бизнес университеті (UIB), Алматы қ., Қазақстан
*e-mail: beimbet.daribayev@gmail.com

Функционалды тілде мәтіннен N-gram шығаруға арналған параллель алгоритмді жүзеге асыру

Берілген мақалада фрагменттелген программалау технологиясын қолданатын LuNA жүйесінің функционалдық тілінде әлсіз құрылымды мәтіннен N-gram-ды шығарып алу параллельді алгоритмінің жүзеге асырылуы қарастырылады. N-gram-ды шығарып алу NLP есептеріне жатады. MPJ Express, Apache Spark және Apache Hadoop технологияларын қолдану арқылы қарастырылып отырған параллель алгоритмнің басқа жүзеге асыруларына талдау келтірілген. Талдаудың негізінде LuNA жүйесін таңдау ұсынылады, себебі бұл жүйеде есептеуіштің процессорлары мен ядроларында динамикалық түрде үлестірілетін, ақпараттық байланысқан есептердің тізбектелген көпмүшесі түрінде қолданылатын алгоритмнің моделінің негізінде алгоритмді нақты есептеу жүйесіне автоматты баптай алу

мүмкіншілігіне ие бола алады. Жұмыста фрагменттелген программалау технологиясын қолдану арқылы берілген алгоритмның жүзеге асырылуының схемасы сипатталады. Мақалада мәліметтер фрагменттері мен есептеу фрагменттерінің бөліну схемасы сипатталған. N-gram-ды шығарып алу алгоритмінің жүзеге асырылу схемасы келтірілген. Сөздер бойынша N-gram-ды шығарып алуға процессорлардың әртүрлі мөлшерінде тестілеулер жүргізілген. Токендерді шығарып алу кезіне алдын-ала жеке мәтіндік қоймада берілетін барлық стоп сөздер жойылған. Тестілеудің нәтижесі LuNA жүйесін қолдану арқылы жүзеге асырылған алгоритмдерге қатысты ұсынылып отырған әдіс жақсы тиімділікті көрсетті.

Түйін сөздер: параллель алгоритм, функционалды тіл, LuNA, N-gram, фрагменттелген программалау.

B.S. Daribayev[1,2*], D.V. Lebedev[1], D.Zh. Akhmed-Zaki[2]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]University of International Business (UIB), Almaty, Kazakhstan
*e-mail: beimbet.daribayev@gmail.com

Implementation of A Parallel Algorithm to Extract N-gram from Text in a Functional Language

This paper discusses the implementation of a parallel algorithm for extracting N-grams from a semi-structured text in the functional language of the fragmented programming LuNA system. The N-gram extraction algorithm relates to NLP tasks. The analysis of other considered implementations of the parallel algorithm using MPJ Express, Apache Spark and Apache Hadoop technologies were carried out. Based on the analysis, it is proposed to choose the LuNA system due to the fact that it is able to automatically configure the algorithm for a specific computer system due to the algorithm model used in the form of a set of sequential information-dependent tasks that are dynamically distributed among the processor and processor cores. The paper describes the implementation scheme of this algorithm using fragmented programming technology. In this paper the scheme of division into data fragments and fragments of calculations is described. The implementation scheme of the N-gram extraction algorithm is presented. Testing was conducted on a different number of processors to extract N-gram by words. When extracting tokens, all stop words that were set in advance in a separate text storage were deleted. Testing showed good efficiency of the proposed approach for the implementation of algorithms using the LuNA system.

Key words: parallel algorithm, functional language, LuNA, N-gram, fragmented programming.

1 Введение

В настоящее время обработка больших текстовых информации используется в различных областях. Один из основных проблем такого рода задачи является высокопроизводительная обработка текста, который выделяет актуальность темы данного исследования. Многие ведущие ученые занимаются этой проблемой по сей день. Высокопроизводительная обработка больших текстовых информации является основной проблемой в области синтеза естественных языков (NLP). Одним из важных задач обработки NLP является извлечение N-gram из текста. Целью данного исследования является разработка высокопроизводительного алгоритма извлечения N-gram из текста. Основной задачей является реализация параллельного алгоритма извлечения N-gram из слабоструктурированного текста на функциональном языке системы LuNA [1,2]. LuNA – это система которая позволяет автоматически настраивать алгоритм на конкретную вычислительную систему за счёт используемой модели алгоритма в виде множества последовательных информационно зависимых задач, которые динамически распределяются на вычислительные ресурсы.

2 Обзор литературы

Такие гиганты как Google и Yandex используют в своих сервисах алгоритмы анализа, обработки и синтеза NLP [3]. Для обработки больших данных в NLP используются различные технологии машинного обучения [4,5]. Кроме того, используются различные высокопроизводительные технологии такие как CUDA [6, 7], Apache Spark [8], Apache Hadoop [9] и т.д. Также нами была рассмотрена работа [10], в котором авторы реализовали параллельные алгоритмы извлечения N-gram на технологиях MPJ Express [11,12], Apache Spark [13,14] и Apache Hadoop [15,16]. В результате тестирования были получены следующие выводы: MPJ Express – очень гибкий, высокая производительность, трудно реализовать параллельный алгоритм и отладить программный код; Apache Spark – по производительности не сильно уступает предыдущей, сравнительно чистый и короткий код, легко настраивается; Apache Hadoop – медленно работает на маленьких наборах данных, трудно настраивается. Учитывая эти недостатки, выбрали систему LuNA для реализации параллельного алгоритма задачи извлечения N-gram из текста.

3 Материал и методы

В системе LuNA используется модель вычислений, называемая фрагментированной программой (ФП). В этой модели данные задачи представляются как множество отдельных единиц, называемых фрагментами данных (ФД). ФД иммутабельны и являются переменными единственного присваивания. Значения ФД могут иметь как базовый тип (целочисленный, вещественный, и т.п.), так и составной (фрагмент сетки, вектор, и т.п.).

ФП задается множеством фрагментов вычислений (ФВ), каждый из которых связывается с набором входных и выходных ФД и вычисляет значения выходных ФД из значений входных. ФВ является процедурой без побочных эффектов.

Вычислительный процесс состоит в том, что ФВ, для которых известны значения всех их входных ФД и неизвестны значения выходных, исполняются, что приводит к вычислению новых ФД. Как следствие, новые ФВ могут быть исполнены, и т.д. Вычислительный процесс заканчивается, когда все ФВ не исполнены.

Для реализации фрагментированного алгоритма в системе LuNA мы создаем два ФВ (Рис.1):

1. Получения списка текстовых файлов из директорий (data) файловой системы;
2. Реализация алгоритма извлечение N-gram из полученных входных ФД (список текстовых файлов).

Фрагменты вычисления каждого процесса работают по готовности входных ФД. Реализация ФВ_GET_FILES – фрагмент вычисления метода получения списка доступных текстовых файлов.

В этом ФВ_GET_FILES мы получаем список текстовых файлов из директорий data. Список файлов является выходным ФД для данного ФВ. Количество текстовых файлов в каждом ФД вычисляется по следующей формуле:

D_SIZE = END - START;

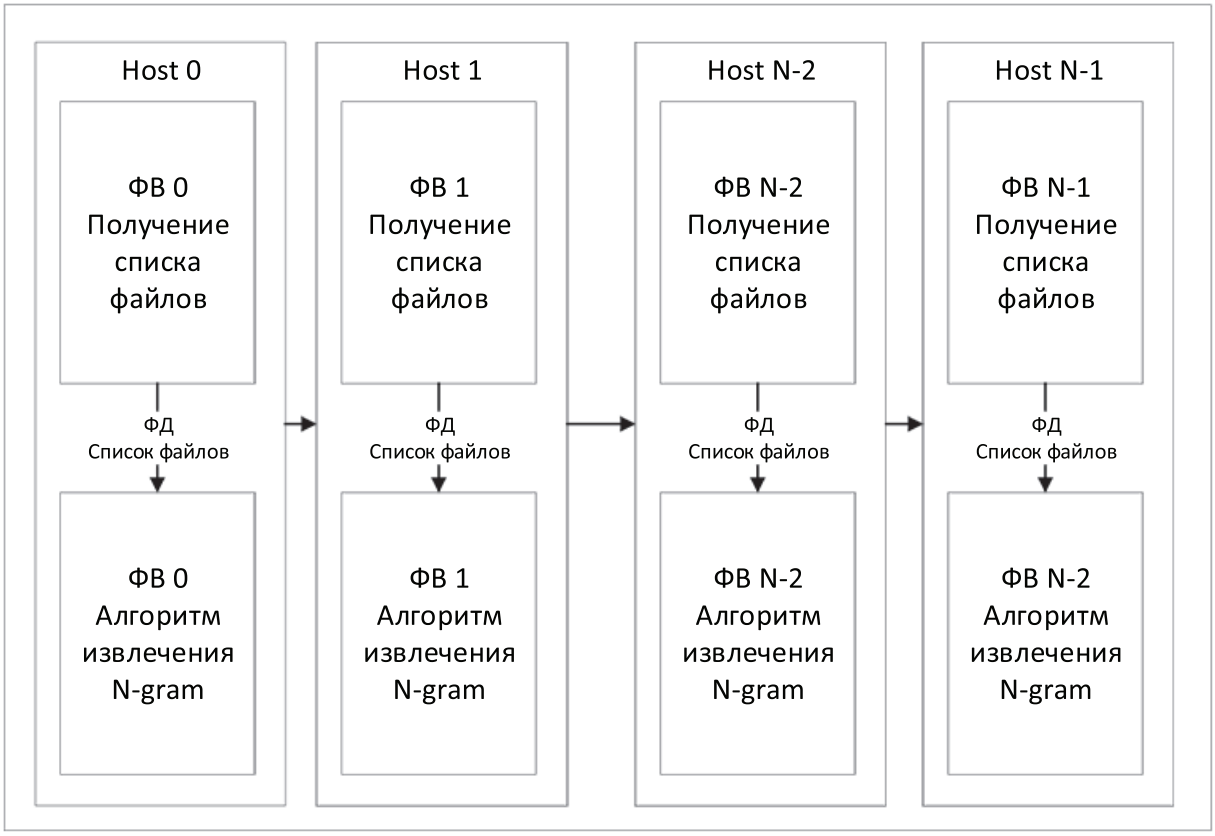


Рисунок 1 – Схема реализации алгоритма извлечения N-gram в системе LuNA

START = rank * N / FC + (rank < N % FC ? rank : N % FC);
END = rank < FC?((rank+1) * N / FC + ((rank+1) < N % FC?(rank+1):N % FC)):FC;

здесь, D_SIZE – количество текстовых файлов в каждом ФД, END – индекс начала списка текстовых файлов каждого ФД, START – индекс конца списка текстовых файлов каждого ФД, rank – ранг (индекс) ФВ, N – общее количество файлов в директорий data, FC – количество фрагментов.

После получения количества текстовых файлов, индексов начала и конца списка, готовим сам список файлов выходного ФД по следующему фрагменту кода на языке C++:

```
out.create(sizeof(string) * D_SIZE);
k = 0;
for(int i = START; i < END; i++)
{
    (out.getData<string>())[k] = inputDataFiles[i];
    k++;
}
```

здесь, out – выходной ФД, inputDataFiles – вектор из списка (имена с расширением)

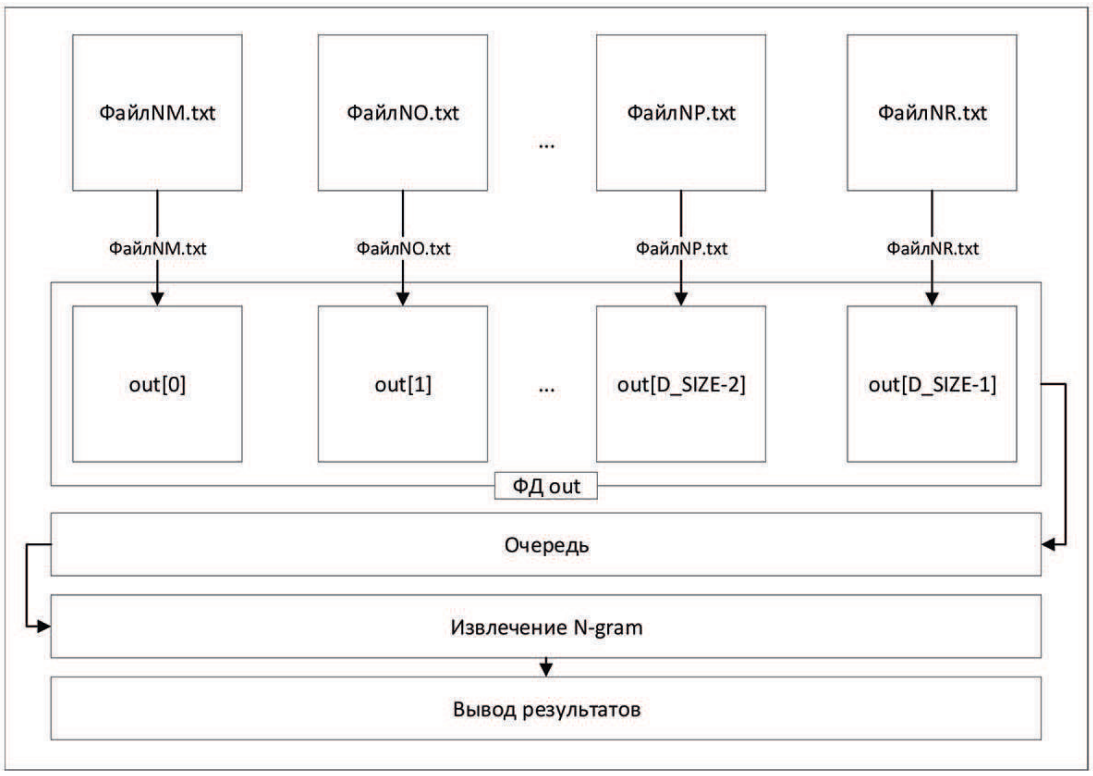


Рисунок 2 – Схема реализации алгоритма извлечение N-gram на ФВ

файлов.

Реализация ФВ_FIND_NGRAMS – алгоритм извлечение N-gram из полученных вектора списка текстовых файлов (Рис.2).

Выходные ФД в ФВ_GET_FILES будут для ФВ_FIND_NGRAMS входными ФД. ФВ_FIND_NGRAMS принимает четыре параметра:

1. ngramN – количество выводимых токенов в N-gram;
2. ngramType – тип извлечения N-gram (посимвольно, по словам и по байту);
3. inputDataFiles – список файлов для каждого входного ФД;
4. inputSize – размер списка файлов для каждого входного ФД.

От этих параметров зависит скорость вычисления программы извлечения N-gram из текста. Оптимальное значение ngramN выбирается между 2 и 5. То есть выбирать количество токенов больше пяти не имеет смысла, а единица означает что извлечения N-gram происходит посимвольно. Выбор значения ngramType зависит от требования задач. В текущем исследовании для тестирования результатов была выбрана извлечение N-gram по словам. При извлечении токенов в этом алгоритме удаляются все стоп слова [17], которые задаются заранее в отдельном текстовом хранилище. Значения inputDataFiles и inputSize зависят от количества текстовых файлов в директорий data которые вычисляются в ФВ_GET_FILES.

4 Результаты и обсуждение

Для тестирования результатов вычисления задачи извлечения N-gram из текста был использован ультрабук Lenovo Thinkpad X1 Carbon (6th Gen). В таблице 1 приведены технические характеристики ультрабука (Таблица1). Результаты тестирования напрямую зависят от характеристик процессора (частота процессора, количество физических ядер, объемы памяти кэшов L2 и L3) и объема памяти ОЗУ выбранного устройства. Тестирования проводились на 1, 2, 4 и 8 потоках процессора данного устройства.

Таблица 1 – Технические характеристики выбранного устройства для отладки и тестирования

№	Наименование	Характеристика
1	Модель	Lenovo Thinkpad X1 Carbon (6th Gen)
2	Процессор	Intel Core i7–8550U, 1800 МГц
3	Количество ядер	4 ядра
4	Объем кэша L2	1 МБ
5	Объем кэша L3	8 МБ
6	Операционная система	Ubuntu 18.04 LTS
7	Оперативная память	16 ГБ, LPDDR3, 2133 МГц
8	Встроенная память	1024 ГБ, PCIe SSD

При тестировании алгоритма количество входных текстовых файлов на разных потоках менялось пропорционально. По росту количества потоков время вычисления уменьшалась, только на 8 потоках по сравнению с 4 потоками время вычисления медленнее (Рис.3). Это можно объяснить тем, что в характеристиках процессора (Таблица1) только 4 физических ядра и 4 логических процессоров.

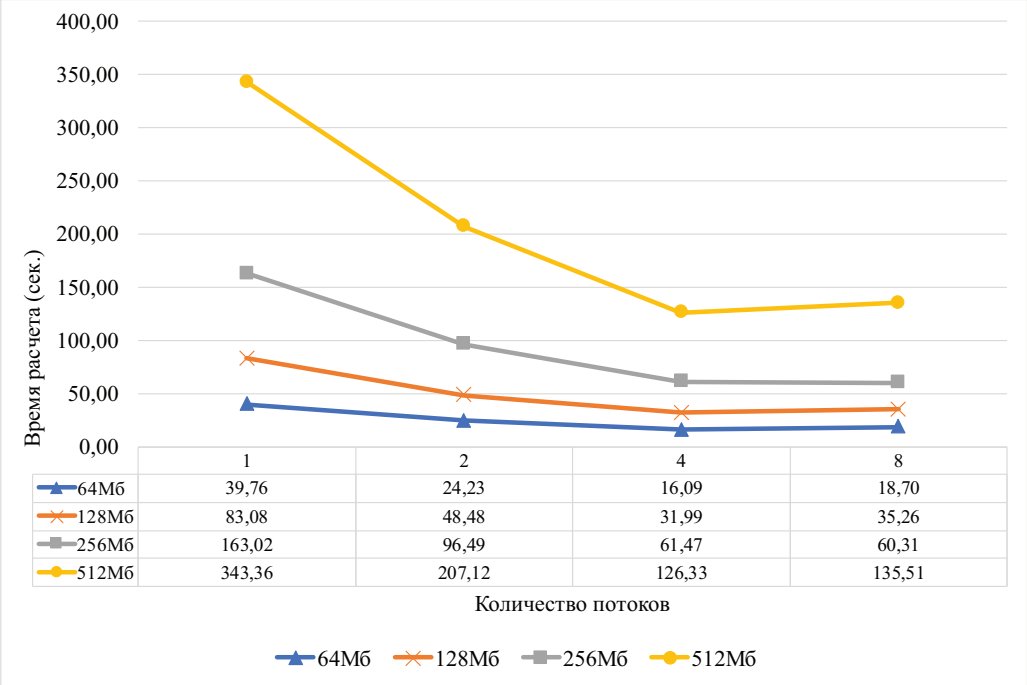
Ускорение вычислительного алгоритма на системе LuNA на 8 (восьми) потоках резко уменьшается, опять это видно, что на это влияет технические характеристики выбранного нами процессора. На Рис.4 показано ускорение вычислительных алгоритмов.

Следующий рисунок показывает эффективность вычислительного алгоритмов:

5 Заключение

В результате исследования был реализован алгоритм извлечения N-gram из текста на функциональном языке системы LuNA. В результате тестирования ускорение и эффективность вычислительных алгоритмов на 8 потоках показали худшие результаты из-за недостатков физических ядер процессора на тестируемым устройстве. В целом алгоритм хорошо работает на системе LuNA, так как отсутствуют пересылки данных между процессами.

В дальнейшем планируется исследовать характеристики алгоритма для определения оптимального варианта запуска.



	1	2	4	8
64Мб	39,76	24,23	16,09	18,70
128Мб	83,08	48,48	31,99	35,26
256Мб	163,02	96,49	61,47	60,31
512Мб	343,36	207,12	126,33	135,51

Рисунок 3 – Время вычисления

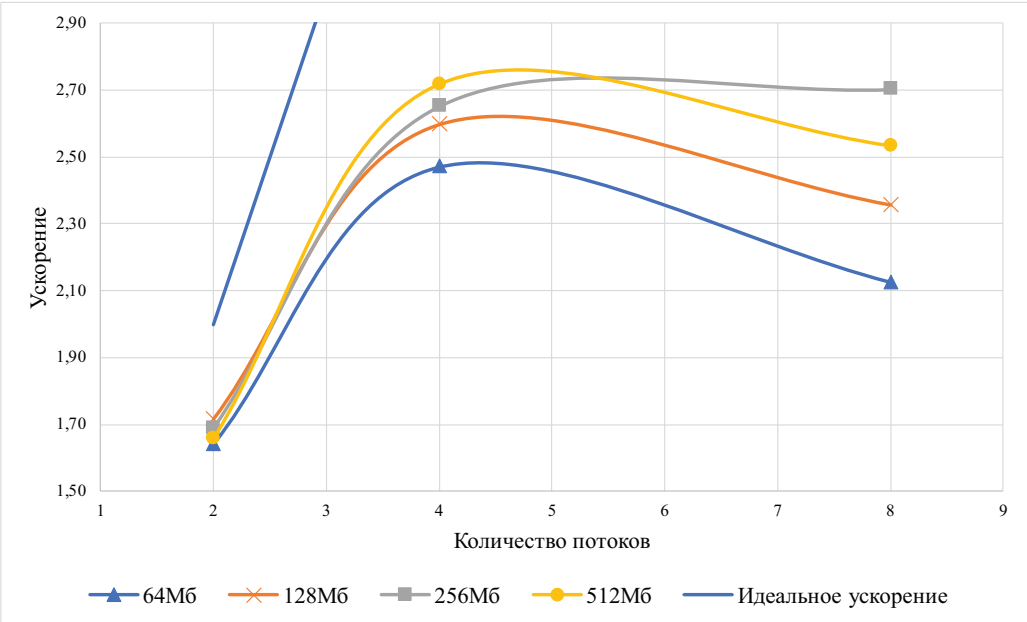


Рисунок 4 – Ускорение вычислительных алгоритмов

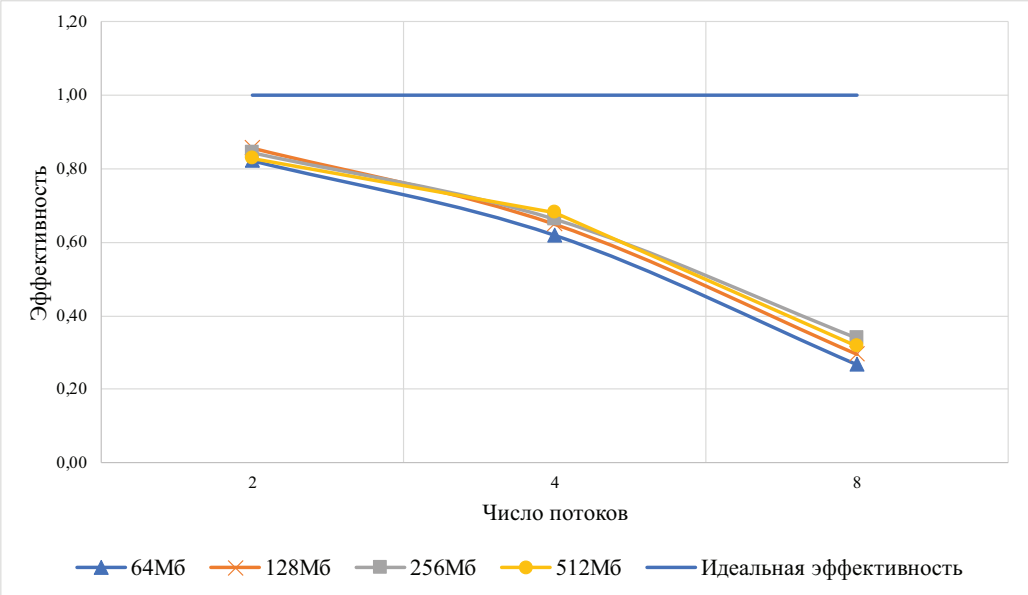


Рисунок 5 – Эффективность

6 Благодарности

Работа выполнена при поддержке грантового финансирования научно-технических программ и проектов Министерством образования и науки Республики Казахстан (грант AP05134651 «Разработка системы управления активными знаниями для автоматизации конструирования высокопроизводительных параллельных программ обработки неструктурированных данных и численного моделирования в задачах фильтрации», 2018-2020 годы).

Список литературы

[1] Малышкин В.Э. Технология фрагментированого программирования // Вестник ЮУрГУ. Сер. Выч. матем. информ. – 2012. - № 1. – С. 45–55.

[2] Malyshkin V., Perepelkin V., Schukin G. Scalable distributed data allocation in LuNA fragmented programming system // Journal of Supercomputing. – Vol.73, N 2. – P. 726-732.

[3] Google Natural Language - https://cloud.google.com/natural-language/

[4] Brants T., Popat A.C., Xu P., Och F.J., Dean J. Large Language Models in Machine Translation // Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning. – 2007. – P. 858-867.

[5] Young T., Hazarika D., Poria S., Cambria E. Recent Trends in Deep Learning Based Natural Language Processing // IEEE Computational Intelligence Magazine. – 2018. – Vol.13, N 3. – P. 55-75.

[6] Srinivasa K.G., Shree Devi B.N. GPU Based N-Gram String Matching Algorithm with Score Table Approach for String Searching in Many Documents // Journal of The Institution of Engineers (India): Series B. - 2017, - Vol.98, No. 5, - P. 467-476.

[7] Banasiak D. Statistical methods of natural language processing on GPU // Advances in Intelligent Systems and Computing. - 2016. - P. 595-604.

[8] Shaikh E., Mohiuddin I., Alufaisan Y., Nahvi I. Apache Spark: A Big Data Processing Engine // 2019 2nd IEEE Middle East and North Africa COMMunications Conference. – 2019.

[9] Bougar M., Ziyati E.H. Addressing Stemming Algorithm for Arabic Text Using Spark Over Hadoop // Advances in Intelligent Systems and Computing. – 2020. – P. 74-82.

[10] Aubakirov S., Trigo P., Ahmed-Zaki D. Comparison of distributed computing approaches to complexity of N-gram extraction // Proceedings of the 5th International Conference on Data Management Technologies and Applications - Volume 1: DATA. – 2016. – P. 25-30.

[11] Carpenter B., Getov V., Judd G., Skjellum A., Fox G. MPJ: MPI-like message passing for Java // Concurrency: Practice and Experience. – 2000. – Vol.12, N 11. – P. 1019-1038.

[12] Baker M., Carpenter B., Shafi A. MPJ Express: towards thread safe Java HPC // IEEE International Conference on Cluster Computing. – 2006.

[13] Meena B., Sarwani I.S.L., Archana M., Supriya P. Comparative Analysis of Apache Spark and Hadoop MapReduce Using Various Parameters and Execution Time // Advances in Intelligent Systems and Computing. – 2020. – P. 719-725.

[14] Sharmila K., Kamalakannan T. Analytics for healthcare using Hadoop MapReduce, Apache Spark and in cloud services // International Journal of Scientific and Technology Research. – 2020. – Vol.9, N 1. – P. 706-710.

[15] Lydia E.L., Satyanarayan S., Kumar K.V., Ramya D. Indexing documents with reliable indexing techniques using Apache Lucene in Hadoop // International Journal of Intelligent Enterprise. – 2020. – Vol.7, N 1(3). – P. 203-214.

[16] Pineiro C., Martinez-Castano R., Pichel J.C. Ignis: An efficient and scalable multi-language Big Data framework // Future Generation Computer Systems. – 2020. – P. 705-716.

[17] Baradad V.P., Mugabushaka A.-M. Corpus Specific Stop Words to Improve the Textual Analysis in Scientometrics // Proceedings of 15th International Society of Scientometrics and Informetrics Conference. – Istanbul, 2015. – P. 999-1005.

References

[1] Malyshkin V.E., "Tehnologija fragmentirovanogo programmirovanija" , *Vestnik JuUrGU. Ser. Vych. matem. inform* no. 1 (2012): 45–55.

[2] Malyshkin V., Perepelkin V., Schukin G., "Scalable distributed data allocation in LuNA fragmented programming system" , *Journal of Supercomputing* 73, no. 2 (2016): 726-732.

[3] "Google Natural Language" , https://cloud.google.com/natural-language.

[4] Brants T., Popat A.C., Xu P., Och F.J., Dean J., "Large Language Models in Machine Translation" , *Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning* (2007): 858-867.

[5] Young T., Hazarika D., Poria S., Cambria E., "Recent Trends in Deep Learning Based Natural Language Processing" , *IEEE Computational Intelligence Magazine* 13, no. 3 (2018): 55-75.

[6] Srinivasa K.G., Shree Devi B.N."GPU Based N-Gram String Matching Algorithm with Score Table Approach for String Searching in Many Documents" , *Journal of The Institution of Engineers (India): Series B* 98, No.5 (2017): 467-476.

[7] Banasiak D. "Statistical methods of natural language processing on GPU" , *Advances in Intelligent Systems and Computing* (2016): 595-604.

[8] Shaikh E., Mohiuddin I., Alufaisan Y., Nahvi I., "Apache Spark: A Big Data Processing Engine" , *2019 2nd IEEE Middle East and North Africa COMMunications Conference* (2019).

[9] Bougar M., Ziyati E.H., "Addressing Stemming Algorithm for Arabic Text Using Spark Over Hadoop" , *Advances in Intelligent Systems and Computing* (2020): 74-82.

[10] Aubakirov S., Trigo P., Ahmed-Zaki D., "Comparison of distributed computing approaches to complexity of N-gram extraction" , *Proceedings of the 5th International Conference on Data Management Technologies and Applications - Volume 1: DATA* (2016): 25-30.

[11] Carpenter B., Getov V., Judd G., Skjellum A., Fox G., "MPJ: MPI-like message passing for Java" , *Concurrency: Practice and Experience* 12, no. 11 (2000): 1019-1038.

[12] Baker M., Carpenter B., Shafi A., "MPJ Express: towards thread safe Java HPC" , *EEE International Conference on Cluster Computing* (2006).

[13] Meena B., Sarwani I.S.L., Archana M., Supriya P., "Comparative Analysis of Apache Spark and Hadoop MapReduce Using Various Parameters and Execution Time" , *Advances in Intelligent Systems and Computing* (2020): 719-725.

[14] Sharmila K., Kamalakannan T., "Analytics for healthcare using Hadoop MapReduce, Apache Spark and in cloud services" , *International Journal of Scientific and Technology Research* 9, no. 1 (2020): 706-710.

[15] Lydia E.L., Satyanarayan S., Kumar K.V., Ramya D., "Indexing documents with reliable indexing techniques using Apache Lucene in Hadoop" , *International Journal of Intelligent Enterprise* 7, no. 1 (2020): 203-214.

[16] Pineiro C., Martinez-Castano R., Pichel J.C., "Ignis: An efficient and scalable multi-language Big Data framework" , *Future Generation Computer Systems* (2020): 705-716.

[17] Baradad V.P., Mugabushaka A.-M., "Corpus Specific Stop Words to Improve the Textual Analysis in Scientometrics" , *Proceedings of 15th International Society of Scientometrics and Informetrics Conference* (2015): 999-1005.

МРНТИ 27.41.19 DOI: https://doi.org/10.26577/JMMCS.2020.v107.i3.06

Ж.М. Кожирбаев*, Ж.А. Есенбаев
Частное учреждение "National Laboratory Astana г. Нур-Султан, Казахстан
*e-mail: zhanibekkm@gmail.com

РАСПОЗНАВАНИЕ ИМЕНОВАННЫХ ОБЪЕКТОВ ДЛЯ КАЗАХСКОГО ЯЗЫКА

Распознавание именованных объектов (NER) считается одной из важных задач обработки естественного языка (NLP). Это способ распознавания объектов реального мира, таких как географическое положение, имя человека, организация и т. д., которые встречаются в предложении. Существует несколько подходов, основанных на созданных вручную правилах грамматики и статистических моделях, таких как машинное обучение и гибридные методы, для решения задачи распознавания именованных объектов. Цель данной работы состоит в том, чтобы поэкспериментировать с методами, основанными на статистическом подходе и на машинном обучение, и проверить как они справляются с агглютинативным казахским языком. В данной работе представлено распознавание именованных объектов на основе подхода машинного обучения, называемого условным случайным полем (CRF), как статистический метод. А также мы используем гибридный подход, сочетающий двунаправленную модель нейронной сети с долгой краткосрочной памятью (LSTM) и модель CRF. Это современный подход к распознаванию именованных объектов. Модель с перекрестным проверенным рандомизированным поиском показывает оценку f1 с 0,95. Гибридная модель LSTM-CRF показывает оценку f1 с 0,88. Результаты выглядит довольно хорошо, и это не требует каких-либо особенностей разработки по сравнению с моделью CRF. Для проведения экспериментов, был создан корпус (kazNER) для задачи NER с такими метками, как имя человека, местоположение, организация и другие. Корпус состоит из 29629 предложений, которые содержат хотя бы одно собственное существительное, содержащее только теги части речи.

Ключевые слова: распознавание именованных объектов, модель с условным случайным полем, нейронная сеть с долгой краткосрочной памятью, векторное представление слов

Ж.М. Кожирбаев*, Ж.А. Есенбаев
"National Laboratory Astana" жеке мекемесі, Нұр-Сұлтан қ., Қазақстан
*e-mail: zhanibekkm@gmail.com

Қазақ тіліндегі жалқы есімдерді тану

Жалқы есімдерді тану (NER) табиғи тілді өңдеудің (NLP) маңызды тапсырмаларының бірі болып саналады. Бұл сөйлемде кездесетін географиялық атауларды, адамның есімдерін, ұйымның аттарын және т.б. сияқты нақты жалқы есімдерді танудың тәсілі. Қолмен жасалған грамматикалық ережелер мен статистикалық модельдерге негізделген бірнеше тәсілдер бар, мысалы, жалқы есімдерді тану мәселесін шешуде машиналық үйрету және гибридтік әдістер. Бұл жұмыстың мақсаты - статистикалық тәсіл мен машиналық оқытуға негізделген әдістермен тәжірибе жасау және олардың агглютинативті қазақ тілімен қалай жұмыс жасайтындығын тексеру. Бұл жұмыста шартты кездейсоқ өріске (CRF) негізделген

статистикалық тәсілмен қазақ тілінің жалқы есімдерін тану ұсынылған. Біз сондай-ақ екі бағытты ұзақ қысқа мерзімді жады (LSTM) негізіндегі нейрондық желі және CRF моделімен біріктіретін гибридтік әдісті қолданамыз. Бұл жалқы нысандарды танудың қазіргі заманғы тәсілі. Кросс-расталған рандомизацияланған іздеу моделі 0,95 f1 көрсеткішінде тоқтаса, LSTM-CRF гибридті моделі 0,88 f1 көрсетеді. Нәтижелер өте жақсы көрінеді және CRF моделімен салыстырғанда ешқандай дизайн ерекшеліктерін қажет етпейді. Тәжірибелер үшін NER тапсырмасына адамның есімі, географиялық атаулар, ұйым атаулары және басқалар сияқты белгілері бар корпус (kazNER) құрылды. Корпус 29629 сөйлемнен тұрады, олардың әрқайсысында кем дегенде бір жалқы есім бар.

Түйін сөздер: жалқы есімдерді тану; шартты кездейсоқ өріс моделі; ұзақ қысқа мерзімді жады; сөздердің векторлық көрінісі

Z.M. Kozhirbayev*, Z.A. Yessenbayev
Private Institution "National Laboratory Astana Nur-Sultan, Kazakhstan
*e-mail: zhanibekkm@gmail.com

Named entity recognition for the Kazakh language

Named Entity Recognition (NER) is considered one of the important tasks of natural language processing (NLP). This is a way of recognizing real world objects, such as geographical location, person's name, organization, etc., that are found in a sentence. There are several approaches based on manually created grammar rules and statistical models, such as machine learning and hybrid methods, to solve the problem of recognizing named entities. The aim of this work is to experiment with methods based on statistical approach and machine learning, and to check how they deal with agglutinative Kazakh language. This paper presents the recognition of named objects based on a machine learning approach called conditional random field (CRF) as a statistical method. We also use a hybrid approach combining a bidirectional neural network model with long-term short-term memory (LSTM) and a CRF model. This is a modern approach to the recognition of named objects. The cross-validated randomized search model shows an f1 score of 0.95. The hybrid LSTM-CRF model shows an f1 score of 0.88. The results look pretty good and it doesn't require any design specifics compared to the CRF model. For the experiments, a corpus (kazNER) was created for the NER task with such marks as a person's name, location, organization and others. The corpus consists of 29,629 sentences that contain at least one proper noun containing only part of speech tags.

Key words: named entity recognition; conditional random field; long-term short-term memory; word embeddings

1 Введение

За последнее десятилетие огромный прогресс был достигнут в области обработки естественного языка с появлением подходов машинного обучения и доступности вычислительных ресурсов для хранения и обработки огромного количества данных. Если большинство неструктурированных текстовых данных, доступных не только из традиционных средств массовой информации, но и из социальных сетей, можно структурировать, это дал бы возможность получить богатые знания из собранных данных. Извлечение именованных объектов составляет основную задачу для предоставления важной информации из полуструктурированных и неструктурированных текстовых источников. В этой работе будет представлено одно из известных решений задачи распознавания именованных объектов для казахского языка с применением условных случайных полей (CRF). А также мы использовали гибридный подход, сочетающий двунаправленную модель LSTM и модель CRF. Гибридный подход применялся на векторном представление слов. Для проведения экспериментов был построен корпус с местонахождением,

организацией, именами и другие. Такая задача обусловлена целями проекта по разработке инструментов обработки текста на казахском языке, частью которого является настоящая работа. Нет сомнений в том, что в подходе нет новизны, но это не было целью. Цель состоит в том, чтобы поэкспериментировать с методами, основанными на статистическом подходе и на машинном обучение, и проверить как они справляются с агглютинативным казахским языком.

2 Обзор литературы

История задачи NER начинается с Sixth Conference on Message Understanding (MUC-6) в 1996 году [9], где задачи были сосредоточены на извлечении информации. В процессе постановки целей это выглядело как отдельная задача при извлечении объектов из документов. Чтобы определить объект, был введен термин «именованная сущность», и задача была названа как распознавание именованной сущности. Предыдущее исследование по извлечению информации из неструктурированных текстов проводилось с целью определения значимости «единиц информации», таких как имена людей, организаций, местоположений и числовые выражения, такие как время, дата, деньги и процентные выражения. Существует большое количество исследований, проведенных по NER для многих других языков. Для тщательного обзора работ по NER читателю рекомендуется обратиться к недавнему обзору [10]. Этот раздел ограничен кратким обзором исследований по NER для казахского языка [7, 8]. В предыдущей работе авторы утверждают, что их модель на основе CRF и особенности, полученные из результатов подхода морфологического анализа, значительно улучшают производительность системы с 69,91

3 Методология

В этом разделе представлен краткий обзор методов, которые были применены к созданному корпусу в этой задаче. CRF и LSTM были выбраны в качестве основного подхода для определения именованных объектов, представленных в предложении. Тем не менее, другие методы машинного обучения также используются для сравнения результатов и демонстрации влияния выбора признаков.

3.1 Случайный лес (Random Forest)

Поскольку задача NER рассматривается как простая задача классификации, древовидная модель Random Forest (RF) будет представлена с использованием простой карты объектов. Было доказано, что простые древовидные модели демонстрируют значительную производительность в задачах классификации. RF-классификатор, одна из самых точных древовидных моделей, может выучить основные правила, по которым помечаются термины. Выбор правильных признаков играет важную роль в производительности системы [1].

3.2 Наивный байесовский классификатор для полиномиальных моделей

Наивный байесовский (NB) подход всесторонне применяется к задачам NLP. Этот метод основан на принципе максимальной апостериорной вероятности. Для классифициро-

ванного объекта вычисляются функции правдоподобия каждого из названных классов сущностей, и из них вычисляются апостериорные вероятности названных классов сущностей. Объект принадлежит к названному классу, для которого апостериорная вероятность максимальна [5]. Есть две известные модели: многозначные модели и многовариантные модели Бернулли. Чтобы упорядочить соответствующий именованный класс сущностей $n*$ для нового термина w, он вычисляет:

$$p(c_i|w_i) = \frac{p(c_i)p(w_i|c_i)}{p(w_i)} \tag{1}$$

3.3 Условное случайное поле (CRF)

Условные случайные поля, являющиеся дискриминационной вероятностной моделью, чаще всего используются для решения проблем мечения и сегментации последовательностей [2]. Поскольку CRF является контролируемым алгоритмом машинного обучения, для его обучения требуется обучающая выборка достаточного размера. CRF может учитывать контекст; например, CRF с линейной цепью может предсказывать последовательности меток для последовательностей входных данных, в то время как дискретный классификатор предсказывает метки только для одной выборки. Приведенная ниже формула предназначена для CRF, где y - выходная переменная, а X - входная последовательность:

$$p(y|X,\lambda) = \frac{1}{Z(X)} \exp \sum_{i=1}^{n} \sum_{j} \lambda_j f_j(X, i, y_{i-1}, y_i) \tag{2}$$

Последовательность выходных выборок моделируется как нормализованное произведение функции функции.

3.4 Нейронная сеть с долгой краткосрочной памятью (LSTM)

Еще одна важная стратегия построения высокопроизводительного метода глубокого обучения - это понимание того, какой тип нейронной сети лучше всего подходит для решения проблемы NER, учитывая, что текст представляет собой последовательный формат данных. Но не любой тип LSTM справляется с этой задачей, так как использование стандартного LSTM для прогнозирования будет учитывать только «прошлую» информацию в последовательности текста. Нам нужно использовать двунаправленные LSTM для NER, поскольку контекст охватывает последовательные и будущие метки в последовательности. Двунаправленный LSTM представляет собой комбинацию двух LSTM: один движется вперед «справа налево», а другой - назад «слева направо» [11].

3.5 Гибридный подход (LSTM-CRF)

Дана входная последовательность $x = (x_1, ..., x_m)$, то есть слова предложения и последовательность состояний вывода $s = (s_1, ..., s_m)$, то есть теги именованного объекта. В

условных случайных полях мы смоделировали условную вероятность того, что выходная последовательность состояний дает входную последовательность:

$$p(s_1, ..., s_m|x_1, ..., x_m) \tag{3}$$

Мы сделали это путем определения карты объектов, которая отображает всю входную последовательность x в паре с полной последовательностью состояний s в некоторый вектор пространственных объектов d-измерения:

$$\Phi(x_1, ..., x_m, s_1, ..., s_m) \subset \mathbb{R}^d \tag{4}$$

Тогда мы можем моделировать вероятность в виде лог-линейной модели с вектором параметров $w \subset \mathbb{R}^d$ как:

$$p(s|x; w) = \frac{\exp(w \cdot \Phi(x, s))}{\sum_{s'} \exp(w \cdot \Phi(x, s')))}, \tag{5}$$

где, $s^{'}$ охватывает все возможные выходные последовательности. Мы можем рассматривать выражение $w \cdot \Phi(x, s) = score_{crf}(x, s))$ как оценку того, насколько хорошо последовательность состояний соответствует данной входной последовательности. Идея состоит в том, чтобы заменить функцию линейной оценки нелинейной нейронной сетью. Мы определяем $score$ как:

$$score_{lstm-crf}(x, s) = \sum_{i=0}^{n} W_{s_{i-1},s_i} \cdot LSTM(x)_i + b_{s_{i-1},s_i}, \tag{6}$$

где W_{s_{i-1},s_i} и b - весовой вектор и смещение, соответствующие переходу от s_{i-1} к s_i, соответственно. Функции оценки также называются textit потенциальные функции. После построения этой функции оценки мы можем оптимизировать условную вероятность $p(s|x; W, b)$, как в обычном CRF, и распространять ее обратно через сеть [12].

4 Источник данных

Набор данных собран из корпуса kazdet: NLA-NU Казахский банк деревьев зависимостей [3], который аннотирован для леммы, части речи, морфологии и отношений зависимости в соответствии с Universal Dependency 2 и хранится в формате UD-native CoNLL-U format. По состоянию на декабрь 2018 года банк содержит 61 тыс. предложений и 934,7 тыс. токенов. Это довольно большой корпус с множеством аннотаций. Однако для задачи распознавания именованных сущностей нет аннотаций. Из kazdet корпуса было извлечено 29629 предложений, которые содержат хотя бы одно собственное существительное, содержащее только теги части речи. После этого был создан корпус (kazNER) для задачи NER. Поскольку теги IOB стали стандартным способом представления структур фрагментов в файлах, корпус kazNER будет в этом формате. Формат тегов IOB содержит теги вида:

- B - TAG_TYPE – для слова в начальном отрезке;
- I - TAG_TYPE – для слов внутри отрезка;
- O – вне любого отрезка.

Теги IOB далее подразделяются на следующие классы:

- LOC = Местоположение объекта;
- ORG = Организация;
- PER = Имя человека;
- OTH = любая другая именованная сущность, например имя питомца, название книги и т. д.

На рисунке 1 показано распределение слов по тегам с тегом O (вне любого фрагмента) и без него.

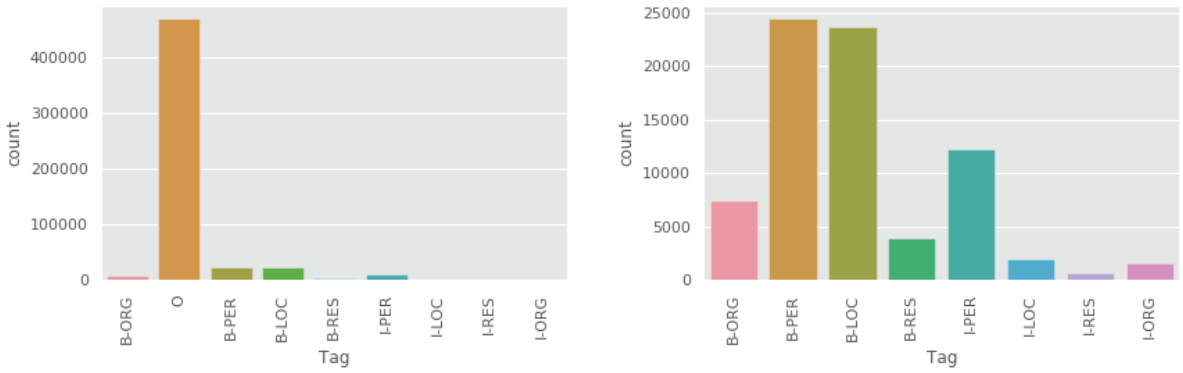


Рисунок 1 – Распределение слов по тегам с (слева) и без (справа) тега O

5 Эксперименты и обсуждения

Для того чтобы использовать методы, упомянутые в разделе “Методология”, необходимо предоставить набор признаков для правильного распознавания тегов. Поскольку классификаторы RF и NB не учитывают контекст, примерный набор признаков, такой как прописные буквы, тип слова (заголовок, строка, цифра), длина слова, символы алфавита, будет представлен для построения этих моделей. Однако метод CRF учитывает контекст. Sklearn-crfsuite [6] позволяет извлекать особенности слова в виде словаря, готового для использования с моделью:

- Текущие слова;
- Предыдущие слова;

- Следующие слова;
- Текущие POS-теги;
- Предыдущий и следующий POS-теги.

Группа Stanford NLP применила эти признаки при использовании CRF для задачи NER [4]. Признаки, такие как прописная буква, нижняя буква, цифра были извлечены для текущего, предыдущего и следующего слова. В дополнение к рекомендованным, в набор были добавлены признаки, такие как istitle, iscamelcase, isabbv, has_hyphen. Модель CRF использует алгоритм LGBFS (градиентный спуск с использованием метода L-BFGS) с упорядоченной упругой сеткой (C1 + C2). Значения упругой сетки регуляризации можно настроить, чтобы проверить их влияние на производительность. Сначала начальные значения были выбраны как C1 = 0,1 и C2 = 0,1 для модели CRF (CRF1). Затем параметры настраивались как C1 = 10 и C2 = 0.1 (CRF2). В третьем эксперименте (CRF3) использовался перекрестный рандомизированный поиск (Randomized CV Search), который представляет собой исчерпывающий поиск по сетке всех комбинаций параметров.

В гибридном подходе, сочетающий двунаправленную модель LSTM и модель CRF, мы сопоставляем предложения с последовательностью чисел, а затем дополняем последовательность. Обратите внимание, что мы увеличили индекс слов на единицу, чтобы использовать ноль в качестве значения заполнения. Это сделано потому, что мы хотим использовать параметр mask_zero слоя внедрения, чтобы игнорировать входные данные со значением ноль. Модель обучается с использованием алгоритма обратного распространения. Оптимизация параметров выполняется с помощью *rmsprop*. Гиперпараметры выбираются на основе производительности набора данных разработки.

Метрика f1-показателя будет использоваться для оценки производительности модели, поскольку точность не является хорошей метрикой для несбалансированного набора данных kazNER.

Таблица 1 – f1-показатель на тестовом наборе моделей NB, RFC и CRF

Модели	**B-PER**	**I-PER**	**B-LOC**	**I-LOC**	**B-ORG**	**I-ORG**	**B-OTH**	**I-OTH**	**Общий с “O” меткой**	**Общий без “O” метки**
NB	0.19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.81	0.06
RFC	0.40	0.00	0.41	0.54	0.45	0.00	0.18	0.02	0.89	0.32
CRF1	0.97	0.97	0.96	0.90	0.80	0.69	0.70	0.60	0.99	0.92
CRF2	0.90	0.92	0.89	0.85	0.72	0.59	0.47	0.34	0.98	0.85
CRF3	0.98	0.98	0.98	0.92	0.87	0.81	0.82	0.76	0.99	0.95

Таблица 1 показывает, что модели NB и RF работали довольно плохо. Значения f1- показателя большинства классов были равны 0. Причиной этого является отсутствие необходимых признаков для принятия соответствующих решений. Кроме того,

Таблица 2 – Показатели на тестовом наборе гибридной моделей LSTM-CRF

Метки	**Точность**	**Полнота**	**F1-показатель**
ORG	0.73	0.73	0.73
PER	0.90	0.93	0.91
LOC	0.92	0.94	0.93
RES	0.58	0.69	0.63
Среднее	**0.86**	**0.89**	**0.88**

обе модели не учитывают контекст и просто запоминают слова и теги, которых недостаточно для точного распознавания. По сравнению с дискретными классификаторами, классификатор CRF показывает отличные результаты. После оптимизации видно, что более низкие значения регуляризации упругой сети (C1 + C2) приводят к наилучшей производительности модели - особенно для C1. Модель с перекрестным проверенным рандомизированным поиском показывает приличную оценку f1 с 0,95 в целом без тега «O».

На Таблице 2 приведены резудьтаты эксперимента на гибридной модели LSTM-CRF. Резудьтаты выглядит довольно хорошо, и это не требует каких-либо особенностей разработки по сравнению с моделью CRF. Преимущество CRF здесь не очень заметна, но если бы у нас был набор данных с более сложными именованными объектами, это было бы безусловно хорошим результатом.

6 Заключение

В данной работе представлена модель NER на основе статистического подхода и машинного обучения для казахского языка. Несмотря на то, что проведенные эксперименты показывают значительную производительность, модель может развиваться по различным направлениям. В будущем эта работа будет улучшена за счет изучения новых признаков, которые влияют на распознавание объектов. Набор данных kazNER будет дополнен новыми предложениями.

Так как NER работает с большим корпусом, нейронные сети очень эффективны в поиске именованных объектов в данных, чтобы обеспечить превосходную модель NER. Использование современных методов, таких как сочетание нейронной сети LSTM и CRF, прост и часто дает хорошие результаты, есть некоторые потенциальные недостатки [13]. Если мы не видели слово во время предвычисления, мы должны закодировать его как неизвестное и вывести его значение из окружающих его слов. Часто слово postfix или prefix содержит много информации о значении слова. Использование этой информации очень важно, если вы имеете дело с текстами, которые содержат много редких слов, и вы ожидаете много неизвестных слов во время вывода. Для кодирования информации на уровне символов мы будем использовать вложения символов и LSTM для кодирования каждого слова в вектор. Мы можем использовать практически все, что создает один вектор для последовательности символов, представляющих слово.

7 Благодарности

Эта работа проводилась в рамках грантов №AP05134272 и №AP08053085, финансируемых Министерством образования и науки Республики Казахстан.

Список литературы

[1] Gislason P.O., Benediktsson J.S. and Johannes R. Random forests for land cover classification // Pattern Recognition Letters. - 2006. - Vol. 27. - P. 294–300.

[2] Lample G., Ballesteros M., Subramanian S., Kawakami K. and Dyer C. Neural architectures for named entity recognition // arXiv. - 2016. - Vol. 1603.01360. - P. 1–11.

[3] Makazhanov A., Sultangazina A., Makhambetov O. and Yessenbayev Z. Syntactic annotation of kazakh: Following the universal dependencies guidelines. a report // Proceedings of the 3rd International Conference on Turkic Languages Processing (TurkLang 2015). - Kazan, Russia, 2015. - P. 338–350.

[4] Manning C., Surdeanu M., Bauer J., Finkel J., Bethard S. and McClosky D. The Stanford CoreNLP natural language processing toolkit // Proceedings of 52nd annual meeting of the association for computational linguistics: system demonstrations. - Baltimore, Maryland, USA, 2014. - P. 55-60.

[5] Murphy K. Naive bayes classifiers // Journal of the University of British Columbia. - 2006. -Vol. 18. - P. 1–60.

[6] Korobov M. sklearn-crfsuite // URL: https://scikit-learn.org. Accessed June 5, 2020.

[7] Tolegen G., Toleu A., Mamyrbayev O. and Mussabayev R. Named Entity Recognition for Kazakh Using Conditional Random Fields // CICLing2019: Springer Lecture Notes in Computer Science. - La Rochelle, France, 2019.

[8] Tolegen G., Toleu A. and Xiaoqing Z. Neural Named Entity Recognition for Kazakh // Proceeedings of the 4-th International Conference on Computer Processing of Turkic Languages. - Bishkek, 2016. - P. 118–127.

[9] Vilain M., Burger J., Aberdeen J., Connolly D. and Hirschman L. A model-theoretic coreference scoring scheme // Proceedings of the 6th conference on Message understanding. - Columbia, Maryland, USA, 1995. -P. 45–52.

[10] Yadav V.and Bethard S. A survey on recent advances in named entity recognition from deep learning models // Proceedings of the 27th International Conference on Computational Linguistics. - Santa Fe, New Mexico, USA, 2018. -P. 2145–2158.

[11] Hochreiter S. and Jurgen S. Long short-term memory // Neural computation 9. - 1997. - P. 1735–1780.

[12] Huang Z., Wei X. and Kai Y. Bidirectional LSTM-CRF models for sequence tagging // arXiv. - 2015. - Vol. 1508.01991. - P. 1–10.

[13] Dong C., Jiajun Z., Chengqing Z., Masanori H. and Hui D. Character-based LSTM-CRF with radical-level features for Chinese named entity recognition // In Natural Language Understanding and Intelligent Applications. - 2016. -P. 239–250.

References

[1] Gislason P.O., Benediktsson J.S. and Johannes R. "Random forests for land cover classification", *Pattern Recognition Letters* vol. 27 (2006): 294–300.

[2] Lample G., Ballesteros M., Subramanian S., Kawakami K. and Dyer C. "Neural architectures for named entity recognition", *arXiv* vol. 1603.01360 (2016): 1–11.

[3] Makazhanov A., Sultangazina A., Makhambetov O. and Yessenbayev Z. "Syntactic annotation of kazakh: Following the universal dependencies guidelines. a report", *Proceedings of the 3rd International Conference on Turkic Languages Processing (TurkLang 2015)* (Kazan, Russia, 2015): 338–350.

[4] Manning C., Surdeanu M., Bauer J., Finkel J., Bethard S. and McClosky D. "The Stanford CoreNLP natural language processing toolkit", *Proceedings of 52nd annual meeting of the association for computational linguistics: system demonstrations, Baltimore, Maryland, USA* (2014): 55-60.

[5] Murphy K. "Naive bayes classifiers", *Journal of the University of British Columbia* vol. 18 (2006): 1–60.

[6] Korobov M. "sklearn-crfsuite", URL: https://scikit-learn.org. Accessed June 5, 2020.

[7] Tolegen G., Toleu A., Mamyrbayev O. and Mussabayev R. "Named Entity Recognition for Kazakh Using Conditional Random Fields", *CICLing2019: Springer Lecture Notes in Computer Science* (La Rochelle, France, 2019).

[8] Tolegen G., Toleu A. and Xiaoqing Z. "Neural Named Entity Recognition for Kazakh", *Proceeedings of the 4-th International Conference on Computer Processing of Turkic Languages* (Bishkek, 2016): 118–127.

[9] Vilain M., Burger J., Aberdeen J., Connolly D. and Hirschman L. "A model-theoretic coreference scoring scheme", *Proceedings of the 6th conference on Message understanding* (Columbia, Maryland, USA, 1995): 45–52.

[10] Yadav V. and Bethard S. "A survey on recent advances in named entity recognition from deep learning models", *Proceedings of the 27th International Conference on Computational Linguistics* (Santa Fe, New Mexico, USA, 2018): 2145–2158.

[11] Hochreiter S. and Jurgen S. "Long short-term memory", *Neural computation 9* (1997): 1735–1780.

[12] Huang Z., Wei X. and Kai Y. "Bidirectional LSTM-CRF models for sequence tagging", *arXiv* vol. 1508.01991 (2015): 1–10.

[13] Dong C., Jiajun Z., Chengqing Z., Masanori H. and Hui D. "Character-based LSTM-CRF with radical-level features for Chinese named entity recognition", *In Natural Language Understanding and Intelligent Applications* (2016): 239–250.

ҒТАМР 20.23.19 DOI: https://doi.org/10.26577/JMMCS.2020.v107.i3.07

О.А. Баймуратов, Д.А. Аязбаев*
Сулейман Демирель атындағы университет, Қаскелең қ., Қазақстан
*e-mail: Dauren.Ayazbayev@sdu.edu.kz

МАМАНДАНДЫРЫЛҒАН СӨЗДЕРДІҢ ВЕКТОРЛАРЫ АРҚЫЛЫ СӨЗДЕРДІҢ ЛЕКСИКАЛЫҚ ТІРКЕСУЛЕРІН АНЫҚТАУ

Сот жүйесінде іс қағаздардың ұйымдастырылуына хатшы жауапты болады. Хаттамаларда қате болған жағдайда, келіспеушілік пайда болуы мүмкін. Сондықтан сөздердің дұрыс лексикалық тіркесуі маңызды. Бұл жұмыста ұйқаспайтын сөздерді табу үшін сөздердің лексикалық тіркесулері есептелінді. Сөздердің лексикалық тіркесулері Skip-gram моделімен анықталды. Skip-gram моделі сөздерді векторлармен сипаттайды. Бұл модельде мағынасы жағынан жақын сөздердің және бір-бірімен лексикалық тіркесетін сөздердің векторлары шамамен бір бағытта болулары керек. Сондықтан екі сөздің бір-бірімен лексикалық тіркесуін анықтау үшін сол сөздердің векторларының арасындағы бұрыштың косинусы есептелінді. Косинустың мәні 1-ге жақындаған сайын екі сөздің лексикалық тіркесулері жоғарлайды. Керісінше, косинустың мәні -1-ге жақындаған сайын екі сөздің лексикалық тіркесулері төмендейді. Бұл жұмыста Қазақстан Республикасының конституциясының бабының мәтініне жаңа сөз енгізген кезде, авторлардың жүйесі енгізілген сөзді табу керек еді. Жүйе кейбір сөздер үшін жоғары дәлдікті көрсеткенімен, кейбір сөздерде қателіктер табылды. өйткені енгізілген жаңа сөз конституцияның бабына қатысты болмағанымен, көрші сөзбен басқа мәтіндерде тіркесе алады. Мысалы, компьютер сөзі мағынасы жағынан конституцияның бабына қатысты болмағанымен, бұл сөз бұрынғы сөзімен лексикалық тіркесе алады. Берілген жұмыс "Отандық білім беруді модернизациялау жағдайында көптілді IT маманының құзыретті инновациялық моделін әзірлеу және енгізу"атты гранттық жоба аясында жүзеге асырылынып жатыр.

Түйін сөздер: сөздің векторы, Skip-gram моделі, сөздердің лексикалық тіркесулері.

О.А. Баймуратов, Д.А. Аязбаев*
Университет имени Сулеймана Демиреля, г. Каскелен, Казахстан
*e-mail: Dauren.Ayazbayev@sdu.edu.kz

Определение лексической сочетаемости слов по векторам специализированных слов

В системе суда секретарь является ответственным за заполнение протоколов. Маленькая ошибка может привести к недопониманию между людьми. Поэтому секретарь должен стараться не допускать каких-либо ошибок. В данной работе был выполнен анализ слов по их лексической сочетаемости. Лексическая сочетаемость слов была определена по модели Skip-gram. Модель Skip-gram представляет слова в виде векторов. В модели Skip-gram векторы слов, имеющие схожий смысл и лексические сочетаемые слова должны иметь приблизительно одинаковое направление. Поэтому чтобы вычислить лексическое сочетаемость двух слов был определен косинус угла между соответствующими векторами. Если два слова лексический сочетаемы друг с другом, то значение косинуса должен быть приблизительно равным 1. В противном случае, значение косинуса должен быть примерно равным -1. В данной работе в качестве тестирования был взят текст статьи конституции Республики

Казахстан. Когда авторы вводили слова не связанные с контекстом, их система должна была определить введенные слова. Система для некоторых слов показала высокую, а для некоторых слов низкую точность. По мнению авторов, это связано тем, что, несмотря на то, что введенные слова не были связаны с контекстом, они были лексический сочетаемы с соседними словами. Например, слово компьютер по смыслу не был связан с текстом конституции, но это слово может употребляться со словом бңрынғы казахского языка. Данная работа выполняется в рамках грантового проекта Министерства Образования и Науки Республики Казахстан "Разработка и внедрение инновационной компетентностной модели полиязычного IT-специалиста в условиях модернизации отечественного образования".

Ключевые слова: векторы слов, модель Skip-gram, лексическое сочетаемость слов.

O.A. Baimuratov, D.A. Ayazbayev
Suleyman Demirel University, Kaskelen, Kazakhstan
*e-mail: Dauren.Ayazbayev@sdu.edu.kz

Identifying lexical compatibilities of words by vectors of specialized words

In court system secretary fills protocols. Filling protocols with mistakes can lead to misunderstanding between people. Hence it is important writing protocols properly. In current work to identify mistakes lexical compatibilities of words were computed. To do it Skip-gram model was applied. In Skip-gram model words are represented by vectors. Words with similar meaning and lexically compatible words should have approximately the same direction. Therefore to calculate lexical compatibility of two words cosine value of angle between corresponding two vectors was identified. Cosine value of highly lexically compatible words should be approximately equal to 1. Lexically incompatible words should approximately have value -1. To test their system authors used the text of article of the constitution of the Republic of Kazakhstan. Particularly, words which are not related to meaning of article of the constitution were inserted, and the system had to identify that inserted words. The system for some words showed high accuracy, however some words showed low accuracy. By authors' opinion, it happened because even inserted words were not related in meaning, they could be lexically compatible with their neighbors. For example, word computer can be used in other contexts with word б?рын?ы(old) of Kazakh language. This research is carried out within the framework of the Ministry of Education and Science of Republic of Kazakhstan grant project "Developing and implementing the innovative competency-based model of multilingual IT specialist in the course of national education system modernization".

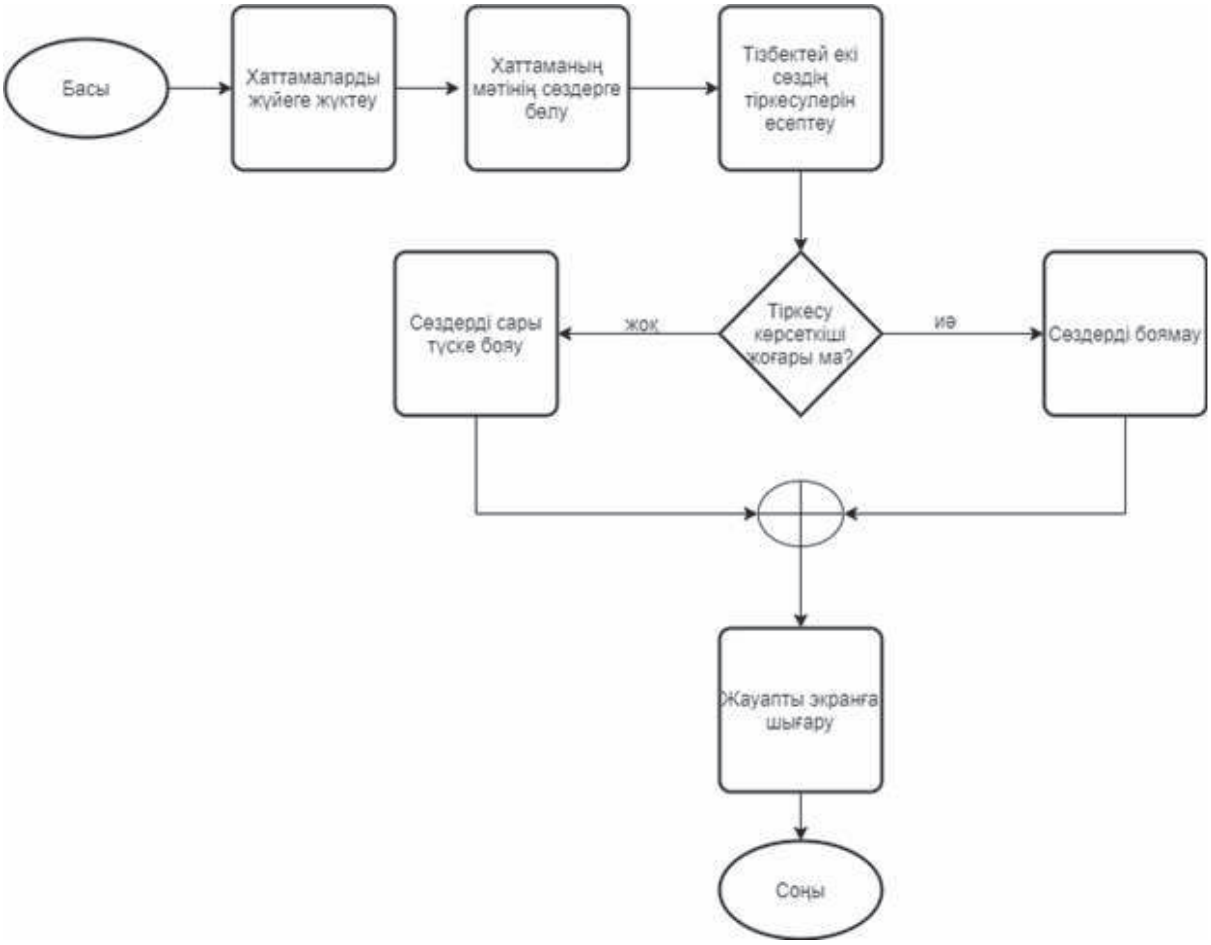
Key words: vectors of words, Skip-gram model, lexically compatibilities of words.

1 Кіріспе

Қандай жұмыс болмасын, ол мұқияттылықты қажет етеді. Мысалы, дәрігер науқас адамға дәріні тағайындағанда, құрылысшылар үйді салғанда, сот шешімін шығарғанда және т.б. Сот жүйесінде іс қағаздардың ұйымдастырылуларын хатшыға тапсырылынады. Хатшы қандай да бір құжатты қате толтырған жағдайда, оның салдары келіспеушілікті тудырту мүмкін. Бұл жұмыста біз сот жүйесіндегі хатшының хаттамаларды толтыруға көмектесетін қосымшаны даярлағымыз келеді. Біздің қосымшамыз сөздердің лексикалық тіркесуін анықтау керек. Ол үшін біз word embedding әдісін пайдаландық. Word embedding сөздерді векторларға айналдыратын әдіс. Word embedding-те векторлар координаталармен сипатталады. Мағынасы жағынан жақын сөздер шамамен бір бағытта болу керек. Сонымен қатар, word embedding-те сөздің векторының координатасы анықталғанда, сол сөздің басқа сөздермен лексикалық тіркесуі ескеріледі.

2 Әдебиетке шолу

Жобамыздың блок-сызбанұсқасы 1-суретте көрсетілді.



1-**сурет** - Жобаның сызба-нұсқасы

1-суретте көрсетілгендей, жүйенің жұмысы хатшының хаттамаларды жүктеуімен басталады. Екі сөздің лексикалық тіркесуін есептеу үшін, сол сөздердің векторларын білу қажет. Сондықтан жүйеде сөздердің векторларынан тұратын сөздік бар.

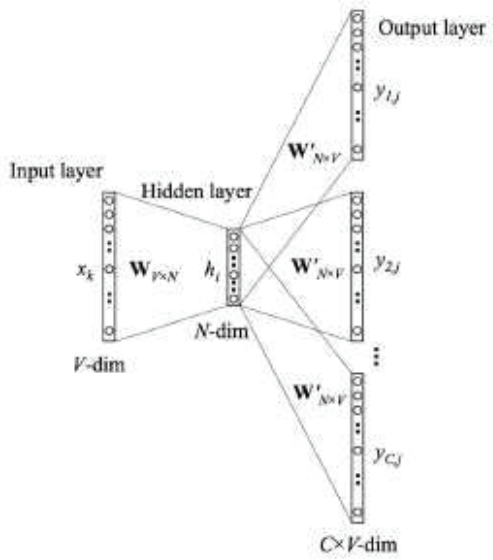
Word embedding-ті әртүрлі салада пайдалануға болады. Мысалы: [1] авторлары word embedding-ті адамдардың пікірлерін білу үшін пайдаланса, [2] авторлары кітаптың ішіндегі кейіпкерлердің өзара байланысын, яғни әлеуметтік желісін (social network) анықтау үшін қолданды.

3 Материалдар мен әдістер

Сөзді векторға айналдыратын бірнеше модельдер бар. Мысалы: Skip-gram, continuous bag of words, GloVe. Бұл жобада сөздің векторын анықтау үшін Skip-gram моделі пайдаланылды. Skip-gram моделі берілген сөздің көрші сөздерінің мәнмәтін ішінде кездесу ықтималдығын анықтайды. Skip-gram моделі сөзді векторға айналдыру үшін нейрондық

желіні пайдаланады [3]. Бұл желіде бір сөздің векторын анықтау үшін келесі қадамдардан өту керек [4–6]

1) Корпустың ішінен анықтайын деп жатқан вектордың сөзі кездесетін сөйлемдерді бөліп шығару. Содан кейін сол сөйлемдерден қайталанатын сөздерді алып тастау керек. Одан қалған сөздер нейрондық желінің енгізу қабаты (input layer) болады. Нейрондық желінің құрылымы 2-суретте көрсетілген.



2-**сурет** - Skip-gram-ның нейрондық желісінің құрылымы

Бұл жерде x – енгізу қабатының нейрондары, W – нейрондардың арасындағы салмақтар, h – жасырын қабатының нейрондары, y – шығу қабатының нейрондары, V – әртүрлі сөздердің саны, C – анықтайын деп жатқан вектордың сөзінің көршілерінің саны(терезенің өлшемі). Енгізу қабатында әр сөзге бір нейрон сәйкес.

2) Іздеуге таңдалған сөздің нейронынан басқа нейрондардың бәрі 0 мәнін қабылдайды. Ал іздеуге таңдалған сөзінің нейроны 1-ге тең болады.

3) Нейрондық желіде барлық салмақтар 0 мен 1 арасында тағайындалады. Енгізу мен жасырын, жасырын мен шығу қабаттарындағы салмақтар әртүрлі бола алады.

4) Енгізу қабатындағы барлық нейрондардың мәндерін енгізу мен жасырын қабаттағы салмақтарға көбейту:

$$h = x^T W. \tag{1}$$

5) Шығу қабатының нейрондарының мәндері келесі формуламен анықталады:

$$u = hW^T, \tag{2}$$

W – жасырын қабатымен шығу қабатының арасындағы салмақтар.

6) Шығу қабатының нейрондарының мәндері softmax функциясымен ықтималдылықтарға айналдырылады. Ол үшін келесі формула қолданылады:

$$p\left(w_{c,j} = w_{o,c} | w_i\right) = y_{c,j} = \frac{\exp(u_{c,j})}{\sum\limits_{j'=1}^{V} \exp(u_{j'})}. \tag{3}$$

Бұл жерде:
$w_{c,j}$ – шығу қабатындағы c-мәнмәтіндегі j-сөз,
$w_{o,c}$ – шығу қабатындағы c-сөз,
w_i – енгізу қабатындағы анықтайын деп жатқан вектордың сөзі.

Нейрондық желіде анықтайын деп жатқан вектордың сөзінің көршілер саны мәнмәтін санын анықтайды. Әр мәнмәтін бір көршіге сәйкес. $y_{c,j}$ – c-мәнмәтіннің j-сөзінің көрші сөз болуының ықтималдығы.

7) Шығу қабатындағы әр нейронға болжау қателігі есептелінеді:

$$e_{c,j} = y_{c,j} - t_{c,j}. \tag{4}$$

Егер c-мәнмәтіндегі j-сөз c-мәнмәтіннің көрші сөз болса, $t_{c,j}$ 1-ге тең болады. Қалған жағдайларда 0-ге тең болады.

8) Шығу қабатының сөздерінің барлық қателіктері қосылады:

$$\mathrm{EI}_j = \sum_{C=1}^{C} e_{c,j}, \tag{5}$$

C-мәнмәтіннің саны.

9) Нейрондық желіде барлық салмақтар келесі формуламен жаңартылады:

$$w_{i,j}{}^{(new)} = w_{i,j}{}^{(old)} - \alpha\ \mathrm{EI_j}\ h_i. \tag{6}$$

Бұл формулада:
α – үйрену жылдамдығының коэффициенті (learning rate),
$w_{i,j}{}^{(new)}$ – жаңа салмақ,
$w_{i,j}{}^{(old)}$ – ескі салмақ,
h_i – жасырын қабатының нейронының мәні.

10) Нейрондық желінің қателігі төмен болғанша 4-9 қадамдарды қайталау.

Бұл жобада екі сөздің лексикалық тіркесуін анықтау үшін, екі сөздің векторларының арасындағы бұрыштың косинусы есептелінді. Екі сөздің мағыналары бір-біріне жақын болған сайын [7, 8] немесе лексикалық тіркесулері үлкейген сайын, косинустың мәні де үлкейеді. Екі векторлардың арасындағы бұрыштың косинусы келесі формуламен есептелінеді:

$$\cos(a) = \frac{a_1 b_1 + a_2 b_2 + ... + a_n b_n}{\sqrt{a_1^2 + a_2^2 ... + a_n^2}\ \sqrt{b_1^2 + b_2^2 ... + b_n^2}}. \tag{7}$$

Бұл формулада n – вектордың өлшемі. Бұл жұмыста n 100-ге тең болды.

4 Нәтижелер мен олардың талқылануы

Сөздердің лексикалық тіркесулерін тексеру үшін, біз Қазақстан Республикасының Конституциясын таңдадық. 90-баптың 1-тармақшасының сөздерінің арасына жаңа сөзді жазғанда, біздің жүйе сол жаңа сөзді табу керек болды. Жаңа сөзді табу үшін сөздердің

векторларының арасындағы косинустары есептелінді. Енгізілген жаңа сөздің оң жағында және сол жағында сөздер болды. Егер енгізілген жаңа сөзбен оның сол жағындағы немесе оң жағындағы сөздердің косинустары қалған басқа сөздердің косинустарынан ең кіші болса, онда жүйе енгізілген жаңа сөзді тапты деп есептелінді. 1-кестеде жүйенің дәлдігін көруге болады.

1-**кесте** – Жүйенің дәлдігі

Сөз	**Дәлдік**
Жасыл	57.14%
Сиыр	100%
Қасқыр	100%
Қалам	71.43%
Компьютер	57.14%
Ғарышкер	28.57%
Көлік	14.29%
Ұшақ	71.43%
Темір	71.43%
Алюминий	85.71%

Жүйенің дәлдігін есептеу үшін жаңа сөз 90-баптың 1-тармақшасының әртүрлі сөздердің араларына қойылды. 1-кестеде көрсетілгендей біздің жүйе әртүрлі дәлдікті қайтарды. Тек сиыр, қасқыр сөздері 100% дәлдікті көрсетті. Өйткені бұл сөздер 90-баптың 1-тармақшасының сөздерімен лексикалық тіркес емес(мысалы: Республикалық сиыр, ресми сиыр). Дегенмен кейбір сөздер үшін жүйенің дәлдігі төмен болды. Өйткені сол сөздер мағынасы жағынан 90-баптың 1-тармақшасына сәйкес келмесе де, оң жағындағы немесе сол жағындағы сөзбен лексикалық тіркесе алады. Мысалы: ұшақ деген сөз бұрынғы деген сөзімен, ғарышкер сөзі ресми сөзімен лексикалық тіркесе алады.

5 Қорытынды

Жоғарыда көрсетілгендей word embedding-тың өзінің кемшіліктері бар. Мысалы, сөздердің лексикалық тіркесулерін анықтау үшін, конституцияның барлық сөздері сөздікте болу керек.Сонымен қатар, екі вектордың арасындағы бұрыштың косинусы арқылы тек осы екі векторлардың өзара лексикалық тіркесулерін бағалай аламыз. Дегенмен, осы векторлардың сөздерінің лексикалық тіркесулеріне оларға дейін және кейін тұрған сөздер де әсер ете алады. Сондықтан жүйеміздің дәлдігін көбейту үшін, біздің phrase embedding-ты пайдаланғанымыз жөн. Қазіргі таңда әртүрлі тілдер үшін векторлардың бірнеше нұсқалары бар. Олар [9, 10] қол жетімді.

Әдебиеттер тізімі

[1] И.В. Бондарева, Д.Г. Лагерев. 2018, Исследование методов векторного представления текстовой информации для решения задачи анализа тональности, Всероссийская научная конференция "Информационные технологии интеллектуальной поддержки принятия решений Уфа-Ставрополь, Россия, 2018, 10-15 стр.

[2] Gerhard Wohlgenannt, Ekaterina Chernyak, Dmitry Ilvovsky, 2016, Extracting Social Networks from Literary Text with Word Embedding, Proceedings of the Workshop on Language Technology Resources and Tools for Digital Humanities (LT4DH), December 11-17 2016. pages 18–25.

[3] http://mccormickml.com/2016/04/19/word2vec-tutorial-the-skip-gram-model/. Қарау датасы: 10.06.2020.

[4] David Meyer, 2016, How exactly does word2vec work? July 31, 2016. Pages 1-18.

[5] https://hmkcode.com/ai/backpropagation-step-by-step/. Қарау датасы: 10.06.2020.

[6] https://www.kdnuggets.com/2018/04/implementing-deep-learning-methods-feature-engineering-text-data-skip-gram.html. Қарау датасы: 10.06.2020.

[7] Nawal Ould-Amer, Philippe Mulhem, Mathias Géry, Karam Abdulahhad, 2016, Word Embedding for Social Book Suggestion, Clef 2016 Conference, 09.05.2016, Volume 1609

[8] Ensaf Hussein Mohamed, Eyad Mohamed Shokry, 2020, QSST: A Quranic Semantic Search Tool based on word embedding, Journal of King Saud University –Computer and Information Sciences, 4 January 2020

[9] https://code.google.com/archive/p/word2vec/. Қарау датасы: 10.06.2020.

[10] https://sites.google.com/site/rmyeid/projects/polyglot. Қарау датасы: 10.06.2020.

References

[1] I.V. Bondareva, D.G. Lagerev. 2018, Issledovanie metodov vektornogo predstavlenija tekstovoj informacii dlja reshenija zadachi analiza tonal'nosti, Vserossijskaja nauchnaja konferencija "Informacionnye tehnologii intellektual'noj podderzhki prinjatija reshenij Ufa-Stavropol, Russia, 2018, 10-15 p.

[2] Gerhard Wohlgenannt, Ekaterina Chernyak, Dmitry Ilvovsky, 2016, Extracting Social Networks from Literary Text with Word Embedding, Proceedings of the Workshop on Language Technology Resources and Tools for Digital Humanities (LT4DH), December 11-17 2016. pages 18–25.

[3] http://mccormickml.com/2016/04/19/word2vec-tutorial-the-skip-gram-model/. Accessed date: 10.06.2020.

[4] David Meyer, 2016, How exactly does word2vec work? July 31, 2016. Pages 1-18.

[5] https://hmkcode.com/ai/backpropagation-step-by-step/. Accessed date: 10.06.2020.

[6] https://www.kdnuggets.com/2018/04/implementing-deep-learning-methods-feature-engineering-text-data-skip-gram.html. Accessed date: 10.06.2020.

[7] Nawal Ould-Amer, Philippe Mulhem, Mathias Géry, Karam Abdulahhad, 2016, Word Embedding for Social Book Suggestion, Clef 2016 Conference, 09.05.2016, Volume 1609

[8] Ensaf Hussein Mohamed, Eyad Mohamed Shokry, 2020, QSST: A Quranic Semantic Search Tool based on word embedding, Journal of King Saud University –Computer and Information Sciences, 4 January 2020

[9] https://code.google.com/archive/p/word2vec/. Accessed date: 10.06.2020.

[10] https://sites.google.com/site/rmyeid/projects/polyglot. Accessed date: 10.06.2020.

4-бөлім **Раздел 4** **Section 4**

Қолданылмалы математика **Прикладная математика** **Applied Mathematics**

МРНТИ 27.17.27; 27.41.41 DOI: https://doi.org/10.26577/JMMCS.2020.v107.i3.08

У.К. Турусбекова[1*], **А.С. Тургинбаева**[2]
[1]Казахский университет экономики, финансов и международной торговли, г. Нур-Султан, Казахстан
[2]Евразийский национальный университет имени Л.Н. Гумилева, г. Нур-Султан, Казахстан
*e-mail: umut.t@mail.ru

ХЕШИРОВАНИЕ НА ОСНОВЕ МНОГОЧЛЕНОВ

В современной криптографии широко используются различные хеш-функции. Хеш-функции - это простые для вычисления функции сжатия, которые принимают входные данные переменной длины и преобразуют их в выходные данные фиксированной длины. Они используются в качестве компактных представлений или цифровых отпечатков пальцев для обеспечения целостности сообщения. Основная проблема использования хеш-функций заключается в том, что существование необратимых функций, исключающих возможность столкновений, не доказано. Кроме того, не существует универсальных методов хеширования, и их следует выбирать в зависимости от области их применения. Особую роль играют теоретико-сложностные проблемы, а именно алгебраическая теория чисел. Одной из таких проблем является поиск неприводимых многочленов заданной степени над конечным полем, которые можно использовать для поиска хеш-кодов сообщений. Актуальность исследования неприводимых полиномов над простыми и расширенными полями Галуа обусловлена их разнообразным применением в различных областях науки и техники. Неприводимые многочлены нашли свое применение в различных областях математики, информационной техники и защите информации. Использование свойств неприводимых многочленов позволяет максимизировать эффективную компьютерную реализацию арифметики в конечных полях, что имеет особое значение для криптографии и теории кодирования. Поиск неприводимых многочленов является сложной для вычисления задачей, особенно над полями большой размерности. Процедура нахождения неприводимых многочленов требует эффективных алгоритмов и больших вычислительных ресурсов, как в случае нахождения простых чисел, что является основной проблемой для построения эффективных алгоритмов хеширования на их основе. В представленной статье описан метод построения хеш-функций, основанный на вычислении остатка от деления на неприводимый многочлен. Кроме того, рассмотрена проблема поиска неприводимых многочленов. Выполнено компьютерное моделирование хеш-функций с использованием неприводимых многочленов над конечными полями. Представлены результаты использования различных неприводимых многочленов и их анализ. Результаты статьи могут быть использованы в криптографических приложениях и теории кодирования.

Ключевые слова: неприводимый многочлен, Хеш-функция, конечное поле, избыточный циклический код, столкновение.

Ұ.Қ. Тұрысбекова[1*], А.С. Тургинбаева[2]
[1]Қазақ экономика, қаржы және халықаралық сауда университеті,
Нұр-Сұлтан қ., Қазақстан
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан қ., Қазақстан
*e-mail: umut.t@mail.ru

Көпмүшеліктер негізінде хештеу

Қазіргі заманғы криптографияда әр түрлі хеш-функциялары кеңінен қолданылады. Хэш - функциялар - бұл өзгермелі ұзындықтағы кіріс қорын қабылдап, оларды тұрақты ұзындықтағы шығыс қорына түрлендіретін, есептеуге оңай сығымдау функциялары. Олар хабарламаның тұтастығын қамтамасыз ету үшін ықшам көріністер немесе сандық саусақ іздері ретінде қолданылады. Хеш-функцияларын қолданудағы негізгі мәселе соқтығысулар мүмкіндігін жоққа шығаратын қайтымсыз функциялардың болуының дәлелденбеуі болып табылады. Сонымен қатар, хештеудің әмбебап әдістері жоқ және оларды қолдану саласына қарай таңдаған жөн. Ерекше рөлді теориялық-күрделілік проблемалары, атап айтқанда алгебралық сандар теориясы атқарады. Осындай проблемалардың бірі ақырлы өрісте дәрежесі берілген келтірілмейтін көпмүшеліктерді іздеу болып табылады, оларды хабарламалардың хеш-кодтарын іздеуде қолдануға болады. Қарапайым және кеңейтілген Галуа өрістерінде келтірілмейтін көпмүшеліктерді зерттеудің өзектілігі олардың ғылым мен техниканың әр түрлі салаларында түрлі қолданылуымен байланысты. Келтірілмейтін көпмүшеліктер математиканың, ақпараттық технологияның және ақпараттық қауіпсіздіктің әр түрлі салаларында қолданыс тапты. Келтірілмейтін көпмүшеліктердің қасиеттерін қолдану арифметиканың ақырлы өрістерде компьютерлік тиімді іске асырылуын арттыруға мүмкіндік береді, ал бұл, өз кезегінде, криптография мен кодтау теориясы үшін ерекше маңызды. Келтірілмейтін көпмүшеліктерді табу есептеу үшін, әсіресе өлшемі үлкен өрістер үшін күрделі мәселе болып табылады. Келтірілмейтін көпмүшеліктерді іздеу процедурасы жай сандар жағдайындағы сияқты тиімді алгоритмдер мен үлкен есептеу қорларын қажет етеді, ал бұл, өз кезегінде, олардың негізінде тиімді хештеу алгоритмдерін құру үшін негізгі мәселелердің бірі болып табылады. ұсынылған мақалада хеш-функцияларды құрудың келтірілмейтін көпмүшелікке бөлгендегі қалдықты есептеуге негізделген әдісі сипатталған. Сонымен қатар, келтірілмейтін көпмүшеліктерді іздеу мәселесі қарастырылады. Ақырлы өрістерде келтірілмейтін көпмүшеліктерді қолдана отырып, хеш-функцияларды компьютерлік модельдеу жүргізілді. Әр түрлі келтірілмейтін көпмүшеліктерді қолдану нәтижелері және оларды талдау келтірілген. Мақаланың нәтижелерін криптографиялық қосымшалар мен кодтау теориясында қолдануға болады.

Түйін сөздер: келтірілмейтін көпмүшелік, хеш-функция, ақырлы өріс, артық циклдік код, соқтығысу.

U.K. Turusbekova[1*], A.S. Turginbayeva[2]
[1]Kazakh University of Economics, Finance and International Trade,
Nur-Sultan, Kazakhstan
[2]L.N. Gumilyov Eurasian National University,Nur-Sultan, Kazakhstan
*e-mail: umut.t@mail.ru

Hashing with polynomials

Hash functions are easy-to-compute compression functions that take a variable-length input and convert it to a fixed-length output. Hash functions are used as compact representations, or digital fingerprints, of data and to provide message integrity. In modern cryptography, various hash functions are widely used. The main problem with using hash functions is that the existence of irreversible functions that exclude the possibility of collisions has not been proven. In addition, there are no universal hashing methods, and they should be selected depending on their area of application. A special role is played by complexity-theoretical problems, namely, algebraic number theory. One of these problems is the search for irreducible polynomials of a given degree over a finite field, which can be used to search for message hash codes. The relevance of the study of irreducible polynomials over simple and extended Galois fields is due to their diverse

application in various fields of science and technology. Irreducible polynomials have found their application in various fields of mathematics, information technology and information security. Using the properties of irreducible polynomials allows you to maximize the effective computer implementation of arithmetic in finite fields, which is of particular importance for cryptography and coding theory. Finding irreducible polynomials is difficult to compute, especially over large fields. The procedure for finding irreducible polynomials requires efficient algorithms and large computational resources, as in the case of finding prime numbers, which is the main problem for constructing effective hashing algorithms based on them. This article describes a method for constructing hash functions based on calculating the remainder of a division by irreducible polynomials. In addition, the problem of searching for irreducible polynomials is considered. Computer modeling of hash functions using irreducible polynomials over finite fields has been performed. The results of using various irreducible polynomials and their analysis are presented. The results of the article can be used in cryptographic applications and coding theory.

Key words: irreducible polynomial, Hash function, finite field, redundant cyclic code, collision.

1 Введение

Системы информационных технологий требуют наличия эффективных инструментов, которые позволили бы значительно сократить объём памяти, необходимый для хранения и передачи больших объёмов данных, доступных ограниченному числу пользователей, и для проверки их целостности. Это также связано с тем, что финансовые операции с денежными средствами и хранение личных данных пользователей осуществляются в Интернете. Для таких целей широко используются хеш-функции. Они преобразуют исходные данные произвольной длины в последовательность фиксированной длины, называемую хеш-кодом или сверткой сообщения.

Хеш-функции целесообразно применять к ценным конфиденциальным данным, доступ к которым могут получить только определенные лица. Такие данные чаще всего представлены в виде текста или последовательности символов. Следует отметить, что при незначительных изменениях во входных данных результат хеш-функции должен полностью измениться, то есть иметь лавинный эффект, чтобы гарантировать, что данные не могут быть фальсифицированы незначительными изменениями. Эта хеш-функция также позволяет использовать их в следующих случаях: для поиска дубликатов в наборе данных; построение ассоциативных массивов; расчет контрольных сумм для последующего выявления и исправления ошибок, возникших при передаче или хранении данных; разработка электронной цифровой подписи; для сохранения паролей в базах данных.

Разработка качественной хеш-функции является сложной задачей. При разработке алгоритмов хеширования следует учитывать уязвимость хеш-функций. Степени набора входных последовательностей и множества всех возможных значений хеш-функции можно найти в любом соотношении. Как правило, набор входных данных имеет большую размерность, чем количество всех возможных значений функции, что приводит к преобразованию различных сообщений в один хеш. Такой случай называется «столкновением» (или «коллизией») и является одним из важных факторов, который учитывается при построении алгоритмов хеширования в криптографических системах [1], а также во многих структурах данных, таких как хеш-таблицы [2].

На данном этапе развития теории хеширования до сих пор нет четкого определения понятия хеш-функции и точных требований к их построению. Общие требования,

которым должны соответствовать хеш-функции, это – необратимость (невозможно создать алгоритм с полиномиальной вычислительной сложностью, который восстанавливает исходные данные в реальном времени), устойчивость к столкновениям, высокая скорость вычислений и наличие лавинного эффекта (с небольшим изменением во входных данных результат должен существенно отличаться). В зависимости от приложения к хеш-функции предъявляются дополнительные требования, такие как сложность вычислений, длина свертки и криптографическая стабильность.

Основная проблема использования хеш-функций заключается в том, что существование необратимых функций, исключающих возможность столкновений, не доказано. Кроме того, не существует универсальных методов хеширования, и их следует выбирать в зависимости от области их применения. На практике используются функции, для которых теоретическая вероятность столкновений близка к нулю, но с появлением более мощных вычислительных устройств поиск столкновений может оказаться не такой сложной задачей. По этой причине существующие алгоритмы требуют постоянного улучшения. Особую роль играют теоретико-сложностные проблемы, а именно алгебраическая теория чисел [3]. Одной из таких проблем является поиск неприводимых многочленов заданной степени над полем k_p или $Gk(p)$, которые можно использовать для поиска хеш-кодов сообщений. В статье рассматривается проблема поиска неприводимых многочленов, а также метод хеширования, основанный на вычислении остатка от деления на неприводимый многочлен.

2 Обзор литературы

В 1976 году Диффи и Хеллман впервые подчеркнули необходимость построения однонаправленной функции как составной части схемы цифровой подписи [4]. Этот год можно считать отправной точкой развития хеш-функций. Хеш-функции используются в качестве строительного блока во многих приложениях. Некоторые хэш-функции, используемые в настоящее время, оказались уязвимыми. В работе [5] автор утверждает, что их замены должны основываться на математической теории. В работе [6] исследованы потенциальные математические принципы и структуры, которые могут обеспечить основу для криптографических хеш-функций, а также представить простую и эффективно вычисляемую хеш-функцию, основанную на неассоциативной операции с многочленами над конечным полем характеристики 2. Общий обзор хеш-функций приведен в работе [7]. В работе [8] в хронологическом порядке развития приведены основные принципы построения алгоритмов хеширования. Отметим работу [9], в которой предложен способ усложнения поиска коллизий хеш-функций методом рандомизации входных данных для функции сжатия. Такой способ позволяет замаскировать коллизии в функции сжатия. Способ позиционируется авторами как отдельный режим работы криптосистемы хеширования без изменения самой ее конструкции. Может быть полезен в цифровых подписях для предотвращения сценария атаки нахождения второго прообраза.

Для изучения методов хеширования, основанных на использование деления по модулю неприводимого многочлена, мы развиваем идеи работы [3]. Кроме того, рассматриваем проблему поиска неприводимых многочленов и их анализ.

3 Материал и методы

3.1 Неприводимые многочлены над конечными полями

Такие разделы алгебры, как теория конечных полей и теория многочленов над конечными полями, все больше влияют на построение различных систем защиты информации, кодирования и декодирования информации. В частности, появились алгоритмы для циклических избыточных кодов [10], которые используют многочлены над полями k_p. Циклические избыточные коды могут использоваться в качестве хеш-функций для обнаружения ошибок и проверки целостности данных.

Поскольку конечное поле является множеством с конечным числом элементов, операции сложения, вычитания, умножения и деления могут выполняться в соответствии с аксиомами поля [11]. Так как конечные поля являются замкнутыми относительно вышеупомянутых операций, то для любых двух элементов поля $a, b \in k_p$, при выполнении любой из операций, результатом является элемент $c \in k_p$, принадлежащий этому полю. Следует иметь в виду, что все вычисления в конечных полях производятся по модулю p, который является характеристикой конечного поля и является простым числом.

Простейшим примером конечного поля является кольцо классов вычетов $Z/(p)$ по модулю простого числа p, которое можно отождествить с полем Галуа $k_p = Gk(p)$ порядка p [6]. Согласно теореме о существовании и единственности конечных полей для любого простого числа p и натурального числа n существует конечное поле из p^n элементов. Чтобы построить поле k_{p^n}, необходимо найти многочлен $S(x)$ степени n, неприводимый над полем k_p. Такое поле представлено многочленами над k_p степенью не выше $n-1$.

В компьютерной криптографии многочлены, особенно неприводимые многочлены, играют значительную роль в последние два десятилетия. Напомним, что *неприводимый многочлен* – это многочлен, который не разлагается на нетривиальные многочлены и является аналогом простых чисел в натуральном ряду. Особенностью неприводимых многочленов является то, что, будучи неприводимым в одной области, многочлен оказывается приводимым в другой области, что нашло применение в теории кодирования и системах защиты информации.

Поиск неприводимых многочленов является сложной для вычисления задачей, особенно над полями большой размерности. Процедура нахождения неприводимых многочленов требует эффективных алгоритмов и больших вычислительных ресурсов, как в случае нахождения простых чисел [12], что является основной проблемой для построения эффективных алгоритмов хеширования на их основе. На данный момент нет эффективных алгоритмов поиска неприводимых многочленов, есть только критерии неприводимости и методы проверки неприводимости. Поиск осуществляется путем изучения мульти-тел и проверки каждого из них на неприводимость. Для проверки многочлена $S(x)$ степени $n \geq 2$ на неприводимость над полем характеристики p существует следующий алгоритм [13], [14]:

1. Инициализируется начальное значение многочлена $G_0(x) = x$.
2. Рассчитывается следующее значение $G_1(x) = G_0(x)^p mod S(x)$.
3. Рассчитывается наибольший общий делитель (НОД) многочленов $S(x)$ и $(G_1(x) - x)$. Если НОД не равен единице, то этот многочлен приводим. В противном случае,

следующее значение рассчитывается по формуле повторения

$$G_i(x) = G_{i-1}(x)^p mod S(x),$$

где $i = \overline{1, \lfloor n/2 \rfloor}$, $\lfloor \rfloor$ – операция взятия целой части числа.

4. Если НОД $S(x)$ и каждого $(G_i(x) - x)$ равен единице, то многочлен $S(x)$ – неприводим.

Недостатком такого алгоритма является низкая скорость вычислений для достаточно больших значений, поскольку на каждом шаге выполняется операция увеличения и нахождения НОД.

Для вычислений в конечных полях используется полиномиальная арифметика. Сложение в поле k_{p^n} соответствует обычному сложению многочленов по модулю p. Умножение выполняется в два этапа – сначала как простое умножение многочленов, а затем вычисляется остаток от деления на неприводимый многочлен, с помощью которого строится поле k_{p^n}. Например, поля одной и той же размерности могут быть построены по-разному, в зависимости от выбора неприводимого многочлена. Они одного порядка и изоморфны друг другу. Это следует из того факта, что для характеристики поля имеется несколько неприводимых многочленов степени n. Примеры неприводимых многочленов для поля k_2 приведены ниже [15]:

$n = 2$ $\quad x^2 + x + 1;$

$n = 3$ $\quad x^3 + x^2 + 1, \;\; x^3 + x + 1;$

$n = 4$ $\quad x^4 + x^3 + x^2 + x + 1, \;\; x^4 + x^3 + 1, \;\; x^4 + x + 1;$

$n = 5$ $\quad x^5 + x^2 + 1, \;\; x^5 + x^3 + x^2 + x + 1, \;\; x^5 + x^4 + x^3 + x + 1,$

$x^5 + x^4 + x^3 + x^2 + 1, \;\; x^5 + x^4 + x^2 + x + 1.$

3.2 Моделирование хеш-функций на основе неприводимых многочленов

В последние два десятилетия значительную роль в компьютерной криптографии играют многочлены, особенно неприводимые многочлены. Одним из возможных способов построения хеш-функции является использование деления по модулю неприводимого многочлена [3]. Для эффективности компьютерной реализации удобно использовать вычисления в полях k_{2^r}. Это позволяет производить расчеты по данным в виде последовательности битов. Поиск оставшейся части деления осуществляется с использованием побитовых сдвигов и разделительной дизъюнкции.

Для хеширования данные кодируются некоторым выбранным способом в последовательности $a_1, a_2, \ldots, a_m$ нулей и единиц, соответствующих определенному многочлену $A(x)$, а хеш-код $h(a_1, a_2, \ldots, a_m)$ представляет собой последовательность битов, полученных делением на неприводимый многочлен $S(x)$, и вычисляется по следующим формулам:

$$B(x) = A(x) mod S(x) \tag{1}$$

$$h(a_1, a_2, \ldots, a_m) = b_n b_{n-1} \ldots b_1 b_0 \quad (2)$$

В формуле (2) $b_n b_{n-1} \ldots b_1 b_0$ – это коэффициенты многочлена $B(x)$, полученные как остаток от деления многочлена $A(x) = a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_{m-1} x + a_m$ на многочлен $S(x) = s_n x^n + s_{n-1} x^{n-1} + \cdots + s_1 x + s_0$ степени n.

Такая функция устойчива к восстановлению исходных данных, поскольку, даже зная размерность поля и используемый неприводимый многочлен, трудно расшифровать данные, особенно для больших степеней неприводимого многочлена. Неприводимые многочлены следует выбирать на основе области действия хеш-функций, так как длина свертки равна степени многочлена. Итак, для применения в системах защиты информации на данный момент оптимальная длина составляет не менее 128 бит и не более 512 бит. Использование многочлена достаточной размерности играет существенную роль. Если выбран многочлен степени l, то множество всех возможных значений, которые может принять свертка функции, равно 2^l. Например, при использовании неприводимого многочлена $S(x) = x^4 + x + 1$ количество всех возможных пакетов будет 16, и поиск сообщений с одинаковыми свертками не составит труда.

4 Результаты и обсуждение

Компьютерное моделирование хеш-функций проводилось на основе неприводимых многочленов степени 32 с разным количеством одночленов. В результате анализ эффективности хеширования проводится с использованием каждого из многочленов. Важным фактором при выборе неприводимого многочлена является количество в нем одночленов. Для более высокой скорости вычислений желательно найти многочлены с минимальным количеством одночленов. Для сравнения результатов хеширования были выбраны многочлены с 5, 12 и 18 одночленами. Скорости вычислений для сверток входных данных различной длины и использования различных неприводимых многочленов одинаковой степени приведены в таблице 1. Неприводимые многочлены были записаны в двоичном представлении, представляющем собой последовательность коэффициентов при одночленах. Коэффициент наибольшей степени здесь не учитывается. Например, для многочлена $S(x) = x^4 + x + 1$ будет верным равенство $x^4 = x + 1$, так как операция вычитания аналогична добавлению по модулю 2. Напишем многочлен в виде $x^4 = 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$, поэтому в двоичном представлении многочлен будет записан как 0011, а количество бит для его записи равно степени многочлена.

На первый взгляд разница в скорости вычислений невелика, но, при обработке объемов данных от 1 МБ или более, разница между вычислениями может составлять один час или более. Этот метод хеширования эффективен для применения небольших объемов данных в пределах нескольких килобайт. Таблица 2 показывает результаты хеширования неприводимыми многочленами из таблицы 1 для произвольной 64-битной строки и для той же строки с небольшими изменениями для проверки лавинного эффекта и свойства смешения.

Функции, реализованные на основе рассматриваемых многочленов, обладают свойством перемешивания. Это означает, что нет никакой связи между сверткой и исходными данными. Поскольку при незначительном изменении исходных данных результат

Таблица 1 – Скорость расчета свертки с использованием неприводимых многочленов степени 32

№	Неприводимые многочлены	Длина последовательности, бит		
		64	256	512
1	00000000010000000000000000000111	1,1	1,8	2,2
2	10000001010000010100000110101011	1,9	2,1	2,5
3	01110100000110111000110011010111	2,1	3,6	4,9

Таблица 2 – Результаты применения хеш-функций на основе неприводимых многочленов степени 32

Исходная битовая последовательность	Неприводимые многочлены		
	1	2	3
0110001100111001	11010011	01000110	01010111
0001110000011111	11101101	00001100	11011111
1110000011001000	01000000	01101101	00101111
0110110100011111	00001110	01100110	01001100
0110001100111001	11010000	01010010	11110010
0010110000011111	11101101	00000101	00010011
1110000011001000	11010000	00100010	11101010
0110110100011111	00101010	10110110	01001010

хеширования должен значительно измениться, в исходной битовой последовательности 19-й и 20-й биты были изменены для проверки соответствия этому свойству. На основании результатов, приведенных в таблице 2, наилучшим лавинным эффектом обладают функции, основанные на многочленах с большим количеством одночленов. Стоит отметить, что, несмотря на небольшую степень приведенных выше многочленов, хеш-функции на их основе имеют некоторое сопротивление столкновениям. При сортировке пачек, полученных обработкой данных в объеме 1000, 5000, 10000 и 30000, коллизий обнаружено не было, хотя это не может гарантировать их отсутствие на больших объемах.

Рассматриваемый метод хеширования подходит для битовых последовательностей, которые могут быть представлены многочленом более высокой степени, чем степень выбранного неприводимого многочлена. Меньшие последовательности должны быть дополнены функцией. В большинстве существующих алгоритмов хеширования добавление к требуемой длине выполняется путем добавления к последовательности одного бита и битов нулей. Кроме того, желательно добавить в последовательность ее первоначальную длину, что уменьшит вероятность столкновения после добавления. Использование остатка от деления на неприводимый многочлен может служить отдельной хеш-функцией и используется в сочетании с другими алгоритмами для улучшения определенных свойств. Также хеш, найденный этим методом, может быть использован в качестве криптографической соли.

5 Заключение

Теория конечных полей может быть использована для построения хеш-функций, но наряду с ее применением возникают проблемы, которые требуют отдельного исследования для дальнейших решений. Одной из таких проблем является нахождение неприводимых многочленов с определенными свойствами. Для полей, характеризующих простые числа большой разрядности, задача поиска неприводимых многочленов определенных степеней значительно сложнее и требует больших вычислительных затрат.

Было показано, что целесообразно использовать неприводимые многочлены достаточно больших степеней. Многочлены, состоящие из небольшого числа одночленов, позволяют находить свертки для меньшего числа операций. Однако многочлены с большим числом одночленов улучшают лавинный эффект хеш-функции. Оба имеют одинаковое сопротивление столкновениям. Неприводимый многочлен должен быть выбран на основе требуемых свойств хеш-функции. Чтобы усилить криптографическую стойкость и улучшить лавинный эффект, необходимо выбрать неприводимые многочлены степени 128 и выше с максимально возможным количеством одночленов. В случаях, когда хеш-функция используется в системах, требующих высокой скорости вычислений, рекомендуется использовать неприводимые многочлены с минимальным количеством одночленов.

Основным недостатком хеш-функций, основанных на неприводимых многочленах, является низкая скорость вычислений для больших объемов данных. Помимо расширений рассматриваемого поля, для увеличения устойчивости к столкновениям необходимо учитывать поля больших характеристик, что является задачей для дальнейшего решения. Это позволит хешировать данные в элементы из большего поля, но следует учитывать, что это усложнит компьютерные операции на компьютере.

Список литературы

[1] Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на Си / пер. с англ.; под ред. Н. Дубновой. // Изд. 2-е.- М.: Диалектика. - 2003. – 610 с.

[2] Sedgewick R. Algorithms in C++, Parts 1-4 // Fundamentals, Data Structure, Sorting, Searching. - 3rd ed.- 1988.-752 p.

[3] Хомич Э.А. Неприводимые многочлены над конечными полями и связь с криптографией // Academic Publicistics.- 2017.-№3.- С.19-22.

[4] Whitfield Diffiee, Martin E. Hellman. New directions in cryptography // IEEE Trans. on Information Theory, Vol. IT-22, No. 6.- 1976. - P.644-654.

[5] Landau S. Find Me a Hash // Notices Amer. Math. Soc. – 2006. - V.53. – P. 330-332.

[6] Shpilrain V. Hashing with Polynomials // Information Security and Cryptology – ICISC 2006. - LNCS 4296. - Springer, 2006. - P. 22-28. DOI: https://doi.org/10.1007/11927587_4

[7] Menezes A., P. van Oorschot, Vanstone S. Handbook of Applied Cryptography// CRC Press. - 1997.

[8] Авезова Я.Э. Современные подходы к построению хеш-функций на примере финалистов конкурса SHA-3 // Вопросы кибербезопасности.- 2015.- №3(11).- С.60-67.

[9] Shai Halevi, Hugo Krawczyk. Strengthening Digital Signatures via Randomized Hashing // Advances in Cryptology - CRYPTO - LNCS 4117. - Springer, 2006. - P.41-59. DOI: https://doi.org/10.1007/11818175_3

[10] Henry S. Warren, Jr. Hacker's Delight. - 3rd ed.// Addison Wesley. - 2013.- 816 p.

[11] Лидл Р., Нидеррайтер Х. Конечные поля. - в 2 т. // пер. с англ.; под ред. В.И. Нечаева. // М.: Мир. - 1988.- Т.1.- 430 с.

[12] Turusbekova U.K., Azieva G.T. Investigation of irreducible normal polynomials special type over a field of characteristic 2 // Вестник КазНПУ им. Абая, серия "Физико-математические науки2019.- №3(67).-С.122-127.

[13] Crandall R. E., Pomerance C. B. Prime Numbers: A Computational Perspective. // New York: Springer-Verlag. - 2005.- 597 p.

[14] Горбенко И.Д., Штанько И.А. Функции хеширования. Понятия, требования, классификация, свойства и применение // Радиоэлектроника и информатика. - 1998. - №1.-С.64-69.

[15] Sankhanil Dey, Amlan Chakrabarti, Ranjan Ghosh. 4-bit crypto S-boxes: Generation with irreducible polynomials over Galois field GF(24) and cryptanalysis // International Journal of Tomography and Simulation. – 2019.- Vol. 32, no. 3.- P.46-60.

References

[1] Shcneier B., *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C* , (1995): 784.

[2] Sedgewick R., *Algorithms in C++ , Parts 1-4: Fundamentals, Data Structure, Sorting, Searching* - 3rd ed. (1988): 752.

[3] Khomich E.A., "Neprivodimyye mnogochleny nad konechnymi polyami i svyaz' s kriptografiyey [Irreducible polynomials over finite fields and connection with cryptography]" , *Academic Publicistics*, Vol.3 (2017): 19-22.

[4] Whitfield Diffiee and Martin E. Hellman, "New directions in cryptography" , *IEEE Trans. on Information Theory* Vol. IT-22, no. 6.(1976):644-654.

[5] Landau S., "Find Me a Hash" , *Notices Amer. Math. Soc.*, vol.53 (2006): 330-332.

[6] Shpilrain V., "Hashing with Polynomials" , *Information Security and Cryptology – ICISC 2006* LNCS 4296 (2006): 22-28. Springer, 2006. DOI: https://doi.org/10.1007/11927587_4

[7] Menezes A., P. van Oorschot and S Vanstone, "Handbook of Applied Cryptography" , *CRC Press* (1997).

[8] Avezova YA.E., "Sovremennyye podkhody k postroyeniyu khesh-funktsiy na primere finalistov konkursa SHA-3 [Modern approaches to the construction of hash functions using the example of the finalists of the SHA-3 contest]" , *Voprosy kiberbezopasnosti*, no. 3(11) (2015): 60-67.

[9] Shai Halevi and Hugo Krawczyk, "Strengthening Digital Signatures via Randomized Hashing" , *Advances in Cryptology-CRYPTO 2006,* LNCS 4117 (2006): 41-59. Springer, 2006. DOI: https://doi.org/10.1007/11818175_3

[10] Henry S. and Warren, Jr., *Hacker's Delight* , - 3rd ed., Addison Wesley (2013): 816.

[11] Lidl R. and Niderrayter H., *Finite Fields* , Cambridge: Cambridge University Press (2000): 768.

[12] Turusbekova U.K. and Azieva G.T., "Investigation of irreducible normal polynomials special type over a field of characteristic 2" , *Vestnik KazNPU im. Abaya, seriya "Fiziko-matematicheskiye nauki"* no 3(67) (2019): 122-127.

[13] Crandall R. E. and Pomerance C. B., *Prime Numbers: A Computational Perspective* , New York: Springer-Verlag (2005): 597.

[14] Gorbenko I.D. and Shtan'ko I.A., "Funktsii kheshirovaniya. Ponyatiya, trebovaniya, klassifikatsiya, svoystva i primeneniye [Hash Functions Concepts, requirements, classification, properties and application]" , *Radioelektronika i informatika*, no. 1 (1998): 64-69.

[15] Sankhanil Dey, Amlan Chakrabarti and Ranjan Ghosh, "4-bit crypto S-boxes: Generation with irreducible polynomials over Galois field GF(24) and cryptanalysis" , *International Journal of Tomography and Simulation*, vol. 32, no. 3 (2019): 46-60.

К СВЕДЕНИЮ АВТОРОВ

1. В журнал «Вестник КазНУ. Серия математика, механика, информатика» (в английской версии «Journal of Mathematics, Mechanics and Computer Science Series») принимаются набранные только в текстовом формате LaTeX 2$_\varepsilon$ на казахском, русском или английском языках, ранее не опубликованные проблемные, обзорные, дискуссионные статьи в области естественных наук, где освещаются результаты фундаментальных и прикладных исследований.

2. Материалы следует направлять по адресу: 050040 Алматы, ул. аль-Фараби, 71, корпус 13, Научно-исследовательский институт механики и математики КазНУ им. аль-Фараби, каб. 418, тел. 22-11-568. Электронная почта: mechmatvestnik@gmail.com (ответственный секретарь редколлегии, Темешева С.М.)

3. Статья должна сопровождаться письмом от учреждения, в котором выполнена данная работа, где указываются сведения об авторах: Ф.И.О. полностью, место их работы (название вуза, центра без сокращений), рабочий или моб. телефон, e-mail, домашний адрес и контактный телефон.

4. В редакцию необходимо представить электронную версию статьи: tex-файлы работы и файлы рисунков на одном диске. Для файлов рисунков рекомендуется использовать средства основного пакета LaTeX 2$_\varepsilon$ или формат .eps [см. п.7]. В редакцию также представляется оттиск работы в двух экземплярах.

5. Объем статьи, включая список литературы, таблицы и рисунки с подрисуночными надписями, аннотации, не должен превышать 17 страниц печатного текста. Минимальный объем статьи - 7 страниц.
   Структура статьи.
   Первая страница:
   1) Первая строка - номер МРНТИ (IRSTI) (можно взять здесь: http://grnti.ru/), выравнивание по левому краю, шрифт - полужирный.
   2) Название статьи (Заголовок) должно отражать суть и содержание статьи и привлекать внимание читателя. Название должно быть кратким, информативным и не содержать жаргонизмов или аббревиатур. Оптимальная длина заголовка - 5-7 слов (в некоторых случаях 10-12 слов). Название статьи должно быть представлено на русском, казахском и английском языках. Название статьи представляется полужирным шрифтом строчными буквами, выравнивание - по центру.
   3) Автор(ы) статьи - Инициалы и фамилия, место работы (аффилиация), город, страна, email – на русском, казахском и английском языках. Сведения об авторах представляются обычным шрифтом строчными буквами, выравнивание - по центру.
   4) Аннотация объемом 150-500 слов на русском, казахском и английском языках. Структура аннотации включает в себя следующие ОБЯЗАТЕЛЬНЫЕ пункты: "Вступительное слово о теме исследования. "Цель, основные направления и идеи научного исследования. "Краткое описание научной и практической значимости работы. "Краткое описание методологии исследования. "Основные результаты и анализ, выводы исследовательской работы. "Ценность проведенного исследования (внесенный вклад данной работы в соответствующую область знаний). "Практическое значение итогов работы.
   5) Ключевые слова/словосочетания - количеством 3-5 на русском, казахском и английском языках.

   Последующая страница (новая):

   Стандартные разделы статьи: **Введение, Обзор литературы, Материал и методы, Результаты и обсуждение, Заключение, Благодарности (если имеются), Список литературы** (названия разделов не менять)

   6) **Введение.** Введение состоит из следующих основных элементов: "Обоснование выбора темы; актуальность темы или проблемы. В обосновании выбора темы на основе описания опыта предшественников сообщается о наличии проблемной ситуации (отсутствие каких-либо исследований,

появление нового объекта и т.д.). Актуальность темы определяется общим интересом к изученности данного объекта, но отсутствием исчерпывающих ответов на имеющиеся вопросы, она доказывается теоретической или практической значимостью темы. "Определение объекта, предмета, целей, задач, методов, подходов, гипотезы и значения вашей работы. Цель исследования связана с доказательством тезиса, то есть представлением предмета исследования в избранном автором аспекте.

7) **Обзор литературы.** В разделе обзор литературы должны быть охвачены фундаментальные и новые труды по исследуемой тематике зарубежных авторов на английском языке (не менее 15 трудов), анализ данных трудов с точки зрения их научного вклада, а также пробелы в исследовании, которые Вы дополняете в своей статье. НЕДОПУСТИМО наличие множества ссылок, не имеющих отношения к работе, или неуместные суждения о ваших собственных достижениях, ссылки на Ваши предыдущие работы.

8) **Материал и методы.** Раздел должен состоять из описания материалов и хода работы, а также полного описания использованных методов. Характеристика или описание материала исследования включает его представление в качественном и количественном отношении. Характеристика материала – один из факторов, определяющий достоверность выводов и методов исследования. В этом разделе описывается, как проблема была изучена: подробная информация без повторения ранее опубликованных установленных процедур; используется идентификация оборудования (программного обеспечения) и описание материалов, с обязательным внесением новизны при использовании материалов и методов. Научная методология должна включать в себя: - исследовательский вопрос(-ы); - выдвигаемую гипотезу (тезис); - этапы исследования; - методы исследования; - результаты исследования.

9) **Результаты и обсуждение.** В этом разделе приводятся анализ и обсуждение полученных вами результатов исследования. Приводятся выводы по полученным в ходе исследования результатам, раскрывается основная суть. И это один из самых важных разделов статьи. В нем необходимо провести анализ результатов своей работы и обсуждение соответствующих результатов в сравнении с предыдущими работами, анализами и выводами.

10) **Заключение.** Обобщение и подведение итогов работы на данном этапе; подтверждение истинности выдвигаемого утверждения, высказанного автором, и заключение автора об изменении научного знания с учетом полученных результатов. Выводы не должны быть абстрактными, они должны быть использованы для обобщения результатов исследования в той или иной научной области, с описанием предложений или возможностей дальнейшей работы. Структура заключения должна содержать следующие вопросы: Каковы цели и методы исследования? Какие результаты получены? Каковы выводы? Каковы перспективы и возможности внедрения, применения разработки?

11) **Благодарности (если имеются).** Например: Работа выполнена при поддержке грантового финансирования научно-технических программ и проектов Министерством науки и образования Республики Казахстан (грант «Наименование темы гранта», 2018-2020 годы).

12) **Список литературы/References.** (оба списка, если статья на русском или казахском. Если статья на английском, то только один список по стилю Чикаго). Список используемой литературы, или Библиографический список состоит из не менее 30 наименований литературы, и из них 50% на английском языке. В случае наличия в списке литературы работ, представленных на кириллице, необходимо представить список литературы в двух вариантах: первый – в оригинале, второй – романизированным алфавитом (транслитерация). Романизированный список литературы должен выглядеть в следующем виде: автор(-ы) (транслитерация) → название статьи в транслитерированном варианте [перевод названия статьи на английский язык в квадратных скобках], название русскоязычного источника (транслитерация, либо английское название - если есть), выходные данные с обозначениями на английском языке (год в круглых скобках) → страницы. Например: Gokhberg L., Kuznetsova T. Strategiya-2020: novye kontury rossi- iskoi innovatsionnoi politiki [Strategy 2020: New Outlines of Innovation Policy]. Foresight-Russia, vol. 5,

no 4 (2011): 8-30. Список литературы представляется по мере цитирования, и ТОЛЬКО те работы, которые цитируются в тексте. Ссылки на литературу оформляются в квадратных скобках с указанием номера литературы. Стиль оформления "Список литературы"на русском и казахском языке согласно ГОСТ 7.1-2003 "Библиографическая запись. Библиографическое описание. Общие требования и правила составления"(требование к изданиям, входящих в перечень ККСОН). Стиль оформления "References"романизированного списка литературы (см. выше), а также источников на английском (другом иностранном) языке для естественнонаучных и технических направлений согласно Chicago Style (www.chicagomanualofstyle.org).

В данном разделе необходимо учесть:

а) Цитируются основные научные публикации, передовые методы исследования, которые применяются в данной области науки и на которых основана работа автора.

б) Избегайте чрезмерных самоцитирований.

в) Избегайте чрезмерных ссылок на публикации авторов СНГ/СССР, используйте мировой опыт.

г) Библиографический список должен содержать фундаментальные и наиболее актуальные труды, опубликованные известными зарубежными авторами и исследователями по теме статьи.

6. Журнал придерживается единого стиля и поэтому предъявляет ряд общих требований к оформлению работ. Исходный (неоттранслированный) tex-файл должен целиком помещаться в горизонтальных рамках экрана за возможным исключением матриц и таблиц и транслироваться без протестов LaTeX 2_ε и сообщений о кратных и неопределенных метках, больших переполненных и незаполненных боксах. Не следует определять много новых команд, изобретая собственный сленг. Авторы могут подгружать другие стандартные стилевые пакеты, но только те, которые не входят в противоречие с пакетами amsmath и amssymb. Естественно файл, кроме всего прочего, должен быть проверен на отсутствие грамматических и стилистических ошибок. Статьи, не удовлетворяющие этим требованиям, возвращаются на доработку.

   Эталонный образец работы с демонстрацией графики, с преамбулой устраивающей редакцию, списки типичных ошибок оформления и методы их устранения можно получить в редакции или на сайте КазНУ им. аль-Фараби http://journal.kaznu.kz.

7. Графические файлы с рисунками должны быть только качественными черно-белыми в формате .eps, либо выполненными в латеховском формате. Рисунки в этих форматах делаются, например, с помощью мощных математических пакетов Maple, Mathematica или с помощью пакета Latexcad. Качественные графические файлы сделанные другими графическими программами должны быть сконвертированы в формат .eps с помощью Adobe Photoshop или конвертера Conversion Artist. Все рисунки должны быть уже импортированными в tex-файл и представляются в редакцию вместе с основным файлом статьи. Графические форматы, отличные от вышеуказанных, отвергаются.

   Редакция вправе отказаться от включения в работу рисунка, если автор не в состоянии обеспечить его надлежащее качество.

МАЗМҰНЫ – СОДЕРЖАНИЕ – CONTENTS

4-бөлім **Раздел 4** **Section 4**

Қолданылмалы математика **Прикладная математика** **Applied Mathematics**